satswana

Company registered number 09329065 www.satswana.com

Contents

A Satswana Update January 2021

1 Recording online meetings?

May we please revisit this issue by extracting below one of the (edited) answers to the question as to whether you should do so, and how long to retain the recording if you did?

This answer referred to the use of Google as a medium and we have since discovered that Microsoft Teams records by default which, for the reasons stated, we suggest should not be the case. We do acknowledge that there may be occasions when you wish to replay a recording to a student who was not able to view it first time around, but believe that this content should be under the control of the school – not Teams.

In response to another customer's question we found information on Microsoft Stream that may be an appropriate option. They state "In the new Stream, video and audio files will be stored on the SharePoint files platform within Microsoft 365 like all other file types; already today, SharePoint powers file experiences for Microsoft Teams, OneDrive, Yammer, and Outlook. This will provide the best of both worlds: intelligent video experiences powered by Stream across the suite, and management of video that leverages the power of SharePoint content services for permissions, sharing, compliance, governance, and customizable portal experiences."

We ask whether it is sensible or appropriate to replay a lesson, that has all the interactions that you would expect, to somebody who did not experience that as a "live" event. You will decide.

In giving advice, may we constantly stress our "mantra" that "you are the Boss". We may express an opinion, but totally accept that it is your right to make your own risk assessment and executive decision in all matters.

It is actually our declared policy – recommended to our customers – that online meetings are NOT recorded, for two reasons. First, because we state that the same conditions should apply as if it was a physical meeting. If you would not record the class session, why should you record an online class just because the medium used allows you to do so? The second reason is the "retention" reason that we have raised as a conundrum on several occasions – how long do you keep it for? They say that "the data you do not keep is the safest". Retention periods and the need to delete data are two very difficult questions that currently challenge every

administration, and within Google the fact that the files do not "auto-delete" precisely expresses why it is a problem. (It is understood that Teams delete after 20 days as a default.)

We absolutely understand any thinking regarding the protection of staff, but our experience there is that this can be a two edged sword. On the one hand it is absolutely true to say that you would have the evidence to discount an unfounded allegation. On the other hand we have unfortunate experience of vexatious parents using their access request "rights" to demand a review of data held, often as a pure "fishing" exercise that seeks to discover something that they can take issue with. If you do not have the data, then you cannot be exposed to that risk. It is an unfortunate reality that something the Teacher has done or said may be perfectly reasonable, until it is taken out of context by a campaigning lawyer. You will have your own view regarding the ease with which reasonable opinions can be misrepresented these days.

In presenting this "argument", it is our belief that the balance of advantage supports a policy of not recording online meetings or class sessions. If you did so, we would then seek to severely restrict the retention period to as short a time as we can persuade you to adopt. But to repeat in conclusion, it is your executive decision to make, and we acknowledge the safeguarding point.

2 Managing the content

Satswana are keen students of the updates issued by Andrew Hall as a Guru of Safeguarding and we note the current advice he provides for the Designated Safeguarding Lead in managing the additional risks that arise from the vast expansion of online learning.

(Andrew Hall (Safeguarding) office@safeguardinginschools.co.uk if you are not on his mailing list).

The DSL already has heavy responsibilities so we noted his advice that you should identify a named senior leader with overarching responsibility for the quality and delivery of remote education, and that the DSL should liaise with that person.

We submit that is a sensible management approach towards the data protection angle as well.

3 Using Third Party Data Resources

The base expertise of Satswana is rooted in Technology and Cyber Security, which we have applied to data protection where we are meant to be pursuing a policy of "protection by design and default".

Thus from a technical perspective we are concerned when techniques are deployed which add considerable additional risk to your systems, specifically where a third party is granted access to your core data in order to transfer it to another processor to hold and provide additional services. We believe that alone at least trebles your risk.

We do understand that you are only doing so because of the lack of capability of your core software to provide the more sophisticated solutions that would be taken for granted in a current design, and seek to constantly

point out that you are not being well served by monopoly suppliers who do not invest in their product. That is an important future discussion, but our concern at the moment is more fundamental.

It is that an examination of their reported finances would suggest that some processors cannot be expected to have the resources to invest in a future, or even maintain their current product.

We are specifically concerned that Local Authorities are suggesting that a third party service can access your data and then provide it to food providers.

Clearly the need is acknowledged, and a solution is required in exceptional times, but we submit this is not the answer for three reasons. First you do not control what data they take, Secondly we suggest that there is risk in using the contractors involved, and thirdly because you have no control over the location of the data within the processors subsequently. All of this offends your responsibilities under the Data Protection Act 2018, and we very much regret the herd like recommendations from the Local Authorities that this risky means of resolving a requirement should be adopted.

As ever we can only advise, and alert you to what we regard as being a security liability, but if necessary it is our recommendation that you provide the information manually if necessary. We also suggest that the entire education community should demand investment in better products from their software providers so as to obviate these risks.

4 What do they know about you?

Have you any idea how much is already known about you? Do you think you have any secrets? And if not, what is the purpose of securing personal data?

We fear that the answer is that somewhere almost everything about you is stored, and there will be organisations that are tasked with assembling it all together in one place, subjecting it to considerable analysis and coming up with conclusions.

If these are respectable agencies, then perhaps that is alright – and in any event there is nothing we can do about it. HMRC are not going to delete your tax and pay records, neither would you probably want the NHS to lose your medical history! The credit reference agencies are more concerning, have you ever seen what they collect about you? Every single payment that you have ever made, to a credit card, on your mortgage, or for any other purpose will be religiously documented month by month, to the penny – with a note permanently recording if you are even a day late, and we have no choice, you cannot opt out of the banks recording this data if you want an account or a card.

The problem is that if the State has the data, then the criminals have it too. Not that they were ever intended to get access, nor perhaps do the data managers know that they have been penetrated, but they will have been. Only last month it was revealed that the Solarwinds software that was used for network protection by some of the most significant organisations in the world had actually been hacked to the point that it was the

protection software was being used to transport malware around the globe! From there sophisticated operators skilled in the dark arts helped themselves, often within a rogue State sponsored structure.

Against that background you may reasonably despair at the energy we are required to put into data protection, but we would make the point that if something is deeply flawed you have to start somewhere, at some point, to start to put it right. And that indeed starts with controlling the personal data that we record and distribute, especially within the wider world of social media.

Did you note the other day that a young lady lost her place at University because of an ill-considered word used in a Snapchat message five years earlier? The message was meant to disappear, but a "friend" saved it and waited all that time to damage her future. How she must wish that she had never posted the message, especially to a person who would do that. And what do we think of the University that exploited the information? Tricky one that, because it was clearly an inflammatory word that did not reflect well on her.

The message must be that there is a very good reason why all of us should take great care into the future, about what we say, do, or write, and where we store it – how long we keep it for – because you may never know when something will be used against you, perhaps by a convincing con trick. Like the unblinking CCTV cameras that follow us all around who know where you are, we also know everything about you, and it is not just GCHQ who are processing it.

5 The Solarwinds attack

Every now and then there is the sort of almost unbelievable data extraction exploit that makes us all stop and think, such as when confidential information from Panamanian lawyers suddenly exposed many of the wealthy. The penetration and use of the Solarwinds software is at that level. We reproduce below the Microsoft statement on the matter. It will be principally of interest to your IT teams, but from the practical layman angle you will note that nothing is sacred and risk is ever present to your data.

Microsoft is aware of a sophisticated attack that utilizes malicious SolarWinds software. On December 17, 2020, Brad Smith posted a blog sharing the most up to date information and detailed technical information for defenders.

As this is an ongoing investigation, Microsoft cybersecurity teams continue to act as first responders to these attacks. We know that customers and partners will have ongoing questions and Microsoft is committed to providing timely updates as new information becomes available. We will make updates through our Microsoft Security Response Center (MSRC) blog at https://aka.ms/solorigate.

There are a number of published resources to assist customers in securing their environments:

- We have published a blog outlining this dynamic threat landscape and the principles with which we are approaching the investigation.

- We have published an anchor blog with technical details of the attack. This blog will be updated with new information as the investigation continues. Customers should look to this blog as the one stop for updates on the sophisticated attack.
- Microsoft Defender antivirus and Microsoft Defender for Endpoint have released protections for the malicious SolarWinds software and other artifacts from the attack.
- Microsoft Azure Sentinel has released guidance to help Azure Sentinel customers hunt in their environments for related activity we have observed with this sophisticated attack.
- Microsoft 365 Defender and Microsoft Defender for Endpoint customers should review the Threat Analytics article within the Defender console (sign-in is required) for information about detection and potential impact to their environments.
- For any Microsoft Threat Experts (MTE) customers, where we have observed suspicious activity in the customers' environments, we have completed Targeted Account Notifications.
- If a customer has any product support related needs, please continue to direct them to Microsoft Support (CSS) who remain the primary place for all customer support needs.
- For Identity professionals and Microsoft 365 admin, we have published a blog with guidance on how to protect Microsoft 365 from on-premises attacks.

6 An update on Processing

We continue to try and engage with Processors in order to update our approved list and find we are getting active support on the one hand, and in other places our request is ignored, in the case of Class Dojo for instance. You are faced with many other challenges to support online learning, so now is not the time to seek change, but we must be quite clear that those processors in the United States who refuse to adopt one of the means by which they can become compliant will be a future data risk for you. As such it will become inevitable that you will have to select a conforming supplier at some time in the future.

The ICO do continuously provide support and guidance and their latest release can be found here

https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/data-sharing-and-children/

They advise that a UK version of GDPR should have been written into UK law by the end of 2020. We have not seen that yet, but it is our expectation that eventually we will settle down to there being "data equivalence" with the EU

7 DfE/NCSC advice and information on Ransomware

As I think you will recall we have frequently covered ransomware and generally the DfE/NCSC advice that we copy below is quite excellent, and we commend it to all those within schools who ask us for an update exercise to confirm they are compliant. This is a subject matter that will take many hours to ensure you are on top of things.

Before copying their content we would like to highlight two issues. Number one, unfortunately we find that there are three problems with their advice regarding backup. First most IT staff just back everything up, the opportunity to select is rarely possible, and if they did do that then they may leave out the wrong thing! Secondly no standard backups are held offline, you have to make a special effort to do that, which is why we recommend your taking a copy of the database once a month so you have something to restore to, because the backup itself will probably be corrupted. Finally – if one IT manager in a thousand has ever tested and restored from a backup, then we will eat our hat!! It is far too traumatic, and is only ever done in extremis.

The only certain protection is to copy your database to a disc that is removed entirely from the network. If you then get a ransom, then you lose all the data since the time that you made the copy, but you have something to restore to. It is also a good idea to choose a backup provider who has automatic file change detection software, because they will not backup an infected file.

Finally, you should never pay, you just lose your money as well as your data, do you think these thieves are gentlemen? No!!

This is the content of their letter:-

Why we are contacting you?

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyberattacks involving ransomware infection affecting the education sector at this time.

The purpose of this letter is to make you aware of the threat and provide high-level information and advice to support your ongoing cyber security preparedness and mitigation work. In all cases the NCSC has been working with the department and the affected providers to contain and support post-incident outcomes.

However, these attacks and incidents have had a significant impact on the affected education provider's ability to operate effectively and deliver services. These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Whilst I would urge you to ensure that your systems, processes and awareness training are up to date, I also want to make you aware of the steps you should take if your educational setting is affected. What should I do if I am affected? Please action the following:

1. Enact your incident management plan
2. Contact the NCSC, via https://report.ncsc.gov.uk
3. Contact your local law enforcement and Action Fraud,viahttps://www.actionfraud.police.uk/
4. Inform the Department for Education at this address:sector.securityenquiries@education.gov.uk What do I need to do now? It is vital that all education providers urgently review their existing defences and take the necessary steps to protect their networks from cyber-attacks. Along with your defences, having the ability to

restore the systems and recover data from backups is vital. You should ask your IT team or provider to confirm that:

- They are backing up the right data
- The backups are held offline
- They have tested that they can restore services and recover data from the backups

What do you need to do next?

The Department for Education would like to signpost guidance in developing defences as well as a number of free offers that the NCSC provide which can help notify you of possible malicious activity on your networks. These have been listed in the annex attached.

We will continue to monitor these situations and will revert with further information if there are further developments.

Yours sincerely, Department for Education

ANNEX A – Ransomware

What is ransomware?

Ransomware is a type of malicious software (malware) that prevents you from accessing your computer (or the data that is stored on it). The system itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017.

Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin) in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. For these reasons, it's essential that you always have a recent offline backup of your most important files and data.

How does it impact education providers? Ransomware is often used by criminals in a way that doesn't initially target specific organisations. Once the malicious software is on a network, the criminals can monitor and control the encryption of data. Their aim is to encrypt data that will have the most impact on the organisation's services. This can affect not just the organisation's computer networks but also services it operates, including telephony and websites.

The data held by these services is also at significant risk, including personal information (student and staff details), financial transactions (staff salaries, payment of ESFA funds, ability to pay suppliers), details on vulnerable people (adult social care), and college and school data (admissions, at risk children). Depending on

the comprehensiveness of disaster / business continuity plans in place, normal service can take weeks, if not months to resume. In some cases, data will never be recovered.

Some ransomware groups have started to steal data from their victim organisation's networks before encrypting what is left. This means that even if the victim can recover from backups the criminals may try to extort money in exchange for not revealing the data online.

Should we pay ransomware? The Department supports the National Crime Agency (NCA) recommendations. The NCA does not encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

ANNEX B

Being prepared Cover the basics

1. Have an incident plan and test it
2. Make sure your data is backed up offline and test the recovery of it
3. Regularly review your defences and controls

NCSC material and support

1. Ransomware advice and guidance for your IT teams to implement, available here:https://www.ncsc.gov.uk/guidance/mitigating-malware-andransomware-attacks 2. How to effectively detect, respond to and resolve cyber incidents, available here:https://www.ncsc.gov.uk/collection/incidentmanagement/cyber-incident-response-processes/developing-yourplan
3. Sign up to the Cyber Security Information Sharing Partnership (CiSP); a safe and secure environment that allows the NCSC to share threat information, available here: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
4. Enrol in the NCSC Early Warning service that helps the NCSC to rapidly notify organisations that might be affected by malicious software, available here: https://earlywarning.service.ncsc.gov.uk/
5. Test your incident response with an "Exercise in a Box", available here: https://www.ncsc.gov.uk/information/exercise-in-abox
6. Finally a data backup strategy and guidance is also available here: https://www.ncsc.gov.uk/collection/small-businessguide/backing-your-data

Further information

1. Back to school audit by NCSC and London Grid for Learning, available here: https://www.ncsc.gov.uk/blog-post/cyber-securitygoing-back-to-school
2. Questions for school governors by NCSC and DfE, available here: https://www.ncsc.gov.uk/information/school-governorquestions

3. NCSC practical tips for everyone working in education, available here: https://www.ncsc.gov.uk/information/resources-for-schools
4. NCSC cyber security risk management guidance, available here: https://www.ncsc.gov.uk/collection/risk-managementcollection

B Satswana guide to use of images in school

1 Introduction

Since technology is increasingly available that involves images of persons, the right to take, save or use an image becomes increasingly a matter of consent within a Data Protection environment. This paper seeks to revisit the related issues, review current practice, and recommend a future approach.

2 Basis of approach

The ICO is absolutely clear in its advice that "the DPA is unlikely to apply in many cases where photographs are taken in schools (and other educational institutions). Fear of breaching the provisions of the DPA should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure." Further that "photos taken purely for personal use are exempt from the DPA".

However, "photos taken for official school use may be covered by the DPA and pupils and students should be advised why they are being taken".

We seek the simplest possible approach to manage and control how that advice is provided.

3 The Admissions Document

This is the starting point for "consent", in that you have statutory data plus supplementary data that you seek a specific consent signature for, such as whether English is a first language, or not. The aim is to embrace every additional requirement into a single document requiring one signature.

Many schools have in the past asked parents to choose from multiple options based on various photographic scenarios. We now seek to dispose of that approach, not least because it is almost impossible to manage and communicate to all staff. In its place we propose a simple statement as follows below that refers to your images policy to be added to the admissions document.

"Where an image of a child is used the school follows the consent procedures outlined within our Images Policy. Where the Data Protection Act applies, specific consent will be sought for the use of any image."

Clearly we will now have to produce that policy, please find an initial production at Appendix A. This may of course be revised over time.

The background reasoning is that most photos will not require consent: where they do, then it must be specifically granted as an "opt in", we cannot deploy allowing them to opt out – that offends the Regulation.

We always seek to avoid any extra work of repeating consent requests. However if you hold multiple choice answers you may wish to replace that with this approach, in which case it should be sufficient to advise the change at an appropriate opportunity without requiring new signatures.

4 Subjects covered

We seek to address those areas where the school requires specific consent for the use of an image, specifically where it is required for a website, or to be published elsewhere, including in the Press.

Added to that will be the addition of clauses to cover the use of online video for educational purposes.

We will incorporate a section on CCTV, rather than publishing that separately. Of course those clauses can be excluded if you do not use any closed circuit TV.

Finally – at Appendix B – we insert a draft processor agreement that might be considered for use with a school photographer

Appendix A

Taking, Storing and Using Images of Children Policy

1. Policy Purpose and Scope

1.1. This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by the School, (referred to as "the School"). It also covers the School's approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, the media and other schools. Also the use of closed circuit television and Internet based remote education.

1.2. It applies in addition to the School's terms and conditions, and any other information the School may provide about a particular use of pupil images, including, for example, signage about the use of CCTV; and more general information about use of pupils' personal data.

1.3. Parents who accept a place for their child at the School are invited to agree to the School using images of them as set out in this policy by signing the consent requested within the Admissions document. Where the person is over 13 we will seek separate consent. We expect parents and pupils to feel able to support the School in using pupil images to celebrate the achievements of pupils, promote the work of the School, and for important administrative purposes such as identification and security.

If consent is not given, the school may make reasonable adjustments to protect your child for safeguarding and or data protection purposes. This may limit their exposure during school events where photography is likely to take place.

The reasonable adjustment could be the child wearing a mask and or clothing, so they could not be identified as a data subject, however allowing for inclusion. It could also mean that the child could not play a prominent part in the show in order to ensure protection for safeguarding and or data protection.

1.4. Any parent or pupil who wishes to limit the use of images of a pupil for whom they are responsible should contact the School in writing. The School will always respect the wishes of parents/carers/pupils where reasonably possible, and in accordance with this policy.

1.5. Certain uses of images are necessary for the ordinary running of the School and its community. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objection raised.

2. Use of Pupil Images in School Publications

2.1. The School will seek specific consent to use images of selected pupils to keep the School community updated on the activities of the School, and for marketing and promotional purposes, including:

a) on internal displays (including clips of moving images) on digital and conventional notice boards within the School premises;
b) in communications with the School community (parents, pupils, staff, governors and alumni) including by email, on the School intranet and by post;
c) on the School's website and, where appropriate, via the School's social media channels, e.g.Twitter and Facebook. Such images would not normally be accompanied by the pupil's full name; and
d) in the School's prospectus, and in online, press and other external advertisements for the School. Such external advertising would not normally include pupil's names, except where express permission has been sought.

2.2. The source of these images is predominantly the School's professional photographer for marketing and promotional purposes, or staff/pupils in relation to school events, sports or trips. the School will only use images of pupils in suitable dress.

3. Use of Pupil Images for Identification and Security

3.1. All pupils are photographed on entering the School and thereafter at various intervals, for the purposes of internal identification. These photographs identify the pupil by name, year group, house and form/tutor group.

3.2. CCTV is in use on School premises, and will sometimes capture images of pupils. Images captured on the School's CCTV system are used in accordance with the Data Protection Act 2018, the School's Data Protection Policy, and any other information or policies concerning CCTV which may be published by the School from time to time.

4. Use of Pupil Images in the Media

4.1. When we are aware that pupil images are likely to be used in the media we make best efforts to ensure that pupils and parents are informed that this is the case.

5. Policy regarding CCTV use

5.1 The School uses Close Circuit Television ("CCTV") within the premises. This policy applies to all data subjects whose image may be captured by the CCTV system. It works in concurrence with the School's Data Protection Policy, Record of Data Processing and Data Retention schedule.

The policy considers applicable legislation and guidance, including but not limited to;

- Data Protection Act (DPA) 2018
- CCTV Code of practice as produced by the Information Commissioner Office (ICO)
- Human Rights Act 1998.

5.2 Management

The CCTV system is owned and operated by the School and the deployment is determined by the Senior Leadership Team, with consultation from the Board of Governors and Data Protection Officer (DPO).

