Consolidation of Update notices from 2020, edited November 2021

(Note please that items may now be historical, whilst referring to Brexit for instance)

satswana

Company registered number 09329065 www.satswana.com

A Winter Update 2020

Index

1 Data Protection Fees

Candidly these are annoying – but even more tedious if you have either a dormant or exempt Limited Company, as many might have for various reasons. From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 require every organisation and business (including sole traders and partnerships) processing personal data to pay a data protection fee to the ICO, unless they are exempt. Schools clearly fall into this category, but every limited company is getting a letter from the ICO that you must not ignore, otherwise they will assume you are a defaulter. Go to the website please and tell them you are exempt or not trading!

2 Request for a copy of an incident on CCTV?

Some thoughts regarding what your response should be following a query from a customer.

The first question was whether or not this should be regarded as a subject access request. We felt not, because it was entirely specific to a nominated event and a singular instance of content, indeed since an employee was injured we felt that it was not so much GDPR as Health and Safety, indeed perhaps safeguarding.

We record video for security, safety and reputational purposes, so if an event occurs that requires study, then is it totally appropriate that the image is used to identify – possibly in this case an assailant?

Indeed do we suggest that as a matter of pastoral care somebody should establish whether there is a continuing issue and determine what the information is needed for? The image would be regarded as the copyright of the School, so you would have to consent for its use in any other application, for an insurance claim for instance.

It will be your decision as to whether it is appropriate to provide a copy.

3 Renewing your HTTPS certificate

Satswana promotes that all our customers websites should be protected by the security certificate that appears as HTTPS instead of HTTP, not least because most browsers these days will state that access is insecure if it is not protected.

So it was really embarrassing the other day when we realised that our own certificate had not been renewed and our website was being flagged as insecure as a consequence. Red faces for us, and lesson learned to be passed on! Please make sure that your certificates are renewed in time!

4 Windows 7 Support

Support for this much loved version ceased on January 14th, so if you are still to change then you really now have to bite the bullet. For those of us who have always hated finding our way around a new release you will be pleased to know that Windows 10 will be incrementally upgraded online, so changes will always be small and you will not have to go through the trauma again!

5 ICO Decision

One of the protections for a public authority from a subject access request is when we can respond that the request is "a manifestly unjustified, inappropriate or improper use of a formal procedure". The almost knee jerk reaction of the applicant is to make a complaint to the ICO. Satswana does not relish being complained about, and we can never be certain of the outcome, so it was comforting the other day to receive a determination that said "I can see that you are relying on section 14 of the act to refuse Mr xxxx request, which you are within your rights to do so."

6 ICO accountability principles

Whilst on the subject of the ICO they recently published "accountability" guidance as a number of principles, reproduced as follows:-

a) Implementing data protection policies;

b) Recording your processing;

c) Taking a data protection by design and by default approach;

d) Having written contracts in place with processors;

e) Implementing appropriate security measures;

f) Recording and, where necessary, reporting data breaches;

g) Appointing a data protection officer;

h) Establishing processes for handling data subject rights' requests; and

i) Carrying out data protection impact assessments.

We feel that all Satswana customers will be able to tick off their compliance with all of these. d) is specifically covered by our provision of approved processor lists, please let us know if you need a copy of this document.

7 Ricoh, or ricochet?

Satswana were somewhat appalled when a customer decided to change their photocopier and received a pretty naked attempt to extort a significant fee from them, starting with the statement "Did you know there are numerous areas within our equipment that store data?" They then referred to the DPA 1998 as justification for a "service" to remove the data. If you are faced with this, please reflect that under DPA 2018 all processors must contract with data controllers to manage personal data, and if a contract ceases they must delete it. The school concerned responded appropriately sharply!

Fact is that many items of modern equipment are installed with hard drives, or other means of storing data, and thought has to be given to what happens to the data when you decide to dispose of them.

8 Password templates

It was a clever question, "can we offer something as a template for passwords", and it made us think! This is how we responded!

If you want the full nine yards can we refer you to the NCSC website here https://www.ncsc.gov.uk/collection/passwords

But the current "short form" advice would be to use a password that you can easily remember, but which is complex in its construction so it cannot be attacked with what is described as "brute force".