The School will:

- Notify the ICO of its use of CCTV as part of its registration.
- Complete a Data Privacy Impact Assessment if amendments are to be made to the deployment or use of CCTV.
- Treat the system and all information processed on the CCTV system as data which is processed under DPA 2018.
- Not direct cameras outside of school grounds onto private property, an individual, their property or a specific group of individuals. The exception to this would be if authorisation was obtained for Direct Surveillance as set up by the Regulatory of Investigatory Power Act 2000.
- Display Warning signs will be positioned clearly in prominent places.

  Specifically, at all external entrances of the school site where CCTV is used and covers external areas. These signs will include information on how to contact the school regarding information or access to the CCTV footage.
- There is no guarantee that this system will or can cover and detect every single incident taking place in the areas of coverage.
- CCTV footage will not be used for any commercial purposes.

5.3 Camera Setup

The CCTV system is comprised of a number of cameras which record day and night covering the Internal and external areas of the School. Their coverage may also extend past the school boundaries to public areas. Cameras will be placed so they only capture images relevant for the purposes for which they are installed, and all care will be taken to ensure that reasonable privacy expectations are not violated.

(CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances. * if applicable)

Members of staff on request can access details of CCTV camera locations.

5.4 Purpose of CCTV

The School uses CCTV for the following purposes:

- To provide a safe and secure environment for the workforce and visitors.
- To protect the school reputation, buildings and assets.
- To assist in the prevention and detection of criminal activity.
- Assist law enforcement agencies in apprehending suspected offenders.

5.6 Covert Monitoring

The school retains the right in exceptional circumstances to set up covert monitoring. For example;

- Where there is good course to suspect illegal or serious unauthorised action(s) are taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances' authorisation must be obtained from the Head Teacher or Chair of Governors.

Covert monitoring will cease following the completion of an investigation.

5.7 Storage and Retention

Recorded data will not be retained for longer than is necessary, while retained the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of people whose images have been recorded. All Data will be stored securely;

5.8 Access to CCTV Images

The ability to view live and historical CCTV footage is only to be provided at designated locations and by authorised persons.

5.9 Disclosure of Images to Data Subjects (Subject Access Requests)

Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.

These requests will be considered a Subject Access Request and should follow the schools Subject Access Request process.

When such a request is made, the footage will be reviewed in accordance with the request.

If the footage contains only the data subject making the request, then the individual may be permitted to view an extracted recording of the footage.

This will be strictly limited to the footage of the data subject making the request and the specific reason for the request.

If the footage contains images of other data subjects, then the school will consider if;

- The request requires the disclosure of the images of data subjects other than the requester, and if these additional data subjects can be anonymised from the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.
- If not, then either it is reasonable in the circumstances to disclose those images to the data subject making the request.

The School reserves the right to refuse access to the CCTV footage where this would prejudice the legal rights of other data subjects or jeopardise an ongoing investigation.

5.10 Disclosure of Images to Third Parties

The School will only disclose recorded CCTV footage to third parties where there is a lawful basis to do so.

Third parties acting on behalf of a data subject will be handled in accordance with the Subject Access Request Policy.

CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place.

If a request is received from a law enforcement agency for the disclosure of footage then the school will follow the Subject Access Request process, obtaining the reasoning for wanting to obtain the footage and any data subjects of concern.

This will help to enable proper consideration of the extent that can be disclosed. This information will be treated with the upmost confidentiality.

If an order is granted by a court for the disclosure of CCTV images then this should be complied with. However, consideration must be given to exactly what the court requires.

In all instances, if there are any concerns as to what should or should not be disclosed then the DPO will be contacted and further legal advice sought as per requirements.

6. Security of Pupil Images

6.1. Professional photographers and the media are expected to be accompanied at all times by a member of staff when on the School premises.

6.2. The School takes appropriate technical and organisational security measures to ensure that images of pupils held by the School are kept securely, and protected from loss or misuse, and in particular will take reasonable steps to ensure that members of staff only have access to images of pupils held by the School where it is necessary for them to do so.

6.3. All staff receive guidance on the importance of ensuring that images of pupils are made and used responsibly, only for School purposes, and in accordance with the School's policies and the law.

7. Use of Cameras and Filming Equipment (including mobile phones) by Parents

7.1. Parents are welcome to take photographs of (and where appropriate, film) their own children taking part in School events, subject to the following guidelines, which the School expects all parents to follow:

a) Parents are reminded that it may occasionally be necessary for the School not to permit the use of cameras or filming equipment at specific events or productions.
b) When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others.
c) In particular, flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events.
d) Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
e) Parents are reminded that such images are for personal use only. Images which may identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
f) Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts.
g) Parents may not film or take photographs in swimming pool areas, changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.

7.2. The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

7.3. The School sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case copies of the DVDs and CDs may be made available to parents for purchase. The specific consent of Parents or pupils taking part in such plays and concerts will be sought if it is intended to make such recordings available more widely.

8. Use of Cameras and Filming Equipment (including mobile phones) by Pupils

8.1. All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff.

8.2. The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas or swimming pool areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

8.3. The misuse of cameras or filming equipment in a way that breaches this Policy, or the School's Anti-Bullying Policy, Data Protection Policies, ICT Policies, or the School Rules is always taken seriously, and may be the subject of disciplinary procedures.

9.0 Conditions applying to online learning

As part of our approach to remote learning we use video platforms for interactive sessions. These conditions should be read alongside our Social Media Policy and our acceptable use policy. In order to create a safe environment for pupils and staff when taking part in an interactive session, the following considerations must be observed:

- By accepting the meeting ID and joining the meeting, with parental responsibility, you agree to the terms set out in this policy
- It is only to be accessed by a device in a communal family space
- The session will be supervised at all times by an adult to deal with any technical or safeguarding difficulties or issues
- Attendees should be dressed appropriately

- The meeting ID is to remain confidential and not to be shared to anyone that it was not designated to

- Recording, photos or screenshots of the meeting are not allowed by anyone taking part unless consent has been obtained. Recordings remains the copyright of the School and nothing should be shared with social media

- For participants some facilities will be disabled by the host teacher. This includes but is not limited to the screen record function, chat and screen share

- The same behaviour expectations that are set within a classroom apply to the interactive meeting and the teacher retains the right to terminate a pupil's participation

10.0 To make a complaint

Please contact our Data Protection Officer Satswana Ltd, with email of info@satswana.com ; telephone number 01252 516898, office address Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix B

Data Processor Agreement for School photographers

This agreement forms a contract detailing your instruction, and therefore the consent, for The Photographer to process data that you provide as specified below.

1. Introduction and Subject Matter

1.1 This agreement re processing of personal data (the "Data Processor Agreement") regulates the processing of personal data on behalf of the School (the "Data Controller"). This is on the basis that the parties have agreed for the Data Processor's delivery of student photographic services (the "Main Services"} with the use of student names data (the "Personal Data"} provided by the Data Controller.

1.1.1 Student Portrait Photographs is one of the Main Services provided. The Personal Data required to complete this service is only needed when the Data Controller requests a data match image CD to update the School database records. This isn't a requisite of the service as there is the option of completing these photographs without the transfer of Personal Data; this will however result in not being able to provide the school with a data matched image CD, the image CD that can be presented will only have the student image without any corresponding student information.

1.1.2 Group Photographs is another of the Main Services provided. The Personal Data required to complete this service is only needed when the Data Controller requests that all people present in the photograph have their names printed underneath the photograph. This isn't a requisite of the service as there is the option of completing these photographs without the transfer of Personal Data; this will however result in not being able to provide the school with a group photograph with names, the photograph can be produced with a title of the group underneath instead.

2. **Applicable Law and Supervisory Authorities**

2.1 The Data Processor Agreement shall ensure that the Data Processor complies with the applicable data protection and privacy legislation
{the "Applicable Law"), and any relevant supervisory authorities including in particular:

i. The General Data Protection Regulation, 25 May 2018 ("GDPR"}.

ii. The Copyright, Designs and Patents Act 1988.

iii. Co-operate with supervisory authorities such as the Information Commissioners Office ("ICO").

3. Processing of Personal Data

3.1 In connection with the Data Processor's delivery of the Main Services to the Data Controller, the Data Processor will process certain categories and types of the Data Controller's Personal Data on behalf of the Data Controller.

3.2 "Personal data" includes "any information relating to an identified or identifiable natural person" as defined in GDPR, article 4 (1) (1) (the "Personal Data"}. The categories and types of Personal Data processed by the Data Processor on behalf of the Data Controller are:

i. Student and/or staff name

ii. Student form/class.

iii. Student admission number.

3.3 The Data Processor only performs processing activities that are necessary and relevant to perform the Main Services. The parties shall update the above list whenever changes occur that necessitates an update.

3.4 The Data Processor shall have and maintain a register of processing activities in accordance with GDPR, article 30 (2).

3.5 The Data Processor processes personal data provided by the Data Controller to enable the Data Processor to produce the photographic product requested by the Data Controller, to administer orders and deliver photographs. The Personal Data is not comprised by this Data Processor Agreement, because the Data Processor is data controller for said personal data, and reference is made to the Data Processor's data protection and privacy policy available on the Data Processor's website.

4. The Data Controller's Obligations and Rights

4.1 The Data Processor may only act and process the Personal Data further to documented instruction from the Data Controller {the "Instruction"). The Instruction is at the time of entering into this Data Processor Agreement and is continued on each and every occasion that the Data Controller provides the Personal Data, this is on the basis that the Data Processor will only process the Personal Data with the purpose of delivering the Main Services.

4.2 The Data Controller guarantees that the Personal Data transferred to the Data Processor is processed by the Data Controller in accordance with the Applicable Law, including the legislative requirements re lawfulness of processing.

4.3 The Data Processor shall give notice without undue delay if the Data Processor considers that Instruction to be in conflict with the Applicable Law.

5. The Data Processor's Obligations

5.1 Confidentiality

The Data Processor shall treat all the Personal Data as strictly confidential information. The Personal Data will be processed in accordance with the Main Services as agreed by the Data Controller. However, the Personal Data may not be copied or transferred in conflict with the Instruction, unless the Data Controller in writing has agreed hereto.

5.1.1 The Data Processor's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this Data Processor Agreement with strict confidentiality and in accordance with our General Data Protection Regulation Policy.

5.2 Security

5.2.1 The Data Processor shall implement the appropriate technical and organizational measures as set out in this Agreement and in the Applicable Law, including in accordance with GDPR, article 32.

5.3 The Data Processor shall ensure that access to the Personal Data is restricted to only the employees to whom it is necessary and relevant to process the Personal Data in order

for the Data Processor to perform the Main Services and obligations specified under this Data Processor Agreement.

5.4 The Data Processor shall also ensure that the Data Processor's employees working on processing the Personal Data and that they only process the Personal Data in accordance with the Instruction to provide the Main Services.

5.4.1 The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing.

5.5 Data protection impact assessments and prior consultation

5.5.1 If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

5.6 Rights of the data subjects

5.6.1 If the Data Controller receives a request from a data subject for the exercise of the data subject's rights· under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation. The Data Processor shall be given reasonable time to assist the Data Controller with such requests in accordance with the Applicable Law.

5.6.2 If the Data Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and such request is related to the Personal Data of the Data Controller, the Data Processor will immediately inform the Data Controller of this request.

5.7 Personal Data Breaches

5.7.1 The Data Processor shall give immediate notice to the Data Controller if a breach of the data security occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed re the Personal Data processed on behalf of the Data Controller (a "Personal Data Breach").

5.7.2 The Data Processor shall have and maintain a register of all Personal Data Breaches. The register shall at a minimum include the following:

i. A description of the nature of the Personal Data Breach, including, if possible, the categories and the approximate number of affected Data Subjects and the categories and the approximate number of affected registrations of personal data.

ii. A description of the likely as well as actually occurred consequences of the Personal Data Breach.

iii. A description of the measures that the Data Processor has taken or proposes to take to address the Personal Data Breach, including, where appropriate, measures taken to mitigate its adverse effects.

5.7.3 The register of any relevant Personal Data Breaches shall be provided to the Data Controller in copy if so requested in writing by the Data Controller or the relevant Data Protection Agency.

5.8 Documentation of compliance

5.8.1 The Data Processor shall after the Data Controller's written request hereof provide documentation substantiating that:

i. the Data Processor complies with its obligations under this Data Processor Agreement and the Instruction; and

ii. the Data Processor complies with the Applicable Law in respect of the processing of the Data Controller's Personal Data.

5.8.2 The Data Processor's documentation of compliance shall be provided within 28 days.

5.8.3 The Personal Data is only processed by the Data Processor at the Data Processor's address. The Data Processor does not transfer the Personal Data to other countries or international organisations.

6. Sub-Processors

6.1 The Data Processor does not engage third-parties to process the Personal Data ("Sub-Processors"). Therefore a sub-processor will not be used without obtaining written, specific authorization from the Data Controller.

7. Duration

7.1 The Data Processor Agreement shall remain in force with the Data Controller until the Data Controller no longer chooses to use the Main Services of the Data Processor.

7.2 All Personal Data provided by the Data Controller will be retained for a minimum period of 2 months and for a maximum period of 6 months following the Personal Data received date, this is to ensure that we can complete the duties required for the Main Services provided. After this date the data received is permanently deleted.

8. Termination of Main Services

8.1 The Data Processor's authorisation to process Personal Data on behalf of the Data Controller shall be annulled at the termination of the Main Services and therefore this Data Processor Agreement.

8.2 The Data Processor shall continue to process the Personal Data for up to three months after the termination of the Data Processor Agreement to the extent it is necessary and required under the Applicable Law. In the same period, the Data Processor is entitled to include the Personal Data in the Data Processor's backup. The Data Processor's processing of the Data Controller's Personal Data in the three months after the termination of the Main Services and therefore this Data Processor Agreement shall

be considered as being in accordance with the Instruction.

8.3 At the termination of the Main Services and therefore this Data Processor Agreement, the Data Processor shall return the Personal Data processed under this Data Processor Agreement to the Data Controller, provided that the Data Controller is not already in possession of the Personal Data. The Data Processor is hereafter obliged to delete all the Personal Data and provide documentation for such deletion to the Data Controller.

Your Name (required)

Your Email Address (required)

- ☐ I agree and instruct the school to process data as laid out in this data processor agreement.
- ☐ I confirm that I am in a position of authority to consent to this agreement.

C 1 Welcome to Satswana

A warm welcome to Satswana, thank you for appointing us to be your Data Protection Officer, in this role we become a peripatetic member of your staff and as such hope you will feel confident to call or mail us at any time for advice.

We seek to offer a very personal service, and absolutely love receiving questions, not least because we always learn as a consequence, firstly what your needs are, and secondly by finding the answer to your question if we do not know it already.

2 The legal bit

Please note that there are certain places that you must publish who your DPO is, on your website Privacy Policy for example. For those purposes the DPO should be Satswana Ltd please, with email of info@satswana.com; telephone number 01252 516898, if you need an office address as well it is Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH. It is likely that you will meet us personally, and we will be very pleased to deal on a personal basis, but we avoid a "named person" for registration purposes in case one of us falls ill.

3 What happens next?

a) We would like to get to know you, either through a virtual, or if possible a personal meeting. If that could be as a part of an existing SLT meeting, then we will try to take as little as possible of your time
b) The next step is to ensure that we conduct an "Impact Assessment" which would involve the significant office holders within the School, starting with the Principal and Deputy Heads, plus the standing members of SLT, and then possibly other staff such as IT relationships, admissions, SEN, estates management etc. who may not necessarily be members of SLT. It tends to become very much a discussion – with a report detailing the "impacts" at the end of it.
c) Normally you will then request documentation from us according to your speciality interest, and we will expect to be able to give you comprehensive guidance on matters such as Retention and approved Processor contracts – for instance. Naturally it will also encompass a review of Policies and the provision of anything considered to be missing.
d) Thereafter we are not only on call for any matter involving the Data Protection Act, such as an Access Request, but we will also be publishing regular updates on matters arising within the Regulations, compliance or security generally. Those in turn might trigger further engagement. (Updates in the first instance will go to our initial contact. If further copies are required, please advise admin@satswana.com to add an email to their list.)

e) We are always happy to be invited to assist with training, and indeed ensure that Teachers are confident regarding GDPR and DPA by addressing inset days, there is never any extra charge for that.
f) We look forward to serving you. Please note we also welcome engagement with any Governors that are now tasked with the Cyber Security brief.

D Advance briefing for Schools prior to a formal impact assessment

Principals and executive staff are requested to read these notes prior to a meeting since we hope to make the actual meeting interesting and engaging with a high level of interaction and involvement. You may also wish to invite Governors or Trustees to consider them.

1 Can Data Protection be interesting?

It may seem a bizarre proposition that the compliance requirements of what started within Europe as the General Data Protection Regulation might be interesting, but we do hope to persuade you that it is extremely relevant and that there is both an underlying personal and intellectual component, as well as your professional discipline.

a) Taking the personal first, the fundamental change from DPA 1998 to what is now within English Law as DPA 2018 is that the individual "owns" their data and any controller or processor must seek your specific consent for any specific purpose. Add to that a new right "to be forgotten", and personal compensation for any errors and I hope you will see that the law change is of great benefit to you as a person.
b) The more global issue is where society is going with the generation of profit from data harvesting, something that remains unconstrained and fiercely protected by the United States constitution. GDPR was the European legislators attempt to restore rights to the consumer, and as far as it applies to data communications with Europe or affecting European citizens, they are able to impose their will. They seem to have "hit the spot" because almost universally the (actually brilliantly drafted) rules have become an accepted basis internationally, except for the US.

With those preliminary thoughts we hope you will have a positive and approving view of the subject as an individual. What we must then go on to consider is how the procedures of a School have to change now that you are responsible for the care and protection of other people's data, rather than what you used to be allowed to regard as "your" information.

DPA 2018 embraced GDPR in full with just two changes, one being the removal of the right to see references from Subject Access Requests, the other a reduction from 16 to 13 as the age when a person has full control over their data. Both may come up as subjects for discussion!

2 Where the buck stops

The Regulation requires that the most senior level of any organisation takes ultimate responsibility for data protection, so we intend no impertinence if we say that Principals, Trust CEO's and indeed the Chairman of any Board, Trust or Governing body must ensure that they are directly involved – especially with the impact assessment discussions.

Whilst you have a statutory requirement to appoint a Data Protection Officer, or employ a fractional service whereby an organisation works as a peripatetic member of your staff (which is Satswana's role), that person has no liability – strange as that might seem. The direction, decisions and leadership are all expected to be set from the very top and we will refer back to this point later on.

You may recall that under DPA 1998 it was frequently the Principal who was registered as the DPO, something the "conflict of interest" provisions made impossible. Subsequently an august body known as the Article 29 working party recognised that there was scope for the appointment within an organisation for somebody who had corporate responsibility and the role of Data Protection Manager was invented, and that person can be the day to day lead, working with the DPO where the regulations specifically require their involvement. (This is a detail that we can bring up if you wish!)

3 The SLT briefing

The following notes are essentially the agenda for the SLT briefing that may well come up again in discussion, but in kindly reading them in advance we can be sure that the syllabus has been covered. We said we would refer back to the direction from the top and would wish to explain that it is our experience that a discussion following the absorption of the topics can be very illuminating (especially to a Principal) as issues that affect other sectors emerge in a manner perhaps not made possible before. It is our hope that you will find that engagement far more worthwhile than our tediously taking time going through these subjects.

a) No fear

The very first point that we would like to make as one of our mantra's is that schools are simply not the target of the Regulator and it would take an extreme situation for there to be any consideration of a fine, or worse, for a breach. Indeed the education sector has always been most diligent in the application of any compliance requirement, and you all had a firm foundation in DPA 1998. We disown any organisation that uses fear within their advertising or copy to seek to promote their product or service.

b) Return on investment

Over time we expect the requirements of "privacy by design and default" will lead us all on a management journey towards greater efficiency and the adoption of new operating methods. This is a major topic for discussion that can be developed internally.

c) Breaches

The ICO recognises that these will happen, there is a criminal community making fortunes from exploits, and you will be a target. When they happen (not if, please note) it is our task to support you, so tell us as soon as possible and we will work the consequences out together. In many cases it will involve “no further action”.

d) Subject Access Requests

If you get one of these (and you will, it is now considered a new “right”) please immediately involve us - as we can help to limit the impact in many instances. Applicants are always well briefed on their rights, but are less aware of the rights that you have; and case law (especially the University of Worcester precedent) is continuously balancing what must be revealed. The same applies to Freedom of Information requests.

e) Processor agreements

As the controller of data a processor must do precisely what you tell them or allow them to do, all with the consent of the data owner. Satswana will provide you with an analysis of those in the market to save you doing so, and we would ask you to let us know of any not on the list so that they can be analysed and added.

f) Retention policy

“The data you do not keep is the safest”, but where do you draw the line? IRMS 2019 published a recommendation for schools that we can provide you with, and we have a precis form. The huge challenge of data deletion, especially digital data, is to actually do it, and that will be a subject that we will all continuously return to.

g) Policies

The most critical is the School Privacy Policy, but there are far too many others that you are required by one form of legislation or another to keep, together with issues such as what you publish. Generally speaking we can provide you with templates, and if we do not have one, then we will recognise the need from your advice and produce a solution.

h) Encryption

If there is one single point that you take away from this briefing, please make it this one. If your data is obfuscated by encryption then even if you are hacked it cannot be read, and indeed we do not have to then report an exploit to the ICO. It is an absolute essential on phones, tablets and (our pet hate) USB sticks. What emails do you encrypt?

i) Myths

As with “no fear” we have two more mantra’s to offer and rejecting myths is one of them. It normally starts with somebody telling you that you “should” - followed by perhaps ‘not take school books home to mark’. We say that the only word that matters is “must” where a statutory requirement means that it is the law. If you choose to consider something to be best practice, then see the next point, but please challenge “myths”!

j) You are the Boss

We wish to constantly emphasise this mantra, because you have to run and manage your affairs, and to do so you have to take decisions, which are always likely to be on the basis of your own risk assessment. There may be times when you decide to do something that might appear to be contrary to GDPR, indeed there are specific exemptions within “Keeping Children Safe in Education”, and sometimes that decision can be challenged or rebound. Be assured that if you have sound reasons, then you will be supported.

4 Summary

Do you notice that, except for mentioning encryption and data deletion we have hardly touched on any IT issue? That is not to say that will not become a material part of our discussion, it almost certainly will, but the consequences of the changes in data protection are almost entirely of a managerial nature, which stresses again why the most senior management of any organisation has to be intimately involved.
Does this agenda cover the subject? No, it is just the entry point for the journey.
We hope to enjoy a wide ranging debate with you and, having covered the basics, look forward to your active involvement and challenge

E Satswana Update March 2021

Contents

1.0 Revision to Guidance Manual

We are pleased to advise that we have updated the guidance manual to version 4.0 on our website, please find it here
https://www.satswana.com/resource/SatswanaGuidanceManualVer4.pdf

We hope that you will find it useful, especially for new customers, but equally a scan through might equally assist established customers as a form of check list. We have specifically added the initial briefing notes that appeared in the Final 2020 Update as Appendix A, so you will find a great deal of "intellectual property" on Data Protection contained in its pages, and we hope you will find that it is now up to date.

During the review we were reminded of a number of issues that had slipped down the priority order, so found it a worthwhile exercise ourselves!

2.0 Children's Code

One day we will try and count up how many statutory responsibilities you are expected to fulfil, with a great many others affecting your control of data other than the Data Protection Act itself.

The latest is the "Age Appropriate Design Code" being its formal title, but it seems to be universally referred to as the Children's Code, you can find the ICO information on it here https://ico.org.uk/for-organisations/childrens-code-hub/. Organisations will be expected to conform to the code by 2nd September 2021.

The ICO states that the code aims to ensure that children have a baseline of protection automatically by design and default, so that they are protected within the digital world rather than being protected from it.

Put simply they say that children are treated differently in the real world; this code ensures they are treated differently in the digital world too.

It probably affects the providers of websites and app services most, with the first point being that privacy settings should be set "high" by default and geo-location services that can reveal the child's location should be switched off. Organisations providing services are not allowed to use "nudge" techniques and notifications to encourage children to give up more personal data.

Expect this to be an issue running up to the September date.

3.0 Ransomware report

We were very pleased to receive a very positive report from the School that suffered the ransomware attack and found that they were nearly fully functional within 48 hours. May we stress again that this was a really well managed school with significant resources, so it really can happen to anybody.

The remedial IT specialist established that entry was achieved via a remote session, which of course you have all been particularly exposed to over the lockdown period as more and more people worked from home.

The virus was identified as being “antirecuvaanddb.exe”, which turned out to be less serious than might have been the case, in that it did not extract any data, which of course made it easier to handle as far as the ICO report was concerned – and it resulted in the biggest arising lesson from the incident.

Originally Satswana advised that the school should be proactive in publicising the attack in order to control the news, as we saw it. The management demurred, preferring to confirm the extent of the problem and we now recognise that they were quite right to do so. We followed up the initial report to the ICO with that qualification.

Furthermore it was found that a backup that had been written to tape had been completed before the infection came through, once again suggesting that this was a relatively unsophisticated attack. We must confirm that we have heard of other examples where all data has been copied, and the attackers have waited until all backups are likely to be infected before declaring their hand.

In this instance hats off to both an IT and administration team who did a great job in trying circumstances having cleansed all servers and restored the data prior to final testing, a task that nobody welcomes. In the meantime staff had access to their Chromebooks and the Internet, meaning that there was no impact on Teaching and Learning, so something that could have been very nasty was coped with brilliantly.

However, we can never relax.

4.0 Phishing Email Incident

There was similar good fortune to report as a consequence of a phishing attack where mails were sent out from a spoofed email account to the contacts list from an Outlook account, we feared the worst.

The computer concerned was thoroughly checked for any form of malware and nothing was found, which removed our worst fears that the attack had managed to leave resident code on the machine to carry out other attacks.

Thus as far as we could see the phishing was only in place to gather login credentials and continue the process, rather than to cause any lasting issues.

The school learned that with their emails on Office 365 there is built in malware, phishing and spam prevention; however things will eventually slip through, as this incident shows. They are looking at whether these filters need to be adjusted in the light of this.

They have concluded that the best protection against these issues in the future is vigilance and over cautiousness.

Before we knew the extent of the issue we reported the incident to the ICO within the initial 72 hour period, and followed that up with a further report once we knew that no data had been compromised. We subsequently received notification that the ICO did not intend to take any action.

5.0 Most likely forms of attack

The document we reproduce below was originally written as a marketing document aimed exclusively at private schools. Since the content is relevant to ALL schools, we have edited it accordingly! It is good information, and your IT may wish to consider whether the identified risks apply to your structure. Similarly the recommendation to plan a response is one we would always support.

What are the most likely forms of attack schools should protect against?

Attacks on schools are frequently motivated by financial gain, and are commonly conducted through:

- Committing invoice fraud against the school and the parents
- Selling personal data to other criminal groups
- Demanding ransom payments in return for unlocking the school's encrypted files and promising not to release stolen data

Schools are seeing an increase in phishing, vishing, and smishing attacks (which use bogus emails, telephone calls, or text messages purporting to be from a trusted entity, tricking recipients into sharing confidential or sensitive information).

Findings from research undertaken in June 2020, by Crowe, KYND and University of Portsmouth illustrate the following to be the most commonly observed risks to schools in the UK:

- **Ransomware risk – 34%** of schools had at least one external service exposed, which would place them at a higher risk of a ransomware attack.
- **Email spoofing – 98.5%** of schools analysed are exposed to having their email addresses spoofed and used to send spam, phishing, or otherwise fraudulent emails (either internally or externally).
- **Vulnerable services – 59.6%** of schools were running at least one service with a well-known vulnerability – putting them at high risk of attack from cybercriminals who specifically target services with known vulnerabilities.

- **Out-of-date services – 13.6%** of schools had at least one internet service that was using software which was out of date and no longer supported by its developer, putting them at higher risk of cyberattack and service failure.
- **Certificate issues – 32.3%** of schools had at least one security certificate which had expired, been revoked or distrusted, representing a significant threat to brand reputation.
- **Domain registration risks – 33%** of schools had at least one domain registered to a personal or individual email address, representing a significant threat to the continuity of a school's operation and domain ownership.

Developing clear and concise incident response plans will help schools to take a proactive stance enabling them to manage impact when cyberattacks occur. By utilising cybersecurity solutions which protect students and teachers from ransomware, trojans, and other active malware, plus off-network backups and multi-factor authentication, schools can better protect themselves against cyberattacks. Adopting written resilience plans at board level will help ensure support for the necessary resources to combat cybercrime.

6.0 ICO decision on images

There are times when we must report matters that we might like to comment on, but we are governed by the decisions of the Regulator and, as with a referee, they cannot be argued with, though we were pleased as ever to receive the following question.

"In this incident, parents of a primary child had stated on the consent form used by the school that images taken were not to be used 'outside of school'. When a class photograph was taken, a proof was sent home to all parents for them to preview. The parents considered that this picture was sent 'outside the school'. The ICO said that the school had failed to implement an appropriate procedure for the handling of pupils' images."

The school further commented "It is customary for proofs to be sent home for viewing before purchase. However, more often it is via the photo studio's website. I thought I would ask your opinion as this surprised me."

It surprised us too, so we commented that there were two arising issues. The first of course is that there is no realistic appeal to the decision of a Regulator, it takes a brave person to say "you are wrong", and that probably would mark your card forever going forwards! The second is that any decision they make becomes a precedent, and thus a facet of case law – it effectively becomes a regulation, so we are going to have to adapt our behaviour.

(A third point is that there appears to be no limit to how mean and petty some parents can be in criticising schools, but once again we are dealing with almost unassailable "rights".)

It was as a consequence of this query that we reviewed the Images Policy that formed the content of our February update.

Appendix A

Online learning advice from Zoom

We felt this was a useful contribution and have produced a precis of the main points that is perhaps a bit more punchy than the elaboration – but you can decide that for yourself by finding the full article here

Tips for Parents to Support Learning from Home - Zoom Blog

This is our precis of the major headings

It's important for parents and caregivers to understand: Learning to learn online is a *big* task, and you should give yourself some leeway as you adjust. Things may get off schedule. Some strategies may not work. That's normal as you get used to a new skill.

In face-to-face learning, going to a physical school building helps children transition into learning mode. The school environment provides a physical reminder of the behaviours and norms that are important for effective learning. When learning online, it's important to create a learning station that helps students transition from "home mode" to "school mode."

When it comes to the technology itself, whether it's school-issued or a parent's or child's device, having it ready and using it effectively will go a long way toward ensuring a successful online learning experience.

After you've created an effective learning environment, it's important for students to understand what their learning journey will look like. An easy-to-read schedule can help, particularly if students have hybrid schedules or A/B days where the schedule changes each day. Be sure to involve children in creating the schedule, and make sure it's realistic for your family and includes a mixture of learning time and unstructured time.

When school and family time are both happening online, the traditional approach to screen time may not be the best way to teach boundaries. Rather than focusing on how many minutes a child spends on the screen, instead make sure they're learning to have a healthy balance among a variety of online and offline activities.

While children have to transition from "home mode" to "school mode," parents and caregivers need to transition from "parent mode" to "learning coach mode." This means helping your child develop good learning habits and helping remove any barriers to effective learning. It *doesn't* mean solving all their problems or doing their work for them.

F Exchange Server Patch Alert received from Microsoft

We are contacting you to alert you to Microsoft's release of patches for multiple different on-premises Microsoft Exchange Server zero-day vulnerabilities that are being exploited by a nation-state affiliated group.

The vulnerabilities exist in on-premises Exchange Servers 2010, 2013, 2016, and 2019. Exchange Online is not affected. We wanted to ensure you were aware of the situation and would ask that you help drive immediate remediation steps.

Specifically, to minimize or avoid impacts of this situation, **Microsoft highly recommends that you take immediate action to apply the patches for any on-premises Exchange deployments** you have or are managing for a customer or advise your customer of the steps they need to take. The first priority being servers which are accessible from the Internet (e.g., servers publishing Outlook on the web/OWA and ECP).

To patch these vulnerabilities, you should move to the latest Exchange Cumulative Updates and then install the relevant security updates on each Exchange Server.

- You can use the Exchange Server Health Checker script, which can be downloaded from GitHub (use the latest release).
- Running this script will tell you if you are behind on your on-premises Exchange Server updates (note that the script does not support Exchange Server 2010).
- We also recommend that your security team assess whether or not the vulnerabilities were being exploited by using the Indicators of Compromise we shared here.

We are committed to working with you through this issue. For additional help, please open a ticket with our Partner Center or contact the help desk.

Resources and information about this issue for partners

- Microsoft On the Issues blog
- Microsoft Security Response Center (MSRC) release - Multiple Security Updates Released for Exchange Server
- Exchange Team Blog
- MSTIC Blog
- MSRC Blog

- Microsoft On the Issues Blog
- Out of Band Exchange Release Customer Alert
- Security Update Guide

Exchange patch information

- March 2, 2021 Security Update Release - Release Notes - Security Update Guide - Microsoft
- CVE-2021-26855 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-26857 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-26858 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)
- CVE-2021-27065 | Microsoft Exchange Server Remote Code Execution Vulnerability (public)

Sincerely,

Microsoft Partner Network

satswana

Company registered number 09329065 www.satswana.com

G Satswana Update April 2021

Contents

1 Stark Fact

94% of cyberattacks start with an email

2 A Data Dilemma

May we share with you a dilemma that connects two subjects together (the second being in Heading 3), with both of them arising *from the fundamental change in the ownership and control of personal information* that was originated within GDPR 2016 and entered into English Law as The Data Protection Act 2018?

The first is the very well-intended work that has historically gone into *finding work placements and assisting with careers advice* – which we also connect with your obligation to provide information regarding *the eventual progress of students to the DfE*. Traditionally this was managed by the School, and there are a number of organisations – many having their origins within the original Local Authority service – who still seek to offer that support, for which they require information to carry out their task.

In the past they asked the School for that information – and you were happy to share it. *What Satswana contends is that you can no longer do that, because it is no longer your data*, it is the Students' and you can only pass that on if you are given their specific consent for the specific purpose. In our submission that means that the support organisations can no longer look to the School to be the provider of information, because you are no longer their customer – it is the individual – and we are very aware of the potential problems that causes.

That is compounded by the perception amongst many youngsters that the information is used institutionally to damage their interests, specifically in the area of benefits. Regrettably many are not prepared to provide consent.

Thus we suggest that the frequent suggestion that a data sharing agreement between the School and the supply organisation can allow data to flow is a nonstarter because you do not have the right to sign that without the specific consent of every single student whose data is provided. Under DPA you have to remain the Controller of that data which makes the supply organisation a Processor, and thus they should be subject to a standard processing agreement.

Furthermore we consider it to be extremely dangerous in computing terms to allow third party organisations to have direct access to your MIS in order to extract data automatically, especially as many of the "sharing agreements" we have seen ask for information that is way beyond the requirements for the task they perform. Why do they do that? Simply because they always did, and in the past they were allowed to, we simply have not returned to consider the core issue now that the ownership of the data has changed.

Having raised the objection and the challenge, can we provide a solution? In suggesting one possibility perhaps we should first define the objective, which is to maintain a connection channel with the student as an individual, because that is their future "customer" status, they cannot be corralled as part of an "institution". *Thus bringing us to our second point*.

3 Student Email

Once again it has been a well-intended policy to provide students with a School email address, though I suspect you will also acknowledge that this had its roots in perceived control and convenience rather than altruism.

As we see it however this is actually stacking up future problems for you whilst frustrating an ongoing relationship opportunity. One really major issue is retention, how long do you keep their data for after they have left – and what do you do when a long lost friend says that they no longer have their only means to contact them?

We suggest that in this age of personal data that they should be responsible for their own email history, and furthermore that puts it out of reach and scope of any access request.

But our strongest case for having this connection with them is that it would probably endure after they left, allowing you a means to contact them that might provide you with intelligence regarding their fortunes, and also keep track of them as alumni.

How else will you do that?

4 Police Powers

Perhaps predictably the rights that were originally written into GDPR 2016 have been weakened within DPA 2018 with additional powers being extended to the Police.

The question came up where a School had taken statements from some students with a guarantee of confidentiality. That would seem to be a pretty clear undertaking, but…

Under the terms of DPA 2018 ICO advice states "…new data protection legislation does not stop (schools) from disclosing personal data to assist police forces or other law enforcement authorities"

Put more succinctly, "Data protection law does not prevent information sharing to save lives and stop crime"

The complete guidance can be found here https://ico.org.uk/about-the-ico/news-and-events/blog-data-protection-law-does-not-prevent-information-sharing-to-save-lives-and-stop-crime/)

Candidly the precise law is not clear, but the intent is within Part 3 Chapter I, clause 30 and 31

The advice remains qualified however, in that it has to be your judgement as to whether organisations can remain confident that the request is "…necessary, relevant and proportionate data (that) can be disclosed in compliance with the law"

The guidance adds "Requests for information made by competent authorities must be reasonable in the context of their law enforcement purpose, and the necessity for the request should be clearly explained to the organisation."

To further interpret this guidance we read "…. (the school) might feel reluctant to voluntarily disclose information to the police if the request appears excessive, or the necessity or urgency appears unjustified. So the onus is on the police to provide as much clarity as they can without prejudicing their investigation." Indeed they state clearly "Don't be afraid to ask the police why the information is required. You should ensure that personal data is not disclosed unless there is a clear and appropriate justification that takes account of the context for the information request from the police."

It is clear that debate continues on the matter and that the ICO is working on updating its Data Sharing Code of Practice – though somewhat bizarrely they go back to referring to DPA 1998 when mentioning that.

To summarise what I suggest can only be an opinion, given this evidence and the absence of any precedent or case law to be substantive – in that the School gave a clear assurance regarding the confidentiality of the statements; in those circumstances you will have to be so totally convinced of the importance of the disclosure to the police that you are prepared to release the confidential information. If on the other hand you consider the police are abusing your knowledge where they could obtain their own statements regarding a relatively trivial matter, you might consider not cooperating.

5 Hidden costs of changing software providers

Satswana constantly seeks to make clear that we consider that the software provided for the use of education establishments is not fit for purpose and too expensive. We plan to cover that further in our update for May.

However, for now, if you are considering any change it is likely that the current ancient designs will not allow you to incept the old data into the new system, meaning that you may be held to ransom by the old provider because you will have to continue to access the files for the retention period.

You may still have a good reason to change, but please take this potentially hidden cost into account.

6 ICO Registration costs

It is a bizarre quirk of the current ICO Registration charging regime that a Multi Academy Trust can have any number of schools within a single Registration, whereas if a school operates an additional service as a Limited Company (in the specific example it was a separately constituted nursery) then that has to pay as an individual entity.

7 Parental Responsibility

As you will be only too aware, when two partners split the school can end up in the firing line between the two as the children are used as ammunition.

In seeking to answer one of the questions that we are continuously grateful to receive we came across the following guidance and draw your attention to it in case it is also helpful to you

Understanding and dealing with issues relating to parental responsibility - GOV.UK (www.gov.uk)

We are unashamed to admit that we are always learning, not least as a result of having to answer your questions.

"If you want tomorrow to be different, you must not do today what you did yesterday"

satswana

Company registered number 09329065 www.satswana.com

H Satswana Update May 2021

Contents

1 Introduction

It is the objective of Satswana in providing its fractional Data Protection Officer Service to Schools to provide proactive input into the subject and we aim by so doing to give our customers a return on investment for the fees they pay us.

Thus we would identify our purpose as being the continuous search for "privacy by design and default", introducing discussion and practical change to design in furtherance of the objectives of the original GDPR, and then ensure that it operates as a default setting. That saves you time and concern, and meets the regulatory challenge.

Towards that end this paper seeks to cover two subjects. First we introduce the concept of the "360° Economy" that will materially change the manner in which data is held and disposed of, massively reducing the liability of a Controller.

Second we seek to bring up the requirement for massive improvement in the quality of software provided to Schools, a subject that we have touched on before, but which is now generating considerable interest. That is not least because any future product should cost you significantly less – delivering a "return on investment".

2 What is the 360° Economy?

Like so much of the jargon of computing and technology it is an attempt to describe a new philosophy within data ownership, just as a "bug" was originally a moth that shorted the insides of a computer – neither party came out well!

It is intended to suggest a complete reversal in the manner that personal data control is managed, and we hope that you will instantly perceive the value that brings to you as an individual.

Just as GDPR sought to transform the ownership of personal data, we now seek to take that to the next stage and introduce personal control of your information in a manner that means you positively consent to its use, and can withdraw that permission at any time.

In turn that creates "one version of the truth", an article of faith in relational programming. It is also gathering support as being "my voice" within the charitable support community, together with "writing their story once".

Indeed, please reflect - why is it that we allowed literally hundreds of organisations to harvest and hold our personal data. Why do we continuously fill in the same information time and time again, whenever we order from a different online store, for instance? Why do we trust them with it when they appear to be almost inevitably hacked, regardless of how "secure" we thought they should be?

The answer of course is that in the early days the macro organisations had computers, and we did not – but all that has changed now. Almost everybody will have a device that is more powerful than those first computers, and thus it is time to rethink the whole issue of the handling, ownership and control of our personal data.

Therefore the 360° Economy describes the complete reversal of the control of our personal information, removing it from the possession of the macro institutions (or even a host of micro ones) and returning it to the absolute ownership and control of the individual. Of course those who rely on using that information in their business must have consented access, but we will come to that in a later briefing – for now we want you to get the message that you will not only own your data, but control it as well.