One approach might be to use a phrase that has meaning to you, such as yellow boat. If you then put a number in front of it, and capitalise the first letter, you get a pretty strong password.

Add a special character at the end (such as an exclamation mark) and it becomes even stronger. In this example it becomes 1Yellowboat!

Recent opinion has favoured sticking to a password that you do not have to write down, rather than the former advice to change it frequently.

Sadly there are examples of passwords becoming compromised, and it is not only wise to then change them, but also not to use the same one in every program.

But if you change them around something that you are familiar with, then that becomes less of an issue. Thus 2Yellowboat! Is different, as is 1Blueboat!

The important thing is that it should be complex enough, and yet memorable to you – in a manner that a third party will not guess.

So, in our example, do not have a blog about sailing your yellow boat!!

9 Something completely different

Absolutely nothing to do with GDPR, but if we have navigated that successfully, can we also navigate by the stars? Thanks to an inspiring "Sky at night" programme may we bring you the North Star, otherwise known as Polaris, and to be discovered by following the two stars at the opposite end of the "handle" of the Plough.

Three fabulous facts, the first being that Polaris is always due North wherever you are in the Northern Hemisphere. Secondly, the angle between you and the star is your Latitude! Finally, because all the stars appear to revolve (anti-clockwise) around Polaris – of course it is actually the Earth that is spinning – the constellation known as the Plough moves around it as a back to front clock.

So next time you are gazing up at the stars you can tell your direction, position and the time. It is a wonderful world!

Contents of this document are the Copyright of Satswana Ltd 2021 ©

B Satswana Spring update

Contents

1 Satchel One, change of compliance status

We have downgraded the above to Category C within our Processor list following a complaint from a customer regarding their misuse of data. Fundamentally that means that we do not consider them to be fully compliant with the requirements of DPA 2018.

The error itself is not the reason for the downgrade, mistakes can happen – and will, even in the best of organisations. No, it is the bland manner of their response that we take issue with, most particularly the following statement:-

As notices and announcements are displayed on each school's public homepage in Satchel One, all of the information temporarily shown could be accessed by any user by navigating to the school's homepage.

An impossibly insecure situation, plus

If a teacher would like to create a notice and share confidential information, we ask that they put this in an attachment and then lock it by clicking the padlock icon to ensure that only students or parents from that school are able to download and view it.

Satswana believes this to be the antithesis of “privacy by design and default”. No supplier today should be expecting their users to “know” that they have to perform a special function that involves specialist training in order to ensure security.

We are further concerned at their apparent claim to be a Controller of data, this is also what they publish:-

We no longer import parent data from schools, which would require explicit consent from parents through the school. Instead, we give parents who wish to use our service the chance to sign up themselves where we elicit their consent through our platform.

That obviously raises questions regarding how they get the initial data from a new school adopting their service, but in this instance the school was regarded as being the controller by the affected parents as regards the breach, and they had to sort it out. Satswana believes they should be a Processor, answerable to the school as the Controller.

Satswana merely reports its concern and sets out what it believes to be the case. It is for the user to consider the associated risk and consider their response. Usually suppliers are quick to correct their position and we hope that will be the case here.

2 Bett Show

Satswana attended this show in order to benefit from the Microsoft Privacy and Security seminar which was surprisingly poorly attended, which meant that many people will have missed out on hearing some of the most senior initiators of change explain what the future holds. Just where that perhaps leads will become the basis for a further paper on strategy and implementation for our customers at the start of the summer term.

But the show itself was awesome for its sheer scale, with vast displays of magnificent and beautifully designed stands, ably manned by capable and enthusiastic people. The entirety paid for in one way or another from your budgets.

Of course it is all a glamourous, but temporary, illusion – whose short lived nature probably justified the paucity of real buyers. Indeed it is the heretical view of Satswana that many exhibitors were selling 'yesterday's' solutions, and that the glitz of today will inevitably be the dust of tomorrow.

If they had paused to wonder whether they had anything to learn, and attended the Microsoft seminar, they would have heard about the work being done by Catholic Education in Western Australia. Their systems integration is not totally transferable to the UK, not least because matters of admissions and the integration requirements of the Department of Education do need specific interfaces. But their concepts resonated entirely with the direction that Satswana believes should be the future, and it should make current suppliers tremble.