That is designing in "privacy" in an entirely new way, and then ensuring that it is the default setting. It is as exciting a development as the original interface that we now know as the World Wide Web.

3 How has the concept developed?

Perhaps no surprise then to find that Tim Berners Lee, the WWW creator is a moving spirit behind this concept, together with original thinkers from the Massachusetts Institute of Technology (MIT). They can be found supporting a business called Inrupt.com and sponsoring a personal data platform called Solid. The term 360° Economy was actually first used by Sandra Ro, CEO of the Global Block chain Business Council. Our particular thought process predates those emerging ideas and can be found within www.cvdox.com in which (to declare an interest) Directors of Satswana are subscribers since, like TBL, we also have track records of original thought within the sector.

There is another close parallel with the World Wide Web in that Tim Berners Lee effectively gave the world his technology free, following what he regarded as being the collegiate spirit of the Internet. Similarly every individual will own and control their own data vault; there will be no single controlling provider and competition for the provision may be fierce, holding it on your phone probably being at no cost.

That is not to say that there will be no charges, clearly if you store your entire life in a data centre somewhere then there will be a cost. Similarly there will be the need to create infrastructure that facilitates and manages organisations requiring consented access to the information that they need for their work. Indeed, just as today there is an entire ecosystem dedicated to providing support services to macro institutions, so an element will migrate to imagining, creating and supporting a nascent 360° Economy. But this will be on a strictly service basis, it is actually the antithesis of the "Unicorn" culture.

4 Summarising, for now

Within this briefing we wanted to introduce the philosophy to you, but whilst we have it all worked out in our minds, we are aware of the "too much to read" syndrome and would wish to share the ideas with you in a manageable form. In our next briefing we will introduce a product for use in Schools that will start to establish a population of your data subjects who control their own vault, and also explain how consent will then work. But for now we would like to leave this subject and come onto the need for improved and lower cost management software.

5 How is an oil company managed?

A bit of history, not least to demonstrate the "art of the possible", only fifty years ago the oil industry started the intensive computerisation of what at that time was still a range of disparate systems – not actually wholly unlike what we find in Schools today! A small start-up consultancy called SAP approached ICI with a consultancy project offering to support them in their "Enterprise Resource Planning" (ERP). Some years later they had a clunky system operating that was better than the previous program, and so an oil company asked them to do the same job for them.

To cut a long story short, by the time they had done five or six oil companies, and several other macro industrial organisations – not least IBM who then saw a whole new market having allowed the original engineers to leave them and set up SAP – they no longer asked questions, they said "this is how you run a business" and (of course with tweaks to suit a specific market) it now has 425,000 customers in over 180 countries.

But the important answer to the question in our heading is that they are managed on a single information system which the chief executive, or any other manager, can query at any stage

and get a completely accurate update on precisely what the organisations position is at that moment.

6 The lesson for Schools

Clearly if an organisation of that size and scale can achieve that level of control and efficiency, how much easier should it be to create an ERP program for Schools, and indeed why has it not been done? Why are you suffering the cost, not just in software charges, but in additional training needs, duplication of effort, IT support, incomplete information, transcription errors – and (in terms of DPA) multiple areas of exploit risk? Here comes the "privacy by design" element.

7 The way forward

As with our first subject we would like to use this briefing to plant seeds whose growth we can check later – not least because we are starting to hear a lot of people within education taking up the cry, and we can learn from their ideas as well.

But the subjects do link together, since if we are to change the fundamental nature of where the access file is located – still entirely accessible, and irrelevant to a computer, but with different rules applying – then we need to change our emerging architecture to suit.

We are not unaware of the immense impact of that, who for instance is going to tell the DfE that they can only have access to personal information where the individual has consented? Indeed what about Local Authorities who have always regarded themselves as being the central power source? Of course we have to produce proper answers to their entirely legitimate (and in some instances statutory) need for information. The message has to be that there will be answers and the inevitable resistance to change that will not want to initially hear them – but we must ensure that all parties learn the lessons of the "art of the possible"; advances in this area are inevitable.

So who and how are we going to see the nettle being grasped. We will suggest a range of options, but equally something entirely "left field" might come out of the blue, let us see what we can forecast for now.

8 An establishment project

Quite the simplest to adopt and accept is if one of the major players invested in change in the same way as the early pioneers of SAP did, and indeed what we have heard of the illusory "SIMS 8" would go a long way towards our objective, containing (as we gather it does) its own integrated accounting system in place of FMS. We are concerned however that they will not go the whole way, favouring the retention of relationships with organisations such as My Concern – when the features of that program could be incorporated in SIMS 8. The message that Satswana has sought to proselytise is that the program should meet ALL the requirements

of the management of a School in a single relational structure – including all the communications requirements and other peripheral purchases that you currently make. One real risk that approach will remove is what we consider to be the very dangerous manner in which third party organisations are allowed access to your systems to pass data to another program. Will anybody step up to the plate?

9 A CRM application

Almost any of the existing customer relationship management programs could be adapted to manage the requirements of a School, perhaps with an existing seamless interface into an accounting program such as QuickBooks. The complex area might be agreeing the structure for reporting purposes to intergovernmental agencies, but that is soluble, given the will

10 Using Microsoft architecture

It perhaps demonstrates how complacent the current producers are if it is pointed out that only perhaps seven interested parties attended the Microsoft Strategy Session at Bett 2019, with the rest of the audience being Microsoft staff and speakers. Satswana was pleased to be one of them!

They missed a presentation by Catholic Education, Western Australia on how they had stitched together disparate Microsoft tools to create what was an immense improvement on what you currently work with, if not absolute in terms of perfection since of course it too lacked the specific DfE and LA interfaces.

That might be a readymade solution, or at least one that can be critiqued and improved upon. Sadly somebody might have to travel to Perth to check it out, and that might not be possible for a while!

11 An entirely new entrant

Where markets are large, consistent payers, and yet inefficient a new supplier often gets attracted to the vacuum, and surely the barriers to entry are not so extreme as to discount this happening. What would be the capital required from a dead start, £100 Million? Let us say that 25,000 schools paid £1000 per annum (how much are you paying in total for all your various requirements?) – is that not a 25% return on capital? Does that not mean a Billion Pound valuation? And that is just for the UK, is education so very different in Eire, Sweden, Germany? It certainly did not seem so in Australia. Are there entrepreneurs out there who would take the leap?

We would, of course, welcome your thoughts. Change is coming.

12 Processor agreements and the Children's code

As a final subject, and to deliver something current in this update, Satswana's team looking after the Processor agreements will seek input from organisations that you use that are likely to have to comply with the Code. May we counsel that we have already had a pretty negative response from most US based software providers following the CJEU decision on Privacy Shield and we expect even more resistance from vested interests with this new regulation.

We urge you to review all and any use of organisations resident in the US and to consider whether there is an equivalent European based provider who will support GDPR and the equivalence agreed with the UK. If you can find one, we recommend change.

I Satswana Password Guidance

Contents

1 Introduction

This is an immensely complex subject which is subject to a range of opinions, but we hope to record what we believe to be the latest thinking. However others must be free to disagree. The two basics however is that it should be complex enough not to be guessed, and yet simple enough for you to remember. We hope to make this guidance easy to understand, but if you want to study the subject in greater depth, then you will find excellent guidance here https://www.ncsc.gov.uk/files/password_policy_infographic.pdf

2 Is it complex enough?

Generally a password should be at least 8 characters in length and most require that you adopt one number and one capital letter. Some also suggest a "special character" and that might be regarded as increasing the complexity by a considerable factor.

3 And is it easy to remember?

How about starting with a number, then adding a word or phrase you can remember – starting with a capital letter, and end with an exclamation mark? It does not matter what formula you use, only that you can remember it.

4 Should you change passwords?

If it is compromised, yes, immediately, but if not the latest thinking is that security is best served by the confident use of passwords that you use all the time. Thus the routine forced change every three months (or whatever) should perhaps be abandoned. If you do change, we suggest you increment the "number" you have chosen, so that 1Difficult! Becomes 2Difficult! For instance, thus you have up to 9 to go before you have to remember a different word or phrase.

5 How do I know if I am compromised?

There is a site that you can check your email address on called https://haveibeenpwned.com - but beware that it may only have seen your email once somewhere and may not have any idea what your password is

6 Low value access

We suggest you adopt a password that you might consider using as a default where you are most unlikely to be compromised, because that then also protects the use of your "secure" password. Examples of where we would use a more general option might be for online shopping or a media site for instance. By definition the people you are giving the information to may be less IT capable and more open to attack, but it may pose less risk to you if it is. By contrast the password you use within Microsoft or Virtual Directory is very important indeed and should be used sparingly.

7 Phishing

May we conclude by reminding you that a very high percentage of exploits start with an email as a phishing attack, so be very careful indeed who you decide to share a login with following an email

8 What does that mean in terms of policy?

For high value secure login purposes staff at the school are required to use a password that is at least 8 characters long, utilising at least one number, a capital letter and a special character. It must be changed immediately if it is known to be compromised.

You are requested to use a "second level" password when logging in to community sites or similar where the protection may be less capable and the password might become known. That is to protect the exploitation of your secure password.

We would remind you of the potential danger posed by "phishing" attacks via email

satswana

Company registered number 09329065 www.satswana.com

J Setswana Update June 2021

Contents

1 Education and Skills Funding Agency pulling out of audits

We note that ESFA are no longer going to be involved with audits, moving the responsibility to a report from your Responsible Officer. Given that Cyber Security and compliance with GDPR are two of the headings you may wish to ask Satswana for some support in covering these two subjects since we are qualified in both, whereas we would not expect this to be a prime discipline of an accountancy concern. As always the fee you pay us is inclusive, there would be no additional charge.

2 Colonial Pipeline paid ransom

It is very irresponsible of a major US Corporation to have paid a ransom, so they were subject to a certain amount of schadenfreude when we read that they found that the tool they down loaded was too slow, and that they actually restored more quickly from backups.

Ransomware remains our number one risk concern because it is potentially catastrophically destructive and we cannot emphasise strongly enough that payment can never really be considered an option – even if you have the money. Not only are you supporting crime, but the likelihood is that you will lose your funds as well as your data.

May we please say it again, if you have not already done so, plan to take a complete backup (maybe only once a term, the timing is up to you) that preserves your history if all else is lost. You may still lose a month's worth of data, but you will have shared information with others (such as emails) where you may be able to rebuild much of your recent activity, and can live with anything that you have still lost. If you haven't got your original history, then you are completely sunk.

Many of you, we know, have already acted, and thank you for that. If you still have not done so, please act without delay. There is plenty of evidence that schools are a current target for the criminal community. Fail to do so, and if you are hit, we can assure you it will be a disaster.

3 Term Scoach

We learned that this word has been adopted to mean "steal with stealth" which is precisely what the denizens of the Dark Net do, they never even have to leave their desk to conduct their trade. May we stress that the modern data criminal is extremely competent, extraordinarily well resourced – and has significant online tools at their disposal. They will be constantly probing for a weak spot and then ruthlessly attacking, probably never to be found, let alone seen. We have to be better in defence than they are in attack, and it is a constantly evolving scenario.

4 Enterprise challenge

Satswana had an interesting and very productive interaction with the Prince's Trust when we advised a customer against signing a data sharing agreement to provide the Enterprise Challenge. Fundamentally it was the Satswana view that their agreement was non-compliant, and the discussion made great progress when their DPO immediately agreed with the Satswana point of view and expressed frustration that she had said so internally but not been listened to!

Our analysis of the PT difficulty was that they were hiding what we consider to be an ulterior objective within the worthy subject of the Enterprise Challenge – where the only data required was the team ID, the school name and the first name of the child.

As we understood the PT managers case they were also funded to provide a mentoring service called Achieve, and they required significant personal and sensitive information in order to demonstrate to their funding sources that they had recruited attendance for this support – which the school did not require, and for which the Student had not consented to provide their data.

To our mind it once again confirmed our deep suspicion of the attempted use of a data sharing agreement to disguise an objective that might once have been acceptable within DPA 1998, but is no longer so, ever since the principles of GDPR 2016 emerged to be embraced within DPA 2018.

5 The Domestic Abuse Act

For the next two items Satswana are once again indebted to Safeguarding specialist Andrew Hall, so if you subscribe to his newsletter (which we strongly recommend) you will already be aware, but we repeat if for those who do not.

The Domestic Abuse Act 2021 has now been enacted and will come into force over the next twelve months or so as legislation once the necessary preparatory work has been completed.

Amongst many aspect of the Act, from a child and schools' perspective the changes will:

- Recognise that a child who sees or hears, or experiences the effects of, domestic abuse and is related to the person being abused or the perpetrator is also to be regarded as a victim of domestic abuse.
- Extend the law to young people over the age of 16
- Create a statutory definition of domestic abuse, emphasising that domestic abuse is not just physical violence, but can also be emotional, controlling or coercive, and economic abuse.
- Provide for a new Domestic Abuse Protection Notice and Domestic Abuse Protection Order.
- Place a duty on local authorities in England to provide accommodation based support to victims of domestic abuse and their children in refuges and other safe accommodation.
- Clarify the circumstances in which a court may make a barring order under section 91(14) of the Children Act 1989 to prevent family proceedings that can further traumatise victims.
- Extend the controlling or coercive behaviour offence to cover post-separation abuse.
- Extend the offence of disclosing private sexual photographs and films with intent to cause distress (known as the “revenge porn” offence) to cover threats to disclose such material. (Preferred phrase now is 'Intimate image abuse'.)
- Create a new offence of non-fatal strangulation or suffocation of another person (the so-called 'rough sex' defence)
- Place the guidance supporting the Domestic Violence Disclosure Scheme (“Clare’s law”) on a statutory footing. (This gives anyone a right to ask the police if they believe that they or someone they know is in a relationship with an individual that could be abusive towards them.)
- Provide that all eligible homeless victims of domestic abuse (include the over-16s) automatically have ‘priority need’ for homelessness assistance.

Further reading

Government Fact Sheets: https://www.gov.uk/government/publications/domestic-abuse-bill-2020-factsheets

6 Cyber Security training for school staff

Satswana offers significant advice on training resources, but this one comes from the National Cyber Security Centre and is thus most authoritative. However, for those of you with less time

a colleague recommends this three minute video!
https://www.youtube.com/watch?v=i0iLy8racHI

Please note their equal concentration and concern on the subject of ransomware.

Since late February 2021, an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities. In March 2021 one of the country's largest Multi-Academy Trusts sustained a ransomware attack affecting its 50 primary and secondary academies leaving 37,000 pupils and staff unable to access their email.

The National Cyber Security Centre (NCSC) previously acknowledged an increase in ransomware attacks on the UK education sector during August and September 2020. The NCSC has therefore updated this Alert in line with the latest activity.

In response the NCSC has launched a free cyber security training course to raise awareness and help school staff manage some of the key cyber threats facing schools.

The training is available in two formats: a scripted presentation pack for group delivery; and a self-learn video for staff to complete by themselves is also available on YouTube.

Find the training programme here: https://www.ncsc.gov.uk/information/cyber-security-training-schools

7 Visitor system

In our May update we “trailered” the first product to embrace the principles of the 360° Economy and said that we would provide more detail in our next version. We would advise that www.idmesafe.com is in its final trial stages and we hope that it might be available for the start of the September term.

As you would expect it is entirely automated, but the major changes are that the individual remains in control of the data – and their identity always remains the same. Indeed if your local pub adopted idmesafe then the same identity would work there.

Whilst initially billed as a visitor system, it is actually an identity system – and we can also provide it as a paper QR code, it does not have to involve a Smart Phone. So schools will be invited to consider whether or not it could provide an automated registration system, and indeed record parents arriving for a parents evening. It can record a change of location as well, so if a child enters a swimming pool (for instance) then you know who is in the pool, and who has left to re-join the main school.

We believe that this is just the first example of how transformative thinking will change our entire approach to the management of data – creating “privacy by design and default”.

8 ICO registration, clarification

In the April Update we mentioned that a MAT only pays £40 for its registration with the ICO, we should have added that this requires them to be either an Academy or have charitable status. Other schools are still charged according to their Staff level, which can be as much as £2900, but is more likely to be "Tier 2" at £60. It is very confusing, so if you have any doubts we will happily check your specific circumstances out for you.

K Section 14 – vexatious and repeated requests

Section 14(1)

In determining whether a request is vexatious, the ICO believes that the key question which public authorities need to consider is whether complying with the request is likely to cause a disproportionate or unjustified level of disruption, irritation or distress. Where this is not clear, public authorities should weigh the impact on the authority and balance this against the purpose and value of the request. Where relevant, public authorities will need to take into account wider factors such as the background and history of the request.

The ICO has published guidance on applying section 14(1) of FOIA which includes information on how to apply to this balancing exercise. You are strongly advised to review this guidance before responding to this letter.

As this guidance explains, when determining whether section 14(1) has been applied correctly the ICO will primarily look for evidence that the request would have an **unjustified** or **disproportionate** effect on the public authority.

Therefore, in light of this please explain why in the circumstances of this case xxxxx relied on section 14(1) to refuse the request. Your response should include:

- Details of the detrimental impact of complying with the request;
- Why this impact would be unjustified or disproportionate in relation to the request itself and its inherent purpose or value;
- And, if relevant, details of any wider context and history to the request if xxxxx believes that this background supports its application of section 14(1). Please provide any relevant documentary evidence / background evidence to support such a claim.

We strongly recommend that your response is guided by recent decision notices, our guidance and our lines to take, which demonstrate our approach to the exemptions and procedural sections of the FOIA.

Having revisited the request, you may decide to apply a new exemption or procedural section. We will consider new exemptions or procedural sections, but it is your responsibility to tell the complainant why the new section applies and to provide us now with your full submissions.

For the avoidance of doubt, you should now do the following:

- Consider whether to change your response to the information request and let us know the outcome.
- Answer all the questions in this correspondence.

satswana

Company registered number 09329065 www.satswana.com

L Satswana Update July 2021

Contents

1 Introduction to this update

In addition to this update distributed with this email, we would refer you to our Resources tab on our website (to be found here https://www.satswana.com/Resources)

There you will find the following new documents, underneath our Reference and Guidance Manual. We are seeking to make them permanently accessible to you, whilst also not using email for distribution – beginning to practice what we preach!

1 (3) Satswana Report to Governors 2021
2 (4) Satswana Data Briefing
3 (5) Satswana Cyber Protection
4 (6) Satswana Data Retention
5 (7) Satswana Exemptions (3 Jan 20)
6 (8) Satswana FOIA Guide

In one sense we apologise for a deluge of information just prior to the Summer Holidays, but seek to explain our purpose. We recognise that it is going to take some time to absorb, let alone action, but believe it is our duty to you to be proactive in creating "privacy by design and default", as well as supporting your DPO requirements.

It is written with the background identified in the May Update, complemented now with the Data Briefing at item 4 that will also be found within the Report to Governors.

The first four items are written following a huge ransomware attack that has affected a very large number of Kent Schools, and the separate complete loss of data from a ransomware attack on Skinners School in Tunbridge Wells. (Incidentally we

commend all of you who have taken our advice to take an independent backup of your data – the need to do so could not have been more clearly identified.)

The essence of our entire presentation to you, and the reason why we have gone into such depth, is to stress the absolute need for change within your software provision and hardware management – for reasons of security, efficiency and cost saving. We recognise that it must be possible to implement any proposals, and for that purpose we reproduce below the "disengagement" advice provided to the affected Kent Schools.

Cyber protection is the other side of the coin, and the document included on that subject was written at the request of one of our customers, and as ever we learn your needs that way. The problem with data retention without change is also relevant to the imperative for new thinking.

We recognise that it will all take a considerable time to read, so we are making these documents available as reference works, to be considered when you can, and shared where you feel that change can be encouraged. There is also a very real challenge in considering how we can successfully communicate and share this information consistently with all the Schools that rely upon us to do so.

2 Disengagement

This is a reprint of information already provided to Schools in Kent

How you disentangle yourselves from a high dependency relationship with a provider without risk is a question that Satswana has been asked frequently over the past three years

An issue made even more pertinent when many of you have been without service from just such a provider

Until recently we had no answer, but (as ever) we learn from our customers, and we have found a pioneer who has successfully put options in place

There are normally a total of five issues, though you may not have all of them

1. The supply of broadband connectivity, including secure website filtering
2. Provision of an email service
3. Hosting of your MIS – usually SIMS
4. Website hosting
5. System backup

Satswana suggest that the first key to any change is extensive planning and evaluation, with the highest possible cooperation between schools, you will all want to be reassured that there is no risk from change, and you also massively increase your negotiating power and influence on a provider if you are working as a group.

Put very simply, if you decide to adopt collaborative tools from either Microsoft or Google, then those are best sourced directly from the providers (not through an agency) – which will give you email. (If you are concerned by that and do not have your own resources, Satswana can introduce an IT supporter with a proven track record of implementation.)

Broadband is complex because of the requirement for web filtering, however the latest "next generation" firewalls support control lists in a manner that used to be far more cumbersome to arrange, and furthermore we have evidence of a quantum change in both the cost and support funding available for change. By arranging change across groups of schools we believe it is likely that you will find a better solution at a lower cost. We do not suggest that you can switch tomorrow, but that you will have options for your next contract period.

Where schools have opted for "hosted" SIMS we believe we can show that you can return to an "on premise" server under your own control. In the alternative our "pioneer" has selected a cloud based provider with a relational database centred solution that we support strongly as a future direction. It is your choice as a group, or singularly, as to how radical you want to make your move.

Website hosting should not be an issue

System backup now has a critical element in that you must be sure that it is proof against ransomware. There are many providers with different techniques to achieve this, so whether you choose an on premise solution, or a cloud variant, then solutions are available

In summary therefore this email is to advise you that we have found that other schools have proved solutions exist, and that with careful and cooperative forward planning you can now consider change without systemic risk to your operation.

Most of you already operate within a collaborative group. It should just be a question of linking those groups together to get the benefit of scale within the planning

3 Email address, anti-Spam – plus domain names

If you have used the same email address for many years, then almost certainly it will have been compromised (check at https://haveibeenpwned.com/) which means that you will be on all sorts of lists that generate spam.

One answer is to create an entirely new email address and start afresh using that. When talking to legitimate correspondents start to use the new one when you reply to them, and they will soon pick it up. Of course you need to continue monitoring traffic on the old address, possibly for a very long time, but you will find increasingly that you can delete most of it.

In the context of the disengagement note above, now might be a good time for change, not least if you adopt either Microsoft 365 or Google Cloud – which please do through your IT expert or provider, not through an Agency that will just charge a huge mark up on the cost – whilst at the same time being an added risk to your data.

At the same time as refreshing your email identity, what about your web address? Can you get a less expensive, shorter and more identifiable name? I know of one that requires no less than three dots and three hyphens to type correctly, and that is a nightmare to get right! You can still use the old address – but if you have placenameprimary.co.uk then is that easier? Anybody typing the old name gets "pointed" at the new one, so it is not a problem!

4 From the Oracle, the ICO letter on Registration

Dear Colin,

Thank you for your email and call to the Registration helpline..

We can confirm the general guidance for schools is they are normally a public body and the fee would be taken from the staff numbers only.

As discussed if a school is registered with company house as a Trust or they are a Multi Academy Trust or if they are registered as a charity or they have charitable status. Then any of these criteria would make the organisation eligible for the lowest fee being £40.00 per year.

We can advise a Multi academy Trust is the data controller and their registration would have all the schools that are part of the Trust under the trading name section of the registration.

In this scenario a school joining or belonging to a Multi academy Trust would cancel their individual registration with us as they are covered under the Trust Registration.

Should you require any further assistance, please contact the Registration Helpline on the number below option 1 extension 6408 and they will assist you further.

Regards

Registration Team
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 545748 www.ico.org.uk

5 Product Integration

It is interesting to note that both Microsoft and Google have made provision to access what would appear to be a competitor in Zoom from their platforms. This is an excellent example of the need by a supplier to place customer convenience above their commercial interest. There is a lesson there for all organisations who might still believe that they can charge independently for a unique specialist service. Expect to say goodbye to them soon if they do not change.

6 Reminder, guide to staff leaving

May we remind you that our staff leaving checklist can be found here:-
https://www.satswana.com/resource/GDPRleavingchecklist.pdf

M Satswana Policy revisions August 2021

Contents

1 Explanation

In producing this revision guide we will seek to explain our basis and how you should consider acting as a consequence. We have based the Privacy Policy in Appendix A on the original Department of Education template guides. Broadly speaking we have sought to highlight that DPA 2018 is subject to English Law rather than the European Law of GDPR 2016.

For the Data Protection Policy in Appendix B we have turned to a draft produced by Kent County Council. Other versions may be equally authoritative. This policy is designed for internal consumption, whereas your Privacy Policy is public facing. (Please note we offer our own paper on Retention, but the Architect of IRMS works for KCC so she is also our primary source!)

In suggesting a review we may be considered pedantic and any policy that you have originally adopted may have continued full legal force so it may not be necessary for you to do anything. We would stress that Common Law is driven by precedent and the decisions of Courts and Regulators, so until a case is determined by a proper authority some matters may remain opinion only – and whether or not a Policy complies has to be in that category until better information emerges. If a change comes along then we will all adopt whatever new information is gleaned!

If you have an alternative form of words, possibly based on a different local authority produced template, or indeed created by an individual legal firm, then may we stress again that there is probably absolutely no need to change anything. We do however recommend you consider adopting the clauses below, first because the identity of a person is important, and second to seek to counter data loss claims. (A subject covered in our September update, copies available from admin@satswana.com)

Finally in Appendix C we provide a generic policy that might be suitable for a Company that has many elements that might be required if you employ people. We include it as an aide memoire in case it prompts ideas and thoughts. If you have a

specialist need please contact us as we have seen other excellent examples and may be able to suggest something suitable.

May we stress again that there is nothing that you HAVE to do, but if you decide to review, then we hope this paper will assist.

2 Suggested additional draft clauses for schools

(Title) Checking your identity and responsible persons

To protect the confidentiality of your information, we will ask you to verify your identity before proceeding with any request you make under this Privacy Notice. If you have authorised a third party to submit a request on your behalf, we will ask them to prove they have your permission to act.

The School recognises persons as having parental responsibility as defined by Section 576 of the Education act 1996 and only qualifying applicants have a right to make an access request. We will only withdraw that right from any party on the basis of a court order and then we would require confirmation that the disqualified party has been advised, together with the provisions of Section 170 of the DPA 2018.

Please note that Section 170 of the DPA 2018 criminalises knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller. Any request for any information on any party must be in writing addressed to the data protection manager and will only be provided if appropriate consent is held. Any party seeking information in any other manner will be pursued under Section 170, whether they are successful or not.

Appendix A

Model Privacy Notice

This Model Privacy Notice has been assembled from the basis provided as a template by the DfE in 2018, with additions where considered helpful and revised to reflect DPA 2018 instead of GDPR 2016.

(Please contact us for a copy in Word if that is more convenient to edit in order to reflect precisely your situation. Also note at the end the requirement for an additional clause for Secondary Schools regarding Youth Support Services.)

[School Name]

Privacy Notice for pupils Draft August 2021

This Privacy notice is for Parent/Carers

The Data Protection Act 2018 provides individuals with a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing this 'privacy notice.' It explains how we collect, store and use personal data about pupils.

We, [School Name] are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Satswana Ltd, email at info@satswana.com ; telephone number 01252 516898, office address Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Name
- Contact details, contact preferences, date of birth, identification documents
- Parental, sibling and extended family details
- Children who are adopted from care, looked after children, under special guardianship
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, language, eligibility for free school meals, Pupil Premium or special educational needs
- Exclusion information

- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs of your child
- Carefully chosen and vetted educational apps
- CCTV images

[Biometric Data (we use an automated biometric fingerprint recognition system which is used to purchase items from the school canteen and in our library to loan books. The system takes measurements of the fingerprint; it does not capture a complete image so the original fingerprint cannot be recreated from the data)]

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing.

In order to meet statutory requirements around appropriate education provision and to fulfil safeguarding requirements, we share information about school history and the latest known pupil and parent address and contact details in the event of a Child Missing Education, or becoming Electively Home Educated. This information also supports the in-year admissions process.

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

We may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using pupils' personal data overlap and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

Children's records are stored securely in paper files and on the school's secure server. We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We will adhere to the Information Management Toolkit for Schools guidance on retention.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with the Data Protection Act 2018)

We may share personal information about pupils with:

- Our local authority (e.g. admissions)
- The Department for Education (e.g. attainment)
- The pupil's family and representatives (e.g. attendance)
- Educators and examining bodies (e.g. SATS test papers)
- Our regulators Ofsted, DFE and the ESFA (e.g. pupil data)
- Suppliers and service providers (e.g. sports coaches)
- Central and local government (e.g. attainment)
- Health authorities (e.g. immunisations)
- Health and social welfare organisations (e.g. social services)

- Professional advisers, bodies and consultants (e.g. Educational psychologist)
- Police forces, courts, tribunals (in relation to safeguarding)
- Collaborating schools for moderating purposes

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research. The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on how it collects and shares research data. You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. Parents/carers can make a request with respect to their child's data where the child is under the age of 13, or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

Your other rights regarding your data Under data protection law

Individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)

- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer

Complaints

We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance. To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

This notice is based on the Department for Education's model privacy notice, amended to reflect the way we use data in this school

Additional requirement for Secondary Schools
Please note changes in drafting here, firstly to recognise the age 13 within DPA 2018 – as against the former 16 under DPA 1998, and GDPR 2016. Secondly to modify what otherwise might be regarded as an illegal "opt out" within clause 3, request has been changed to instruct. Satswana nevertheless advise that consent is sought to provide anything other than name, address and DOB. Within 4 "We will seek appropriate consent…" has been specifically added. Adopters should recognise that this is untested drafting and may wish to seek additional advice and comment.

Youth support services

1. Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
2. This enables them to provide services as follows:
    - youth support services
    - careers advisers

3. A parent or guardian can instruct that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 13.
4. We will seek appropriate consent to also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
5. This enables them to provide services as follows:
    - post-16 education and training providers
    - youth support services
    - careers advisers
6. For more information about services for young people, please visit our local authority website.

Appendix B
Data Protection Policy

Kent County Council
Model GDPR and Data Protection Policy for Schools

<Insert Name of School>
GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives
The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the School and all staff comply with the legislation.

Scope of the Policy
Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

[1] GDPR Article 4 Definitions

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[2].

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[3]

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

[3] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[4] unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    - (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    - (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    - (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    - (e) the processing relates to personal data which are manifestly made public by the data subject
    - (f) the processing is necessary for the establishment, exercise or defence of legal claims

[4] GDPR, Article 9

(g) the processing is necessary for reasons of substantial public interest
(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
(i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

Automated Decision Making
Where the school carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The School must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within 21 days.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like

pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. Follow this link to the GDPR page on KELSI where you will find the model privacy notice(s) for schools to use:

http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr

Purpose Limitation
Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights
Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court.

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so

- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security
The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information
Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:
http://www.kelsi.org.uk/__data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Training
The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply
The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

United Kingdom General Data Protection Regulation ('UK GDPR'): Regulation EU 2016/679 https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as confirmed in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

Appendix C

GDPR PRIVACY NOTICE For COMPANIES (Draft to be amended as required)

Introduction

The Company collects and processes personal information, or personal data, relating to its employees, workers and contractors to manage the working relationship. This personal information may be held by the Company on paper or in electronic format. The Company is committed to being transparent about how it handles your personal information, to protecting the privacy and security of your personal information and to meeting its data protection obligations under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018. The purpose of this privacy notice is to make you aware of how and why we will collect and use your personal information both during and after your working relationship with the Company. We are required under the GDPR to notify you of the information contained in this privacy notice.
This privacy notice applies to all current and former employees, workers and contractors. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.
The Company has appointed an external data protection officer to oversee compliance of this privacy notice. If you have any questions about this privacy notice or about how we handle your personal information, please contact our Data Protection Officer, Satswana Ltd at info@satswana.com or 01252 516898

Data protection principles
Under the GDPR, there are six data protection principles that the Company must comply with. These provide that the personal information we hold about you must be:
1. Processed lawfully, fairly and in a transparent manner.
2. Collected only for legitimate purposes that have been clearly explained to you and not further processed in a way that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to those purposes.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits your identification for no longer than is necessary for those purposes.
6. Processed in a way that ensures appropriate security of the data.

The Company is responsible for, and must be able to demonstrate compliance with, these principles. This is called accountability.

What types of personal information do we collect about you?

Personal information is any information about an individual from which that person can be directly or indirectly identified. It doesn't include anonymised data, i.e. where all identifying particulars have been removed. There are also "special categories" of personal information, including personal information on criminal convictions and offences, which requires a higher level of protection because it is of a more sensitive nature. The special categories of personal information comprise information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.
The Company collects, uses and processes a range of personal information about you. This includes (as applicable):

- your contact details, including your name, address, telephone number and personal e-mail address
- your emergency contact details/next of kin
- your date of birth
- your gender
- your marital status and dependants
- the start and end dates of your employment or engagement
- recruitment records, including personal information included in a CV, any application form, cover letter, interview notes, references, copies of proof of right to work in the UK documentation, copies of qualification certificates, copy of driving licence and other background check documentation
- the terms and conditions of your employment or engagement (including your job title and working hours), as set out in a job offer letter, employment contract, written statement of employment particulars, casual worker agreement, consultancy agreement, pay review and bonus letters, statements of changes to employment or engagement terms and related correspondence
- details of your skills, qualifications, experience and work history, both with previous employers and with the Company
- your professional memberships
- your salary, entitlement to benefits and pension information
- your National Insurance number
- your bank account details, payroll records, tax code and tax status information
- any disciplinary, grievance and capability records, including investigation reports, collated evidence, minutes of hearings and appeal hearings, warning letters, performance improvement plans and related correspondence
- appraisals, including appraisal forms, performance reviews and ratings, targets and objectives set
- training records
- timesheets

- annual leave and other leave records, including details of the types of and reasons for leave being taken and related correspondence
- any termination of employment or engagement documentation, including resignation letters, dismissal letters, redundancy letters, minutes of meetings, settlement agreements and related correspondence
- information obtained through electronic means, such as swipecard or clocking-in card records
- information about your use of our IT systems, including usage of telephones, e-mail and the Internet
- photographs

The Company may also collect, use and process the following special categories of your personal information (as applicable):

- information about your health, including any medical condition, whether you have a disability in respect of which the Company needs to make reasonable adjustments, sickness absence records (including details of the reasons for sickness absence being taken), GP or occupational health medical reports and related correspondence
- information about your racial or ethnic origin, religious or philosophical beliefs and sexual orientation
- trade union membership
- information about criminal convictions and offences

How do we collect your personal information?

The Company may collect personal information about employees, workers and contractors in a variety of ways. It is collected during the recruitment process, either directly from you or sometimes from a third party such as an employment agency. We may also collect personal information from other external third parties, such as references from former employers, information from background check providers, information from credit reference agencies and criminal record checks from the Disclosure and Barring Service (DBS).

We will also collect additional personal information throughout the period of your working relationship with us. This may be collected in the course of your work-related activities. Whilst some of the personal information you provide to us is mandatory and/or is a statutory or contractual requirement, some of it you may be asked to provide to us on a voluntary basis. We will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Your personal information may be stored in different places, including in your personnel file, on the Company's HR management system and in other IT systems, such as the e-mail system.

Why and how do we use your personal information?

We will only use your personal information when the law allows us to. These are known as the legal bases for processing. We will use your personal information in one or more of the following circumstances:

- where we need to do so to perform the employment contract, casual worker agreement, consultancy agreement or contract for services we have entered into with you
- where we need to comply with a legal obligation
- where it is necessary for our legitimate interests (or those of a third party), and your interests or your fundamental rights and freedoms do not override our interests.

We may also occasionally use your personal information where we need to protect your vital interests (or someone else's vital interests).

We need all the types of personal information listed under *"What types of personal information do we collect about you?"* primarily to enable us to perform our contract with you and to enable us to comply with our legal obligations. In some cases, we may also use your personal information where it is necessary to pursue our legitimate interests (or those of a third party), provided that your interests or your fundamental rights and freedoms do not override our interests. Our legitimate interests include: performing or exercising our obligations or rights under the direct relationship that exists between the Company and you as its employee, worker or contractor; pursuing our business by employing (and rewarding) employees, workers and contractors; performing effective internal administration and ensuring the smooth running of the business; ensuring the security and effective operation of our systems and network; protecting our confidential information; and conducting due diligence on employees, workers and contractors. We believe that you have a reasonable expectation, as our employee, worker or contractor, that we will process your personal information.

The purposes for which we are processing, or will process, your personal information are to:

- enable us to maintain accurate and up-to-date employee, worker and contractor records and contact details (including details of whom to contact in the event of an emergency)
- run recruitment processes and assess your suitability for employment, engagement or promotion
- comply with statutory and/or regulatory requirements and obligations, e.g. checking your right to work in the UK
- comply with the duty to make reasonable adjustments for disabled employees and workers and with other disability discrimination obligations
- maintain an accurate record of your employment or engagement terms
- administer the contract we have entered into with you
- make decisions about pay reviews and bonuses
- ensure compliance with your statutory and contractual rights

- ensure you are paid correctly and receive the correct benefits and pension entitlements, including liaising with any external benefits or pension providers or insurers
- ensure compliance with income tax requirements, e.g. deducting income tax and National Insurance contributions where applicable
- operate and maintain a record of disciplinary, grievance and capability procedures and action taken
- operate and maintain a record of performance management systems
- record and assess your education, training and development activities and needs
- plan for career development and succession
- manage, plan and organise work
- enable effective workforce management
- operate and maintain a record of annual leave procedures
- operate and maintain a record of sickness absence procedures
- ascertain your fitness to work
- operate and maintain a record of maternity leave, paternity leave, adoption leave, shared parental leave, parental leave and any other type of paid or unpaid leave or time off work
- ensure payment of SSP or contractual sick pay
- ensure payment of other statutory or contractual pay entitlements, e.g. SMP, SPP, SAP and ShPP
- meet our obligations under health and safety laws
- make decisions about continued employment or engagement
- operate and maintain a record of dismissal procedures
- provide references on request for current or former employees, workers or contractors
- prevent fraud
- monitor your use of our IT systems to ensure compliance with our IT-related policies
- ensure network and information security and prevent unauthorised access and modifications to systems
- ensure effective HR, personnel management and business administration, including accounting and auditing
- ensure adherence to Company rules, policies and procedures
- monitor equal opportunities
- enable us to establish, exercise or defend possible legal claims

Please note that we may process your personal information without your consent, in compliance with these rules, where this is required or permitted by law.

What if you fail to provide personal information?

If you fail to provide certain personal information when requested or required, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations. You may also be unable to exercise your statutory or contractual rights.

Why and how do we use your sensitive personal information?

We will only collect and use your sensitive personal information, which includes special categories of personal information and information about criminal convictions and offences, when the law allows us to.

Some special categories of personal information, i.e. information about your health or medical conditions and trade union membership, and information about criminal convictions and offences, is processed so that we can perform or exercise our obligations or rights under employment law or social security law and in line with our data protection policy. Information about health or medical conditions may also be processed for the purposes of assessing the working capacity of an employee or medical diagnosis, provided this is done under the responsibility of a medical professional subject to the obligation of professional secrecy, e.g. a doctor, and again in line with our data protection policy.

We may also process these special categories of personal information, and information about any criminal convictions and offences, where we have your explicit written consent. In this case, we will first provide you with full details of the personal information we would like and the reason we need it, so that you can properly consider whether you wish to consent or not. It is entirely your choice whether to consent. Your consent can be withdrawn at any time.

The purposes for which we are processing, or will process, these special categories of your personal information, and information about any criminal convictions and offences, are to:

- assess your suitability for employment, engagement or promotion
- comply with statutory and/or regulatory requirements and obligations, e.g. carrying out criminal record checks
- comply with the duty to make reasonable adjustments for disabled employees and workers and with other disability discrimination obligations
- administer the contract we have entered into with you
- ensure compliance with your statutory and contractual rights
- operate and maintain a record of sickness absence procedures
- ascertain your fitness to work
- manage, plan and organise work
- enable effective workforce management
- ensure payment of SSP or contractual sick pay
- meet our obligations under health and safety laws
- make decisions about continued employment or engagement
- operate and maintain a record of dismissal procedures
- ensure effective HR, personnel management and business administration

- ensure adherence to Company rules, policies and procedures
- monitor equal opportunities
- pay trade union premiums

Where the Company processes other special categories of personal information, i.e. information about your racial or ethnic origin, religious or philosophical beliefs and sexual orientation, this is done only for the purpose of equal opportunities monitoring and in line with our data protection policy. Personal information that the Company uses for these purposes is either anonymised or is collected with your explicit written consent, which can be withdrawn at any time. It is entirely your choice whether to provide such personal information.
We may also occasionally use your special categories of personal information, and information about any criminal convictions and offences, where it is needed for the establishment, exercise or defence of legal claims.

Change of purpose
We will only use your personal information for the purposes for which we collected it. If we need to use your personal information for a purpose other than that for which it was collected, we will provide you, prior to that further processing, with information about the new purpose, we will explain the legal basis which allows us to process your personal information for the new purpose and we will provide you with any relevant further information. We may also issue a new privacy notice to you.

Who has access to your personal information?
Your personal information may be shared internally within the Company, including with members of the HR department, payroll staff, your line manager, other managers in the department in which you work and IT staff if access to your personal information is necessary for the performance of their roles.
The Company may also share your personal information with third-party service providers (and their designated agents), including:

- external HR support (Solutions for HR)
- external organisations for the purposes of conducting pre-employment reference and employment background checks
- payroll providers
- benefits providers and benefits administration, including insurers
- pension scheme provider and pension administration
- occupational health providers
- external IT services
- external auditors
- professional advisers, such as lawyers and accountants

The Company may also share your personal information with other third parties in the context of a potential sale or restructuring of some or all of its business. In those circumstances, your personal information will be subject to confidentiality undertakings.
We may also need to share your personal information with a regulator or to otherwise comply with the law.
We may share your personal information with third parties where it is necessary to administer the contract we have entered into with you, where we need to comply with a legal obligation, or where it is necessary for our legitimate interests (or those of a third party).

How does the Company protect your personal information?
The Company has put in place measures to protect the security of your personal information. It has internal policies, procedures and controls in place to try and prevent your personal information from being accidentally lost or destroyed, altered, disclosed or used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, workers, agents, contractors and other third parties who have a business need to know in order to perform their job duties and responsibilities. You can obtain further information about these measures from our Data Protection Officer, Satswana Ltd at info@satswana.com or 01252 516898
Where your personal information is shared with third-party service providers, we require all third parties to take appropriate technical and organisational security measures to protect your personal information and to treat it subject to a duty of confidentiality and in accordance with data protection law. We only allow them to process your personal information for specified purposes and in accordance with our written instructions and we do not allow them to use your personal information for their own purposes.
The Company also has in place procedures to deal with a suspected data security breach and we will notify the Information Commissioner's Office (or any other applicable supervisory authority or regulator) and you of a suspected breach where we are legally required to do so.
For how long does the Company keep your personal information?
The Company will only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. The Company will generally hold your personal information for the duration of your employment or engagement. The exceptions are:

- any personal information supplied as part of the recruitment process will not be retained if it has no bearing on the ongoing working relationship
- personal information about criminal convictions and offences collected in the course of the recruitment process will be deleted once it has been verified through a

DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by the Company as relevant to the ongoing working relationship

- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the Company as relevant to the ongoing working relationship
- if it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after six months or once the conviction is "spent" if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession)
- disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of your employment).

Once you have left employment or your engagement has been terminated, we will generally hold your personal information for one year after the termination of your employment or engagement, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal information for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. We will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for six years after the termination of your employment or engagement. Overall, this means that we will "thin" the file of personal information that we hold on you one year after the termination of your employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IT systems and we will also require third parties to destroy or erase such personal information where applicable. In some circumstances we may anonymise your personal information so that it no longer permits your identification. In this case, we may retain such information for a longer period.

Your rights in connection with your personal information

It is important that the personal information we hold about you is accurate and up to date. Please keep us informed if your personal information changes, e.g. you change your home address, during your working relationship with the Company so that our records can be updated. The Company cannot be held responsible for any errors in your personal information in this regard unless you have notified the Company of the relevant change.

- As a data subject, you have a number of statutory rights. Subject to certain conditions, and in certain circumstances, you have the right to: request access to your personal information - this is usually known as making a data subject access request and it enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- request rectification of your personal information - this enables you to have any inaccurate or incomplete personal information we hold about you corrected
- request the erasure of your personal information - this enables you to ask us to delete or remove your personal information where there's no compelling reason for its continued processing, e.g. it's no longer necessary in relation to the purpose for which it was originally collected
- restrict the processing of your personal information - this enables you to ask us to suspend the processing of your personal information, e.g. if you contest its accuracy and so want us to verify its accuracy
- object to the processing of your personal information - this enables you to ask us to stop processing your personal information where we are relying on the legitimate interests of the business as our legal basis for processing and there is something relating to your particular situation which makes you decide to object to processing on this ground
- data portability - this gives you the right to request the transfer of your personal information to another party so that you can reuse it across different services for your own purposes.

If you wish to exercise any of these rights, please contact our Data Protection Officer, Satswana Ltd at info@satswana.com or 01252 516898. We may need to request specific information from you in order to verify your identity and check your right to access the personal information or to exercise any of your other rights. This is a security measure to ensure that your personal information is not disclosed to any person who has no right to receive it.
In the limited circumstances where you have provided your consent to the processing of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on your consent before its withdrawal. If you wish to withdraw your consent, please contact our Data Protection Officer, Satswana Ltd at info@satswana.com or 01252 516898. Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose you originally agreed to, unless we have another legal basis for processing.
If you believe that the Company has not complied with your data protection rights, you have the right to make a complaint to the Information Commissioner's Office (ICO) at any time. The ICO is the UK supervisory authority for data protection issues.

Transferring personal information outside the European Economic Area

The Company will not transfer your personal information to countries outside the European Economic Area.

Automated decision making

Automated decision making occurs when an electronic system uses your personal information to make a decision without human intervention.
We do not envisage that any employment decisions will be taken about you based solely on automated decision making, including profiling. However, we will notify you in writing if this position changes.

Changes to this privacy notice

The Company reserves the right to update or amend this privacy notice at any time, including where the Company intends to further process your personal information for a purpose other than that for which the personal information was collected or where we intend to process new types of personal information. We will issue you with a new privacy notice when we make significant updates or amendments. We may also notify you about the processing of your personal information in other ways.

Contact

If you have any questions about this privacy notice or how we handle your personal information, please contact our Data Protection Officer, Satswana Ltd at info@satswana.com or 01252 516898.

I acknowledge receipt of this privacy notice and I confirm that I have read and understood it.
Signed: . . . .
Print name: . . . .
Dated: . . . . . .

satswana

Company registered number 09329065 www.satswana.com

N Satswana Update September 2021

Contents

1 Immediate action required

Welcome back, but with a new school year we must ask you to immediately adopt six resolutions, not just to ensure that you are compliant with the Data Protection Act – because that is the easy bit – but to ensure that you have done everything you can to protect your people, your reputation and your heritage; because all of those might be so easily compromised if you do not take management action. We will list the six essential headings and would ask all Principals, SLT and Governors/Trustees to make it their business to ensure that the subjects have been addressed.

a) Are you in control?

Not a trick question, because you might very reasonably NOT be in control, you may be relying on all sorts of specialist support and contractors, but we intend to show you why that has to change, why you must be the source of all authority, control the decision making. Some of these are outlined below but they are just examples because new subjects are going to constantly emerge and if they do not follow your policy, your direction, then you will continue not to be in control – and going forward from now onwards, that must be regarded as being unacceptable.

This is a subject that Satswana will be constantly referring to in the belief that restoring control to the persons in authority is essential to your future protection. Specifically in data of course, but we contend that extends to pupil, staff, parent and management security as well, they are now one and the same thing.

So we ask you to challenge every current decision you have made to subcontract a service, capability, function or supply arrangement. Who is taking the management decisions regarding their control and daily tasks? Are they sufficiently under the command of one of your staff, and if so do you feel confident that they are seeking your opinion and informing you regarding the decisions they are taking.

We repeat, this is not a trick question, but very many Principals and Governors/Trustees reading this will be saying to themselves, "actually I have no idea". Please immediately forgive yourselves, but our mission this year has to be to change that, and we would remind you that legally you must consult your DPO on such matters!

b) Is your data encrypted?

By now if the answer to this is no, or even worse, I don't know, then this has to be addressed immediately. Do not assume that if your data is subcontracted somewhere that it is being properly managed. Recall that in the attack on both Talk Talk and British Airways they only discovered that any hacker could read their data AFTER the attack (and just how much were their IT staff paid?) Recall please that "assume" "makes an ass of u and me"! As a Principal you must KNOW the answer, please never rely on a third party.

c) Have you trained your staff?

Many of them will be new to you this term; others may have forgotten instructions that were originally concentrated on in 2018. Yet others will not be aware of how much more dangerous the world has become since then. Please see item 6 below for some refresher thoughts.

d) What is your email strategy?

With 94% of cyber-attacks originating within a phishing email we must all be planning to dramatically change our reliance on email communication in favour of modern collaborative tools. Very specifically we suggest that no staff be authorised to click on any link within an email, or open any attachment, without specific management authority to do so. We recognise how difficult that may make things, especially when exchanging information with other agencies that may refuse to cooperate. But you can absolutely guarantee that the "phishers" will find a way of posing as that agency – and use that as a means of infecting a target with a ransomware attack. It may not be the agency that suffers, but you will, and their convenience is not worth that risk.

e) Consider your policies

Please see item 2 below as to why you must update your privacy and data protection policies. The claims specialists are targeting you for their next earnings opportunity.

f) Backup

Regular readers will be fed up with hearing this and will have taken action to ensure that they have a completely isolated historical "snap shot" of their data hidden away somewhere. The purpose is to have a historical record that you can go back to if you do get hit with ransomware as the Harris Federation was, and also The Island Education Federation over the summer holidays. It will be chaotic trying to rebuild your current data if you lose it, but you have a chance up to about three months old. Over that, can you remember what you did?

To conclude, these are six management functions that we advise you to address at the first opportunity. The most important is that you must assert YOUR management control over the decisions that are being taken.

2 Claims for damage and distress

In a most unwelcome development we have discovered the emergence of "claims specialists" willing to exploit any accidental sharing of data that is too easy to occur in a busy school.

The "claim" is normally in a template format and is likely to refer to a protocol to be found here https://www.justice.gov.uk/courts/procedure-rules/civil/protocol/prot_def
It is probably worth quickly familiarising yourselves with the detail, both in terms of the required response and also the resolution procedures. Please note that we recommend you state you are a "Litigant in Person" in any initial acknowledgement so that any subsequent Court would be aware that you were not a professional respondent at that time.

Until we have precedents and case law to further inform us we cannot really see where this is going, but the firms generally work on a "no win, no fee" basis so the more they can play up the "damage and distress" then the more they are likely to get paid. Satswana suggests that we have to move to create whatever defence position we can in advance of any conclusion.

In both current instances details of a mother's location were accidentally revealed to an abusive father in circumstances where it was claimed that the school had been instructed that information was not to be provided.

There are many arising aspects, none of which we can currently answer, but we would postulate how any school can possibly ensure that every member of staff is sufficiently aware of all data circumstances in order to be certain that a question from a known family member is not answered in an innocent fashion? If the answer is that you cannot, and neither can you contract out of your liability (or we do not think you can as per DPA 2018) how can you protect yourselves?

Pending any better ideas we note that Section 170 of the DPA 2018 criminalises knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller. The thought process is twofold; first we would seek to use it as a deterrent in the first instance, secondly as a means of financial recourse from a discloser of information in the event the school is pursued. Neither is perfect, because we cannot guarantee that a family member is aware of the risk, or that they have the means to compensate the school, but until we have better ideas it is a start.

Satswana recommend that you add the following clause to your Privacy Notice. Of course you may develop different ideas and have access to alternative specialist advice, this is just a start.

"The School recognises persons as having parental responsibility as defined by Section 576 of the Education act 1996 and only qualifying applicants have a right to make an access request. We will only withdraw that right from any party on the basis of a court order and then we would require confirmation that the disqualified party has been advised, together with the provisions of Section 170 of the DPA 2018.

Please note that Section 170 of the DPA 2018 criminalises knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller. Any request for any information on any party must be in writing addressed to the data protection manager and will only be provided if appropriate consent is held. Any party seeking information in any other manner will be pursued under Section 170, whether they are successful or not."

An appropriate awareness and discipline clause should also be added to your staff procedures.

The bottom line is that it is now just too risky for any staff to disclose any information to either a parent or what might otherwise have been considered a person who could be given the requested detail. How you control that, to include every TA and any temporary staff, will remain difficult, especially as the questioner may be very well aware that they should not be asking, and thus seeking to take advantage of innocence. The defence we now have is that at least that person will now face some sanction. It is worryingly imperfect and we hope that a better solution emerges.

(Please note that we published the following guidance link on parental responsibility in our April 2021 update Understanding and dealing with issues relating to parental responsibility - GOV.UK (www.gov.uk)

3 Data Sharing agreements

May we please advise again that within the education sector we can see no purpose for so called data sharing agreements. They are always overlong, written in complex legal language, normally originally based on the DPA 1998 without reflecting changes from GDPR 2016, and may have some underlying vested interest hidden within their content.

Recently we have considered three situations, the first being with the Police, who we would all wish to support. Candidly any requirement there is very well covered by legislation, and does not need a separate agreement. The second was with the Prince's Trust, where their own DPO immediately said that Satswana was reflecting the very points that she had been making internally – we are expecting wholesale change as a consequence. Finally we had a similarly constructive engagement with another Contractor which resulted in the very much simpler agreement we reproduce below. Please note that the key is in the title, it is a Data PROCESSOR agreement, reflecting your role as a Controller, and theirs as a Processor. That is what DPA 2018 covers.

Please contact us if you are asked to agree a data sharing agreement, we can hopefully save you a great deal of administration time.

(Name of school), as Data Controller, appoint Contractor as a data Processor to arrange virtual work experience placements for some of their students for the duration of the work experience. As part of that, Contractor will provide feedback to (Name of school) as appropriate.

(Name of school) will supply student data to Contractor having obtained the appropriate consent from their students.

Contractor may process basic contact information relating to students to provide this service, and all processing must be kept confidential, secure, and in strict compliance with all data protection regulations.

Contractor is responsible for assisting (Name of school) with their obligation to any requests from Data Subjects to exercise their rights.

(Name of school) reserve the right to audit Contractor to ensure compliance with data policies and relevant regulations.

Once the personal data has served its purpose, it should be deleted securely or anonymised so much as it applies to the service.

Any breach of any data protection regulation by Contractor must be notified to (Name of school) immediately on becoming aware of the breach.

Contractor is permitted to appoint sub-processors in relation to this agreement where strictly necessary provided that all sub-processing is conducted under the protection of a written agreement between Contractor and any sub-processors. Contractor is responsible for strict oversight of Sub-processors to ensure compliance.

(We have not named the Contractor because they have now spent considerable time seeking to dilute and obfuscate this simple agreement in favour of their original complex data sharing version leading to a standoff with both schools. If "the customer is always right" then the schools must win this one!)

4 Looked after Children record retention

We had very helpful advice from Surrey County Council on this subject passed on to us, as follows.

The Social Care element of children's records needs to be kept for 75 years, however the education element only needs to be kept until they are 25, or 31 if they had an EHCP. (Social Care data is normally held by the Local Authority.)

5 New version of KCSIE

The 2021 version can be found here

Keeping children safe in education 2021 (publishing.service.gov.uk)

Relevance of KCSIE to DPA 2018

Whereas the Data Protection Act has a very general approach to Regulation, there is a much greater degree of definition of some matters relating to data privacy and security contained within KCSIE.

In terms of compliance, all staff are expected to read Part One, though Annex A contains a subset for those not in direct touch with children. Annex G contains a summary of changes for those familiar with earlier versions

The vital statement that says essentially that safeguarding trumps GDPR can now be found at Clause 60 in Part I and 110 in Part 2. We would also ask you to note the following points that will inform Satswana's advice on Data, the number referred to is the Clause number in the Act.

112 Refers to the transfer of the child protection file to a new school. The DSL must ensure its secure transit and obtain a confirmed receipt, ensuring that the receiving DSL is aware

113 Covers the sharing of additional data

127 Useful guidance on remote learning

131 Covers information security and access management, very much a DPO role

132 (Also 133) Covers online safety in the same way

198 You can ask for a self-declaration from short listed candidates with an affirmation of truth. This may be particularly useful since it can cover overseas information, especially now that European data is no longer available through the TRA

203 Study this section and following clauses for guidance on references

250 What is required for the Single Central Record, critical data for all schools

258 Defines the six month period that you can retain a DBS record for

259 Defines other records that should be kept on the Personnel file

372 Covers confidentiality in investigation situations, broadly speaking consent is still required

373 Within this clause the Police are expected to obtain consent from the person before sharing

KCSIE has a lot to contribute to the detail of data management.

6 Refresher training

For those who wish to reinforce the issue of Data Protection at the start of the year, or perhaps introduce the subject to new staff, may we start by referencing heading 2.5, page 14, in our guidance manual, to be found here

https://www.satswana.com/resource/SatswanaGuidanceManualVer4.pdf

There are two videos, one being a somewhat formal affair from the ICO, the other is much more fun and seeks to show how easy it is to capture data about people – it makes an otherwise dull subject a bit more engaging – especially for younger staff

If you want to go a little further, then please find below a reproduction of the item we carried in our June update, as follows:-

Cyber Security training for school staff

Satswana offers significant advice on training resources, but this one comes from the National Cyber Security Centre and is thus most authoritative. However, for those of you with less time a colleague recommends this three minute video! https://www.youtube.com/watch?v=i0iLy8racHI

Please note their equal concentration and concern on the subject of ransomware.

Since late February 2021, an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities. In March 2021 one of the country's largest Multi-Academy Trusts sustained a ransomware attack affecting its 50 primary and secondary academies leaving 37,000 pupils and staff unable to access their email.

The National Cyber Security Centre (NCSC) previously acknowledged an increase in ransomware attacks on the UK education sector during August and September 2020. The NCSC has therefore updated this Alert in line with the latest activity.

In response the NCSC has launched a free cyber security training course to raise awareness and help school staff manage some of the key cyber threats facing schools.

The training is available in two formats: a scripted presentation pack for group delivery; and a self-learn video for staff to complete by themselves is also available on YouTube.

Find the training programme here: https://www.ncsc.gov.uk/information/cyber-security-training-schools

If you wish there is a much longer one there from the NCSC but (apart from the American accent) their seven points cover the points well in a short time.

7 Whither SIMS

You will be aware by now that Satswana considers almost every example of software offered to the education community to be unfit for purpose, with no better example than SIMS – which only survives because of its almost ubiquitous adoption, meaning that it is a familiar product, and nobody welcomes change.

Everybody agrees that it does not meet modern standards, not least of all the SIMS engineers who have promised us a cloud based "SIMS 8" for many years. Most encouragingly it was to use a Capita owned and developed relational accounting package that would be integrated in place of FMS. (Quite what was going to happen to the good folk at ESS was not explained.)

They need not worry for a bit, because it is still "not available", new customers are still being offered the antique SIMS 7. Doubtless those former local authority service companies that survive selling services (sic) and perhaps hosting the product (as those based in Kent will be regretting) will also heave a sigh of relief. Because according to reports, SIMS 8 was only going to be sold direct – a decision that we consider to be correct, but which maroons a great deal of their past support infrastructure. (Similarly Schools should only contract directly with Microsoft for their 365 product, not through an agent.)

Against that background Capita's sale of SIMS to "private equity" looks like a smart move. They escape a developmental money pit and bank £400 Million, probably knowing full well that their customers are likely to abandon the product in droves just as soon as any sort of realistic competition emerges.

The big question is whether or not the buyer obtained rights to continue to use the accounting software in the development product? The engineers will have wanted that, but did the clever (sic once more) money men doing the deal even consult them? Time may tell, "another two years" – nothing like Groundhog day then.

But from the point of view of the patient and resigned users it is out of the frying pan and into the fire. Capita may have been a ponderous monolith of an owner that failed to reinvest its considerable cash flow from education into a modern product, but that pales against the rapacious reputation of private equity.

What do we know of their modus operandi? First that it will be an unashamed exercise in financial engineering, aimed at sucking as much money as possible out of the organisation up front whilst loading it with debt. They may throw it together with other sectoral assets and appoint a suitably safe corporate figure to maximise profits, achieved by "reviewing" all jobs, expenditure, investment; any and every

figure in the pay column. At the same time every opportunity will be taken to raise prices, the whole being entirely legitimate and legal activities. They will then await their opportunity to unload it onto the market at a profit.

We do not know whether SIMS will go that way, but wonder at the logic of making the management of Parent Pay the apparently senior control organisation. We also question the experience of the requirements of education of a man who ran American Express for almost twelve years. To our way of thinking that does not bode well. Will they join the other "groups" who have bought educational software assets for their revenues, and not with any strategic future purpose in mind?

What you can be sure of is that many excellent engineers and competent managers that used to work there will end up as roadkill in the gutter, but there is hope in that. History has many examples of entrepreneurs emerging from such ruins to found next generation solutions. Money may be regarded as a measure of achievement, but Satswana regards a good job, well done – and fairly priced as being an infinitely more satisfying ambition.

8 Age Appropriate Design Code

Did you read that children are being targeted with content about eating disorders, self-harm and sexualised images within 24 hours of creating a social media account? Theoretically the so called "Children's Code", effective from September, should counter some of this abuse, but the reality is that it will not do so for a long time.

In the name of free speech the United States has allowed an uncontrolled feeding frenzy of greed to exploit innocence and they will fight to preserve their cash flow.

We will all do our best to call them out, and the Code provides us with an additional weapon to do so, but the abusers have had a very long time to consolidate their position, acquiring huge resources to deploy in their defence.

That can only spell trouble. See article 10 below.

9 Meaning of educational record

There is general confusion regarding the age of consent, made all the more problematic by the (in our view pretty inexplicable) reduction from the 16 quoted in GDPR to 13 within DPA 2018. When it comes to a Subject Access Request, under DPA we must require that the child who is 13+ makes the application, not the Parent.

However, the Education Act enshrines the right of a Parent to a copy of their child's education record up to age 18. So the question is what does that consist of, as

distinct from the data to be provided under SAR? (To confirm in passing that the Freedom of Information Act does not allow the disclosure of personal data.) We reproduce the guidance below, but the obvious (and welcome) exclusion would be any correspondence within email. We construe it as being limited to any formally recorded state or condition that applies to the pupil.

The following extract is taken from The Education (Pupil Information) (England) Regulations 2005 (legislation.gov.uk)

3.—(1) Subject to paragraph (4), in these Regulations "educational record" means any record of information which—

(a)is processed by or on behalf of the governing body of, or a teacher at, any school specified in paragraph (2);

(b)relates to any person who is or has been a pupil at any such school; and

(c)originated from or was supplied by or on behalf of any of the persons specified in paragraph (3),

other than information which is processed by a teacher solely for the teacher's own use.

(2) The schools referred to in paragraph (1)(a) are—

(a)any school maintained by a local education authority; and

(b)any special school which is not so maintained.

(3) The persons referred to in paragraph (1)(c) are—

(a)any employee of the local education authority which maintains the school or former school attended by the pupil to whom the record relates;

(b)in the case of—

(i)a voluntary aided, foundation or foundation special school; or

(ii)a special school which is not maintained by a local education authority,

any teacher or other employee at the school or at the pupil's former school (including any educational psychologist engaged by the governing body under a contract for services);

(c)the pupil to whom the record relates; and

(d)a parent of that pupil.

(4) In addition to the information referred to in paragraph (1), an educational record includes—

(a)any statement of special educational needs; and

(b)any personal education plan,

relating to the pupil concerned.

(5) For the purposes of this regulation, "processed" shall be construed in accordance with the definition of "processing" in section 1(1) of the Data Protection Act 1998(1).

Parents are entitled to request access to, or a copy of their child's educational record, even if the child does not wish them to access it. This applies until the child reaches the age of 18. A parent is not, however entitled to information that the school could not lawfully disclose to the child under the GDPR or in relation to which the child would have no right of access.

10 The danger behind Apple's good intentions

Surely we would all support and endorse Apple reporting traffic in extreme, illegal and criminal pornography?

Anything that puts a stop to such exploitation you might cry, though the vocal "freedom" merchants will seek to support "rights" – along with their guns probably.

Those are the obvious points, but there is a greater danger in the manner in which software must be written in order to detect illegal traffic from legal traffic. Put simply it has to open, read and analyse absolutely everything that you write, access and send in order to make an initial binary selection as being data that is either "good" or "not good".

You will follow immediately that anything in the "not good" selection then has to be passed through further analytics and processing to decide how bad it is, and what to do about it. But consider - what is to stop Apple performing similar analytical processing on your "good" traffic? That's right, absolutely nothing, so they are going to market your data for all its worth, and that could be a very great deal.

It is true of any "exemption" software, take the facial recognition element of Facebook, which you are able to opt out of. However, in order to exclude any use of your image, they must first store and record what your image is, and then compare it with the exclusion database. So they cannot use it to tell you that you are in a picture posted by a friend, but what stops them using that information internally for their own purposes? You know the answer again.

Clearly the very savvy marketers of all these social media organisations focus on what might be perceived as the social good that they are doing, but we should not be deceived. What they are actually saying is that we can analyse absolutely everything about your life, your image, your wants and your desires. You can "opt out" of certain uses we may put that data to, but we remain all knowing, all powerful.

Against this largely American reality, consider the initial brilliance of those who drafted the original GDPR – where they made opting out illegal; you have to actively opt in for consent to be valid. That changes the nature of the control of data, now you are only allowed to hold it if I have consented – as opposed to your having the information but not being able to use it in a certain way.

Then, when we applaud Apple for taking action against the worst abusers we might recall who it was that created the opportunity in the first place, and how rich they have become through exploiting it.

11 Students are cyber targets

It was such a tiny article, hidden away in the corner of The Times, written by their Education Editor, Nicola Woolcock, but it contained information of extreme concern and importance to every school. Most particularly anybody involved in any element of data awareness should be actively considering the threat.

We will reproduce the article in full and then comment.

"Universities are being warned about hackers mimicking their websites to dupe students.

The standards watchdog, The Quality Assurance Agency for Higher Education, said the sector was also dealing with a spike in ransomware attacks that use mass disruption as leverage for distortion or blackmail.

The latest threat comes from essay mills, or contract cheating websites, which complete work for students. The watchdog said that criminals were hacking university websites and putting in links that appear to be legitimate and relate to university services. But they contain hyperlinks to contract cheating websites or genuine links that have been hijacked.

It said this activity had been picked up at American and Australian institutions and that similar tactics were expected in the UK."

Indeed, we knew about ransomware, and you can bet they will target schools as well as universities, so the message is please to immediately review any links or connections that you have authorised to your own website. Reverting back to where we started this update, to point 1 a) – you must be in absolute control of anything connected to you and if it is a third party link that might be hijacked or faked, do you remain content to take that risk?

We believe that the article deserved greater prominence.

O Urgent Data Risk Warning – September 2021

Please be advised that there is immediate risk to your data from a known Microsoft vulnerability which nevertheless remains unpatched. It is currently being exploited by criminal elements creating ransomware attacks. There are two immediate impacts.

The first is that you must stop using any centralised print server that you are currently relying upon. We recognise that could cause considerable problems, but it is currently the path that is being exploited and we have no other "lock" for it.

Secondly, if you have not already done so, you MUST have an entirely separate and independent copy of your data – a snapshot taken at a specific date – stored OFF your network. What this gives you is a history file to refer back to WHEN (not IF) a ransomware attacker deletes your backups online. Of course you will still lose current data, anything after the snapshot, but you do not lose everything.

We provide further information below that is the best state of knowledge we currently have, but you will be hearing of schools being successfully attacked all over the Country, with major impacts in both Kent and on the Isle of Wight. You must act please, all it takes is somebody falling for a "phishing" attack (and they are increasingly clever at goading people into clicking on a link) and you are done for.

You might well consider instructing staff never to click on a link in the meantime. Even if it appears to be the Local Authority, ensure that more than one person looks at it to ensure it is genuine please.

In one instance the attackers have been identified as a group calling themselves 'Vice Society'.

Further information on their activities is available online via the Cisco Talos security group: Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Vice Society Leverages PrintNightmare

In all likelihood, access was gained via the academies remote desktop system via stolen credentials. It's possible that these will have been sourced via a phishing attack which any member of staff could have fallen victim to or reuse of academy credentials on another web site which was itself hacked.

Since students also have access to this service, it is also possible credentials have been inappropriately shared by someone.

Once on the remote desktop server, albeit with very limited access, the attackers were able to elevate their level of privilege via a vulnerability in the Windows

printing subsystem (known as 'Print Nightmare') to run their own software with administrative levels of access. It's well documented that various patches have been released by Microsoft to attempt to patch this vulnerability but it has remained the case that it can still be leveraged. The print set-up at xxxx was vulnerable to such an attack in such a way that couldn't (at the time of the attack) be patched.

P Satswana Update October 2021

Contents

1 Phishing

"Congratulations you have been selected to enter an Amazon experience survey, click here to start". Great, except when you look at the sender it is not Amazon, it is yet another very clever phishing tactic to catch you off guard. Two rules, first, never click on anything. Second, no really, never click on anything – because even if it did say Amazon, then it could have been a spoofed address. We are very sorry, but the landscape has changed, you cannot trust email.

2 Guild

https://guild.co/ is a UK business advertising itself as an advertisement free alternative to Whatsapp, and we are trying it as "Satswana Customer Group". If you would like to experiment with us and try it, please feel free. If it can reasonably and logically replace some of your email traffic, then that has to be what we are all looking for.

3 A further briefing for Governors

To remind you please that we have a long form here Satswana report to Governors 2021.pdf, and also that we request that at least the Governor / Trustee responsible for GDPR/DPA is provided with a copy of our updates. But the Head of one Trust asked for a short version in bullet point format. In case that suits you as well, here it is:-

- The greatest risk to data flows from email, with 94% of attacks stemming from a phishing exploit. Because email is fundamentally insecure we must all find an alternative means of communication wherever possible. If you click on a link in an email that is compromised then it will give criminals access to your server.
- The most serious consequence of an exploit is the encryption of data known as ransomware. Whilst deploying active protection we must also concentrate on 'BCDR', business continuity and disaster recovery procedures. Because you cannot pay it takes a long time to rebuild an infected IT structure, and that assumes you have a backup you can use, otherwise you will lose all your data.
- There is a sub culture of "campaigning" websites that encourage parents to claim perceived rights, often taking the form of subject access requests or freedom of information act requests. Within guidance that was effective from 1/1/21 Trustees and Governors are encouraged to be aware of the burden this imposes on staff. It may be low in absolute percentage terms, but Satswana describes this as "parent risk", because it can lead to very aggressive behaviour, which in turn is distressing and stressful to staff, with both complaints procedures and references to the ICO being deployed as weapons. The resulting mental health risk to staff flows from the perceived requirement to support the rights of an applicant, but those must be more actively balanced by the parallel rights of the respondent. Satswana would say that the health of educational staff should be the paramount concern.
- Trustees and Governors are considered to be responsible for "Cyber Security" and (again with effect from 1/1/21) guidance described this as being "information management". Both terms are so broad, with many layers of underlying detail, that comprehension without considerable study cannot be expected. For this reason it was recommended that nominees within the Board became DPA (GDPR) specialists, and they will discover that the IT structures within education are all very dated – thus vulnerable and inefficient. There has to be a comprehensive movement towards the aim of "privacy by design and default". That will impose two new burdens on the leadership in education, both of which will be generally unwelcome additions to their already considerable duties. One is a concentration on what the IT requirements are for the future – and you cannot rely on current suppliers to initiate this. Secondly it will be to adopt the change that their conclusions dictate. However that fundamentally is what is meant by "information

management" within a DPA context, and the leadership in education will require considerable support and encouragement to advance it.

- It is the duty of the DPO to the Trust to be actively involved in the promotion of change as required by the Data Protection Act and to advise on the impact on the institution.
- These major points should not obfuscate the daily detail required to ensure data is appropriately protected, whether in digital or paper form. Also that the physical security of the premises is properly considered. Staff must be trained to be continuously aware of the responsibilities now placed on them by regulation.

4 Data sharing agreements, again

Hopefully you will have noted our objection to data sharing agreements, and the piece following this one was written in order to assist understanding. However, since it was written we discovered the following article in the magazine dedicated to Further Education

https://feweek.co.uk/dfe-broke-student-data-protection-laws-damning-ico-audit-reveals/

We did not expect our fears and worries to be so comprehensively supported by an ICO report on the data handling of the DfE, but it is a "must read".

The fundamental problem is that probably very well meaning and decent people have simply not come to terms with the change in culture dictated by the return of the ownership of personal data to the individual within GDPR 2016, and now reinforced by DPA 2018. Too many support organisations still expect to be "given" data by schools without the consent of the data owner, often disguised as a "data sharing agreement".

You simply must not supply anything to anybody without the "specific consent" of the data owner for the "specific purpose", and all parties must adjust to what that means.

5 FE, the conflict between intent and reality

(Information for this article was gleaned from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1002972/Careers_statutory_guidance.pdf)

Without exception we would all support the objectives of careers guidance and further education, yet there are three absolute collision points with data protection that have the same nature as being between a rock and a hard place.

Sorting the issue out is not helped by frequent references in documentation to "statutory guidance", for there can be no such thing. It is either a matter of statute, in which case the requirement is defined in law or it is guidance – to be followed or not as being appropriate to the decisions of the executive involved.

The first "collision" is where schools are required to "maintain accurate data for at least three years after they leave school". That involves the processing of personal data "for which schools need to satisfy themselves they have the proper legal basis." There can be only one legal basis in our submission, and that is consent. Whether their reasons are good or not are not part of this subject, but suffice it to say that many students will refuse their consent, and that creates an impasse.

The second "collision" is where schools must comply with the (now statutory, since 2/1/18) Baker Clause which allows vocational training and apprenticeship providers to advertise their courses in school. In Satswana's experience this has led to distinct opportunism from all sorts of providers, often within the recruitment spectrum. They interpret it as an opportunity to demand what we consider to be an inappropriate "data sharing agreement" that includes a clause giving them the right to be a controller. We state that they are not, they are a processor at best, and that the school is the controller, meaning that all that is required is an acceptable privacy policy. Our analysis of the legal "mumbo jumbo" that is produced suggests that the data sharing agreement is just a device to circumvent the consent of the individual, and we caution against entering into them.

The third collision in data terms is probably the most dangerous of all in the context of data privacy, and that is where those seeking access to your data wish to do so by automated means, Compass + being an example. It is Satswana's data protection objective to campaign against any third party access to any computer holding personal data.

May we please repeat our absolute support for career planning, but how does a school comply with its statutory duty under Section 72 of the Education and Skills Act 2008 (to provide information to local authority services) if the student does not consent under DPA 2018? Section 13 is probably even more of a problem, because students believe that this notification would affect their benefits (and it probably does).

Possibly of even greater concern would be Ofsted's view, since the subject is noted as being one of the key areas that informs inspector's overall judgements on personal development.

You are truly "between a rock and a hard place".

6 What does "IT" do?

To most of us they talk a totally foreign language, and indeed they do, their expertise is based around very specific engineering training that requires very strong technical knowledge and considerable experience in implementation.

To get an insight into it, you may wish to watch the video we reproduce below regarding the installation of a Smoothwall firewall. It is only 3 minutes (once you get past the ads) but it will give you an awareness of what they are doing. It will not lead to understanding, but will certainly assist appreciation.

Smoothwall https://www.youtube.com/watch?v=1uX4Nao1WbI

7 Can you help the police?

The relevant words are:-

"Organisations should remain confident that when asked for personal data to assist the police whether in an emergency, or in their ongoing community policing activities, ***necessary, relevant and proportionate data*** can be disclosed in compliance with the law". (Satswana italics!)

So our reading is that if it is both relevant and proportionate, it is OK.

However we do also always counsel caution, because in our experience the Police never voluntarily recognise the boundaries of powers that they are given!

8 Dealing with abuse

You will be well aware that this subject is receiving a great deal more attention, and there are those better qualified than Satswana to comment.

However we noted that one of the key messages from one piece of research was *that 'even where school and college leaders do not have specific information that indicates sexual harassment and online sexual abuse are problems for their children and young people, they should act on the assumption that they are'.*

Furthermore it was stated that Inspectors will make this assumption too, so it is essential that schools have done their own internal review and have a plan for minimising the risks of abuse between peers.

It seems that a wholly new peril is attached now to the philosophical debate around proving a negative.

9 Our language

Did you know that 90% of the 300 Billion emails sent daily are in English? Not that it is the language of the British Isles per se; indeed we are only the sixth largest country in which English is a common language – after America, India, Pakistan, Nigeria and the Philippines. We apparently only generate 10% of the total mass of new English derived words employed around the world, a figure that is expected to drop to 3% by 2060!

10 Update on Print Nightmare

Bearing in mind that this was a bug which was first reported to Microsoft in December 2020 by a chap called Victor Mata from FusionX, of Accenture Security, and that we were told in August that there was a patch, it is troubling to note that there was a further patch in September indicating that systems were still vulnerable in August. Thus whether or not this is the final answer remains to be seen, but regardless it has caused problems for administrators who have to intervene to add any new device.

For more detailed information please visit here PrintNightmare: Admins left to fix network printing • The Register

11 How did it all happen?

This extract was taken from "How they tell me the world ends" by Nicole Perloth and explains why we have to spend our time being concerned with Cyber Security.

Zero day is a software bug that allows a hacker to break into your devices and move around undetected. One of the most coveted tools in a spy's arsenal, a zero day has the power to silently spy on your iPhone, dismantle the safety controls at a chemical plant, alter an election, and shut down the electricity grid (just ask Ukraine).

For decades, under cover of classification levels and non-disclosure agreements, the United States government became the world's dominant hoarder of zero days. US government agents paid top dollar—first thousands, and later millions of dollars—to hackers willing to sell their lock-picking code and their silence.

Then the United States lost control of its hoard and the market. Now those zero days are in the hands of hostile nations and mercenaries who do not care if your vote goes missing, your clean water is contaminated, or our nuclear plants melt down.

12 The internal risk

Satswana considers James Timpson (CEO of Timpson Group) to be an exceptional leader whose support of ex-offenders is inspirational.

In a recent article on risk he correctly identified that the risk from inappropriate activities of your own staff is at least as great as the external threat, and that is the reason for our reproducing his comments.

He pointed out that most internal theft issues (including data theft of course) results from things that go wrong in a person's life. Furthermore that can normally be traced to one of three causes, gambling, bad financial planning and drugs. He added that Timpson's can help with all of those, if they know about them, so they have a culture that encourages their staff to ask for help.

It made us wonder whether we had thought about the internal risk in the first place, and if so whether we had even considered keeping our eyes open for a problem, and probably failed on both counts. Almost certainly our culture would not be seen as one that allowed people to ask for help, and that caused considerable reflection.

If you find the same applies to you, then we will be doing our bit towards limiting the internal risk.

Q PRIVACY NOTICE FOR STAFF, GOVERNORS AND ROLE HOLDERS

'Staff' means employees, workers, agency staff and those retained on a temporary or permanent basis.

'Governors and Role Holders' includes, volunteers, contractors, agents, and other role holders within the School including former staff and former Governors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

'Personal data' is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the Data Protection Act 2018 (the "DPA") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by (Name) School which is the data controller for your data.

The School works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the School and our community. The organisations referred to above will sometimes be 'joint data controllers'. This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration

then the data controllers will be independent and will be individually responsible to you.

The School will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date/leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates,

immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;

- To administer Governors' interests
- To provide a reference.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

We may process sensitive personal data relating to staff, Governors and role holders including, as appropriate:

- information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
- your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties.

These types of data are described in the Data Protection Act 2018 as 'Special categories of data' and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.

We may process special categories of personal data in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the School including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or

where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The School is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. **The right to access personal data we hold on you**
   - At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
   - There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. **The right to correct and update the personal data we hold on you**
   - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. **The right to have your personal data erased**
   - If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
   - When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. **The right to object to processing of your personal data or to restrict it to certain purposes only**
   - You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. **The right to data portability**
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained**
   - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. **The right to lodge a complaint with the Information Commissioner's Office**.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page [add URL]. This Notice was last updated (on date)

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints contact our Data Protection Officer - Satswana Ltd, email info@satswana.com ; telephone number 01252 516898, Office address Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

satswana

Company registered number 09329065 www.satswana.com

R Satswana Update, November 2021

"Leadership is solving problems. The day soldiers stop bringing you their problems is the day you have stopped leading them" Colin Powell, My American Journey (1995)

Contents

1 Linking Policies?

As we constantly seek to stress, we benefit hugely from the interaction with our customers – firstly when we are asked a question, then when we identify a "best practise" solution, finally as a consequence of being able to share it with our community.

In this instance we were asked by a Trust for the impact of KCSIE 2021 on both the Data Protection Policy and the Staff Code of Conduct. After a great deal of research and reading back through linked legislation we came to the conclusion that it would be easy to run the risk of "over thinking" matters, not least because guidance states that "all staff who work with children ….must read either Part One or Annex A … of KCSIE 2021" – so the content is in there, reproduction would just be duplication.

However the Trust concerned did refer to four other policies within their (substantially standard) template Data Protection Policy, and we thought that it was an excellent idea to create cross linkage. For your consideration the four they used were:

Freedom of Information Act Policy and Publication Scheme
Child Protection Policy
Staff Code of Conduct
E-Safety Policy (Applicable use)

Within the Staff Code of Conduct there was an even more extensive list, demonstrating just how many policies you are expected to have, but crucially

including within the Staff Code, identification of their responsibility to read Annex 1 of KCSIE.

Once again we reproduce their list for your consideration, you may have different titles

This policy is linked to the following policies:

- Allegations of Abuse made Against Staff
- Anti-Fraud, Corruption and Bribery Policy
- Behaviour for Learning Policy (titled Behaviour Policy in Primaries)
- Child Protection Policy
- Complaints Policy
- Data Protection Policy
- Equality Policy
- E-Safety Policy
- Health and Safety Policy
- Information Systems Policy
- Intimate Care Policy (TLAP & TLHP)
- Physical Restraint and Reasonable Force Policy (TLA)
- Sex and Relationship Policy
- Staff Discipline Policy
- Staff Dress Code Policy
- Trips and Visits Policy
- Whistleblowing Policy

What we then identified was that these were excellent and appropriate documents that dealt comprehensively with any issues between adult and student. However, please read next subject.

2 Handling new KCSIE requirements

What these policies did not do, and as far as we have been able to determine, nothing else does, is to cater for what might be regarded as an entirely new responsibility to manage the inter student issues that have been added into KCSIE 2021.

If we may remind you, we identified the following within our October update:-

We noted that one of the key messages from one piece of research was *that 'even where school and college leaders do not have specific information that indicates sexual harassment and online sexual abuse are problems for their children and young people, they should act on the assumption that they are'.*

Furthermore it was stated that Inspectors will make this assumption too, *so it is essential that schools have done their own internal review and have a plan for minimising the risks of abuse between peers.*

To our mind that is a wholly new "data impact" of KCSIE that needs to be considered, not least because it is inevitable that any management of the issue will require a record – which in turn would be extraordinarily sensitive – and very dangerous content in terms of any access request.

We think that this is such a big issue that it requires discussion amongst Principals on the various forums to arrive at an approach that meets the requirement. From a DPA point of view we can provide thoughts on the use of relevant exemptions to ensure that a recorded "suspicion" is protected from disclosure, but suggest that it requires an entirely new storage methodology linked to specific management of the subject (probably not the pupil record?). Two things must be clear. Firstly all children in the care of a school will be subject to an emerging understanding and exposure to their sexual being, and secondly that is always likely to lead to trauma of some sort or other. Is it now the implication within KCSIE that schools have a responsibility to monitor that? At what point would intervention be considered? How do you manage and record such a requirement? How are staff trained to manage it? Whatever - it is "data" that must be controlled and a "policy" should exist to cover it. Furthermore we must prove to Ofsted that we are reviewing it with the purpose of creating a plan.

This is not the end of the story.

3 Biometrics use for school meals

The Daily Mail made headlines, as is their wont, as a result of schools in Scotland adopting facial recognition to identify and bill children for their school meals. Apparently they found it to be a very quick and accurate means of control. Of course the piece was classic journalism, but except for the fact that some people are influenced by the headlines, you should not concern yourself with their scare talk.

May we make two points? Firstly Facial Recognition Technology is Biometrics. To a computer identifying a fingerprint or a face is identical in practise – it relies on comparing a stored and known image with the one presented to it, and confirming the identity from various points that it measures. Fundamentally it is just maths.

Secondly, you are using it within a single purpose in a closed user group community, so it is not in any sense "public". (Clearly it gets much more emotive if used by Police to identify a criminal in a crowd, but that absolutely does not apply.)

Thus the use of FRT for either surveillance or marketing use could not be further from your mind.

You are deploying it as a legitimate business interest to effectively control canteen management and processing.

Also you are likely to have requested consent for biometrics, which still applies, but is not essential given the consent basis above.

So this inflammatory nonsense has to be kept in perspective, but that will never make a headline!

As a postscript, you may have noted that Facebook are recanting from their emphasis on facial recognition. That should be taken with a large pinch of salt, since as previously explained – even if it is not used you have to retain the processing to know you are excluding it. The absolute and total risk from social media which has been exposed so recently remains.

4 CPOMS purchase by Raptor Technology

Many users of CPOMS wrote to express concern at the notification that they had been purchased by Raptor Technologies, an American Company.

At first sight we don't believe that there is any reason for immediate concern, CPOMS almost certainly will continue to operate within the UK and under the control of the ICO. If they seek to change the location of their servers, or any aspect of their privacy policy, then we will all have to consider our position.

Raptor appears to be just a visitor/volunteer/Emergency management system, and they have probably bought CPOMS to provide a more mature product to their US base, but also of course they will try to sell their visitor system in the UK to CPOMS customers.

Such an expectation is most disappointing, since we regard that as a cul de sac – it does absolutely nothing to shake up the legacy providers of multiple and disconnected software that education is expected to fight with (and pay over the odds for.)

Once again (as with The Key buying Arbor, and SIMS going into the hands of venture capitalists) we see organisations seeking to perpetuate the divisions in software, rather than working towards an operational consolidation. That may increase their revenues in the short term, but they are exposed to anybody who sensibly invests in a modern support product that embraces all the requirements in one package.

We continue to seek that option for our customers and hope that it will be available to you well before CPOMS in American hands becomes a problem!

5 What do you transfer to a Secondary?

As you will hopefully be aware we love questions and received this one the other day in the context of whether anything had to be edited before it was sent, answering it as below. If we have got anything wrong, or missed anything out, then please let us know!

Generally there are three aspects that make up this data. The first is the "Common Transfer File" (CTF) that will automatically transfer your MIS data that you received as "admissions" information initially, but updated over time to the new school. That may include pupil information that has been entered by staff, and that knowledge may be useful to the next school. Because it is all staying within the educational "community of interest", we do not think you have to edit any of that.

The second is any SEN based information which may be in all sorts of forms, but that should be gathered together and hand delivered to the SENCO at the new school, with a signature for its receipt obtained please. Hopefully this will not involve too many schools to visit, and of course you can parcel them up together for each secondary. If you are using CPOMS or MyConcern (or some other digital storage) you might have to agree with the Secondary as to how they wish to receive that information. (If you use USB or similar, it MUST be encrypted!)

You will then be left with the general detritus of several years of engagement with the child and family, happy memories possibly, but redundant now, and (as the questioner correctly suggested to us) irrelevant to the next school. They will not want that, and we recommend that it is securely shredded once you are sure you have no further interest in it. Similarly, once transferred, you can (and must actually) delete all the old records.

The only exception to this that might make you consider keeping something is if there has been a dispute with the parents, an argument over EHCP, or similar. Then you might consider keeping any vital bits of evidence "in case" – in a bottom drawer, hopefully never to be looked at.

6 Five things to ask suppliers before making a change

With the CPOMS transaction in mind we found this article published on July 8, 2020 by Phil Sanders, Director at PM Sanders Consulting Ltd. and in a subsequent discussion further found a knowledgeable support resource. However we have not persuaded him yet to invest in creating a "Satswana" compliant product! This is a precis of his article.

"With the announcement of the sale of Capita's ESS business it seemed a good time to look at the current UK (excluding Scotland) school MIS vendor landscape.

Over the last three years Capita's dominant market share with SIMS has remained resilient and according to DfE census data has dropped by only 5% to 75% for all schools between 2017 - 19. Opinions vary but delays in the release of next gen SIMS8, future uncertainty with the ESS sale and increasing competition from cloud-based vendors may mean more institutions will consider going out to market.

In a recent broadcast interview with SIMS former Managing Director and creator Phil Neal, he talks about the questions that Multi-Academy Trust (MAT) leaders should be asking MIS suppliers if they are considering a change of system.

1. ***System security*** – with sensitive personal data at stake, how secure is the software, can the supplier provide evidence of regular penetration testing?

2. ***Financial security*** – will they be around for the long term? Can a supplier with 1,000 schools be financially viable, without requiring substantial investor support to fund new software development and testing?

3. ***Access to data in the cloud*** – if a supplier did go bust, what would happen to the data that is in their cloud? MIS suppliers are paying for the cloud directly, if a supplier stops paying their cloud supplier, how long will that data remain available for the MAT/school to use? How will they facilitate getting the data out of the cloud to the next MIS supplier and what control will the MAT have?

4. ***User involvement in the procurement process*** – involve the right balance of technical people and businesspeople in the process, ask users to clearly articulate and then verify functionality they require to meet their needs.

5. ***Test supplier claims*** – challenge the supplier, ask to see evidence of achievable savings, check there's access to equivalent functionality to the current system. Trial functionality in a hands-on workshop environment and make key user features part of the acceptance testing – especially for secondary schools where requirements are more demanding. Ask what business continuity measures the supplier has in place.

7 Business email compromise (BEC)

Thanks solely to the caution of an alert member of staff one of our schools avoided falling for a criminal payment request from a "spoofed" school email address.

On the technical DPO front, since there had been no loss as a result of the attack then there is no further "risk to persons" and thus we did not have to report what is a clear breach to the ICO.

On the computing front, it was an absolutely classic case of "business email compromise" – BEC as an acronym – and it is enabled by all the fundamental security issues that are endemic within email. The IP address they identified had "spoofed" an account and as such would have bypassed any Multi Factor Authentication. The absolute and brutal reality is that you cannot make email secure – and only staff awareness is a protection against this criminal activity.

It is just possible that the attackers managed to get somebody to click on a "phishing" link – or had a "man in the middle" access (normally through the use of insecure wifi)- and for that reason if you are attacked it would be wise to change all user passwords and have a look around any available network logs, you might see an access you do not recognise.

But beyond that there is very little you can do, as we have to constantly point out the security issues within email date back to the original authors in the 70's who only thought about the brilliance of communication and in those days were not troubled by security. Email has to be phased out over time in favour of communication through Teams for instance, and nobody should ever click on a link in an email, even if it is from a friend they know. (What easier way of distributing a virus than through a "joke" that you know people will pass on?) SEND documents should be encrypted either using Outlook 365 or Egress.

The FBI describes BEC as being "one of the most financially damaging online crimes".

8 Comparing PIPL and GDPR

It is quite remarkable how GDPR has influenced international thinking regarding data privacy, with the only unfortunate exception being the United States where they are still gated by their First Amendment. Thus as a final offering for your amusement we reproduce below a comparison between GDPR and the Chinese equivalent (Personal information protection law)!

Similarities between the PIPL and GDPR include:

- Both the PIPL and GDPR are extra territorial.
- The PIPL and GDPR define personal data as involving identified and identifiable natural persons.
- The PIPL uses the GDPR's lawful basis approach to data processing. Many other Asian privacy laws use the consent-based approach or an approach akin to the US approach of notice-and-choice.
- Both the PIPL and GDPR have special protections for sensitive data, but they differ on the types of data they recognize as sensitive.
- Both the PIPL and GDPR have a data breach notification requirement.
- The PIPL and GDPR recognize many of the same rights.
- Both the PIPL and GDPR require workforce training.

- Under certain circumstances, both the PIPL and GDPR require DPOs.
- Both the PIPL and GDPR require data protection impact assessments (DPIAs) in certain situations.

Differences between the PIPL and GDPR include:

- The PIPL has no lawful basis of legitimate purposes, which the GDPR recognizes.
- The PIPL uses some different terminology than the GDPR. GDPR "data subjects" are called "individuals" under the PIPL. GDPR "data controllers" are called "personal information handlers" under the PIPL. GDPR "data processors" are referred to as "entrusted parties" under the PIPL.
- The PIPL has a strong data localization requirement.
- The PIPL recognizes a few different types of sensitive data than the GDPR. For example, financial data is sensitive under the PIPL but not under the GDPR.
- The PIPL has a post-mortem right for personal data after death.
- The PIPL requires a representative in China for foreign data handlers.
- The PIPL has less stringent requirements for cross-border data transfer than the GDPR.
- Under the PIPL, data breach notification must be "immediate" without the GDPR's specific 72-hour deadline.
- The PIPL has a prohibition on personnel responsible for violations from holding high-level management or DPO positions.
- The PIPL has fines up to 5% of annual revenue. The GDPR has fines of 2% and 4% of annual revenue. The GDPR looks to worldwide annual revenue; the PIPL is unclear about whether the fine is based on annual revenue in China or worldwide annual revenue.

The most interesting one to Satswana is the post mortem right to data, since we believe that your "history" has to be maintained in an increasingly online world to avoid a future "digital dark age".

S Supplement to exemptions

1 Supplement to exemptions

This supplement is produced by Satswana following consideration of legal advice given to one of our schools with additional exemptions. It is our belief that Satswana now has considerable practical experience in dealing with requests of all kinds and we have considerable awareness of the determination arrived at by the ICO in given circumstances. Thus we believe that where the letter of the law must be considered, there is also the spirit of the law which involves interpretation. Indeed it is this interpretation that leads to the precedents and case law that make up English Law.

There can be no dispute as to what the law actually says, only how it is applied and the following supplement indicates how Satswana believes that life can be made easier for respondents.

2 What constitutes personal data?

Very often an applicant will be using a SAR in order to seek evidence and will have been led to believe that it is their "right" to receive "everything" that has ever been said about them, but anybody, to anybody else. Satswana seeks to take a narrow view of personal data and have used "the rights of others" and the University of Worcester precedent to exempt much of the contentious commentary that might be difficult or embarrassing if taken out of context.

Let us be aware of what a strict reading of the law might advise.

Information must do more than simply identify an individual to constitute personal data; it must relate to that individual. i.e. it must "concern" the individual in some way. The practical consequence of this is that data can reference an individual and yet not amount to their personal data because it doesn't actually concern them. To help decide whether data "relates" to an individual you need to consider

(i) the content of the data i.e. is it about the individual?
(ii) what is the purpose for which the data is being processed? and
(iii) will the individual be impacted by the processing in any material way?

Pseudonymised data is not the same as anonymised data. GDPR does not apply to personal data that has been truly anonymised i.e. information that does not relate to an identified or identifiable individual. Consequently, anonymised data will fall outside the scope of any SAR.

The test is, if you could at any point use any reasonably available means to re-identify the individuals, then the data will not have been successfully anonymised but will only have been pseudonymised.

The GDPR singles out some types of personal data ("Special Category Data") as more sensitive, and gives them extra protection. This is because use of this type of data is more likely to interfere with a person's fundamental rights or open someone up to discrimination.

For the avoidance of doubt, the special categories of personal data are where the information pertains to:

• the racial or ethnic origin of the data subject;

• their political opinions;

• their religious beliefs or other beliefs of a similar nature

• whether the data subject is a member of a trade union;

• the data subject's genetic data;
• biometric data for the purpose of uniquely identifying the data subject;

• data concerning health; or

• data concerning a data subject's sex life or sexual orientation.

Information about criminal allegations, proceedings or convictions does not fall within the definition of Special Category Data, however additional safeguards apply in relation to the same.

Once a person dies information about them ceases to be personal data for the purpose of the GDPR

(Satswana comment) As will be seen "the Law" is necessarily fairly general as it seeks to cover a wide range of options, we believe we are correct to offer less, not more.

3 Application of Exemptions

Thus it is established that In general, a requestor will not be entitled to information that is not their personal data. For example, they would not be entitled access to general business information about the running of your organisation or personal data about other people or any information that falls under an exemption as set out in the DPA. We now set out these additional exemptions to our Chapter C.

a) Third party personal data (Paragraph 16 of Part 3, Schedule 2, Data Protection Act 2018)

Under GDPR, a student is only entitled to request their own personal data. They have no automatic legal right of access to information that identifies anyone else such as another student (third party personal data).

Information that relates solely to another individuals' personal data will fall outside the scope of the SAR. For example, if a student makes a SAR for the biology assessment grade of another student, this can be refused on the basis that the requestor has no legal right of access to personal data that relates solely to another person.

However, sometimes responding to a SAR necessarily involves providing information that relates to both the requestor and another individual, i.e. where personal data relating to the requestor and the other individual are "co-mingled". This could happen where teachers document a discussion on the ranking of two or more students.

If you receive a SAR that would require you to disclose personal data that relates to both the requestor and also another person (a third party), the DPA provides an exemption that aims to balance the privacy rights that you owe to the third party against the requestor's right of access.

The third party personal data exemption only applies where the requested information also includes the personal data of the third party. The exemption works in the following way:

The general rule is that a SAR only covers information held in respect of a requestor, and third-party personal data is exempt from disclosure unless either:

• The third party has consented to the disclosure of their information; or,
• It is reasonable to disclose the information to the requestor without the consent of the third-party.

In determining whether it is reasonable to disclose third party personal data, an education establishment must have regard to all of the relevant circumstances, including:

• The type of information;
• Any duty of confidentiality owed to the other individual
• Any steps taken to seek consent and whether consent has been refused;
• Whether the third party is capable of giving consent; and

• Any express refusal of consent by the third-party.

Therefore, whether third party personal information may be disclosed needs to be decided on a case-by-case basis. This decision involves balancing the requestor's legal right of access against the third party's rights in respect of their own personal data. For example, where consent is provided, you may disclose the third party's personal data to a requestor. If consent is not forthcoming, then you must decide whether it is reasonable to disclose by considering the above factors.

In respect of any documentation included within a SAR that includes third party data, the ICO will expect you to first consider whether the information requested may be supplied, redacting any information that would identify the third party individual. For the avoidance of doubt, the information that should be redacted may be more than just the third party individual's name, as other information included could make the individual identifiable.

If the only way to withhold third party data is to refuse to disclose the whole document, then you will need to be able to justify that decision.

b) Assumption of reasonableness: Education-related workers

We have been considering how to deal with SARs that involve third party personal data where the relevant third party is another student. Where personal data relating to a teacher or other professional that falls within the definition of 'education-related worker' is mixed with the requestor's personal data, the position is different:

Under the DPA, it is assumed to be reasonable to disclose third-party personal data to a requestor without the consent of that third party where the individual concerned meets the education data test. An education-related worker is defined widely, and includes teaching staff, employees of an educational authority other than a teacher, such as a member of an academy trust's internal HR team, and any educational psychologist engaged under a contract for services.

On this basis, where the personal data of the requestor and the personal data of an education-related worker are mixed, the starting point would be to assume that disclosure of the education-related worker's information may be disclosed. In order to withhold this information, it is necessary to show that the presumption of reasonableness does not apply by showing that it is unreasonable in the circumstances to disclose.

As detailed above, whether it is reasonable to disclose personal data about an education-related worker depends on a range of factors, and information must be considered in full, taking account of all of the relevant circumstances. For example, it may be reasonable to include the names / roles / email addresses of an academy

trust's employees who are identified in documents where they are acting in their professional capacity. However, if information of a purely personal nature is included in the documents, then it may be reasonable to redact or withhold that information.

c) Exam scripts and exam marks (Paragraph 25 of Part 4, Schedule 2, Data Protection Act 2018)

This exemption applies to personal data contained within exam scripts, exam marks or other information processed by a controller for the purposes of determining exam results.

This means that candidates do not have the right to obtain copies of their exam answers. However, any information recorded by the controller (specifically for the purposes of determining exam results or in consequence of determining results) is not exempt. However, where a SAR is made for this information, special time limits apply:

Where a SAR is submitted before publication of results, information must be provided:
• within five months of receiving the request; or
• within 40 days of the announcement the exam results (if this is earlier).
In the context of this exemption, the term "exam" is broadly defined to include "an academic, professional or other examination used for determining the knowledge, intelligence, skill or ability of the candidate."

This year, students will not actually be sitting exams and so strictly speaking there will be no exam scripts. This exemption would however still be likely to apply to SARs specifically in relation to information about how grades and rankings were determined. On this basis, if a request is submitted before the day on which the exam results are announced then the response to the requestor should note the specific time limits that apply.

Please note, if a SAR is submitted after the publication of results, the usual statutory timescales will apply. i.e. the SAR will need to be complied within one calendar month.

d) Legal professional privilege ("LPP") (Paragraph 19 of Part 3, Schedule 2, Data Protection Act 2018.

It is the practice of Satswana to make a liberal interpretation of the use of LPP, including for example exempting discussions that may be about a tribunal.

A strict reading of the law says communications between an educational institution and their legal advisors may also be exempt from disclosure. Specifically, the DPA

provides an exemption from the right of access in relation to personal data that consists of:

(a) information for which a claim to LPP could be maintained in legal proceedings, or
(b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser.

This means that information that attracts LPP as well as other confidential information provided by or sent to a professional legal advisor would fall within the scope of the exemption. The most common forms of LPP are as follows:

e) Legal Advice Privilege

This applies to confidential communications that pass between a client and the client's legal advisor; and which have come into existence for the purpose of giving or receiving legal advice about what should prudently and sensibly be done in the relevant legal context. For instance, this will apply in relation to correspondence between an educational institution and its legal advisor(s) that contains legal advice, and documents recording confidential communications, including, for example, notes taken at meetings.

f) Litigation Privilege

This applies in relation to confidential communications (1) between a legal advisor and a third party/between a client and a third party; (2) which have come into existence after litigation is contemplated or commenced; and (3) have been made with a view to the litigation, either for the sole or dominant purpose of obtaining or giving advice in regard to it, or for obtaining evidence to be used in it.

In order to establish whether litigation privilege applies there are three key questions to consider:

(1) Who created the document? i.e. was it a lawyer, the school/college or a third party (such as an expert witness) (Satswana note: it is not just legally qualified people who can give advice that falls under legal privilege, the Police for instance might do so, as would a DPO.)

(2) When was the document created? i.e. was this after litigation was contemplated or commenced?

(3) Why was the document produced? i.e. was it for the sole or dominant purpose of litigation?