3 Change!

Which brings us again to the eternal subject of change "the only constant" – in that this was first postulated by Heraclitus of Ephesus (c. 535 BC – 475 BC he was a Greek philosopher, known for his doctrine of *change* being central to the universe) it is, together with the strategy of Sun Tzu (545 – 470 BC) a reminder that we have all had to face this throughout history.

(Fascinating that they both lived at the same time, could they possibly have met?)

Even if the basics apply they could not have conceived of the current pace, and candidly none of us can expect to enjoy having to abandon the happy certainties of knowing how our systems operate, having to learn something that is distinctly different, possibly indeed beyond our experience and training.

This poses two challenges, the first arising from a statement that Satswana noted recently from a learned commentator:-

"Cyber security is not just a technological matter for the IT department, but an enterprise risk management issue that requires board-level attention."

That is all very well, but what if the "board level" within education has always left it to (and relied upon the advice of) the IT department? Heads will have been dedicated to teaching, not computing, and the paper based systems they were familiar with did the job perfectly adequately.

Satswana would wish to contribute three arising thoughts to you. First, whilst acknowledging that it may be outside your comfort zone, please take charge regardless because it is no longer IT per se, it is the direct management of the school, and you must lead it. Secondly, issues that used to be horribly complex are getting much easier – to the point that if it cannot be explained in a manner that you understand, then it is probably the wrong product being promoted by an incompetent person. Finally you should be expecting us as your DPO to make sure that it is made comprehensible to you.

However one of the issues you will quickly recognise brings us to the second arising point, which is that quite regardless of what our actual job is the future employee in any role is going to have to be fluently capable with "information" delivered increasingly seamlessly on many mediums, including a smart phone. It is a paradox that many of your students are already there, the moment they get a phone it becomes an extension of their fingers – and a desperate distraction! They will never feel the barrier that some might feel right now.

But therein lies a clue to the future, because the products they are using are seamless, intuitive, wonderfully designed and delivering benefits that justify any effort required learning their use. They are not the klunky, old fashioned, unstructured and poorly presented programs of the past, which required extensive training before an "expert" could do anything with them.

You WILL understand and be able to use the product, because if you do not, then it is no good, and will not become adopted! Demand simple explanations!

4 Identity lost?

We were actually pleased to note that a child had seen his identity subsumed to being "Harry 2" with the parents complaining.

That led the ICO to clarify 'While data protection law gives special status to the data of children, it does not prevent a child's full name being written on a schoolbook.'

Satswana constantly campaigns against the myths that arise from over thinking regulation and mistakes can be just as bad when they cause organisations to take privacy too far as when they don't go far enough.

5 Wifi on your phone?

Naturally enough when we are at home or at our place of work we will stay logged onto wifi, but recent reports have identified the dangers of leaving it on when you travel elsewhere since you may connect to a rogue source that has anything other than your interests at heart!

This is especially true when it comes to coffee bars or similar public spaces. Possibly we can all recall the joy of finding an unprotected source that we can log onto and update our email, but now that we know it could be an exploiter then it is clearly unsafe to do so. If you travel a lot an alternative is to buy a dongle that connects to the GSM network – yes you have to pay, but data lasts a long time just downloading email.
So the recommendation is to turn wifi off when you are not at a secure location. You will find there is an added benefit from a battery that lasts longer, since the phone will not be hunting for a signal all the time!

6 Another Quango

Once again we are most grateful to the school that brought this matter to our attention so we can share it with you.

Hot on the heels of discovering a quango called “the Surveillance Camera Commissioner” comes another – this time “The Copyright Licensing Agency”, and it is a condition of the licence (that you possibly did not know you had [but which is paid for apparently by the Department of Education]) whereby you “must cooperate” with their data gathering exercise.

One of the five documents they print on their website is a Privacy Policy, so that is OK then. Unsurprisingly one is a copyright notice and another their terms of use. The remaining two are an accessibility and anti-slavery policy – so “virtue signalling” is alive and well at this organisation.

Of course you will be pleased to hear that they are a non-profit, but when you see the endless list of board members and senior leadership team (all with qualifications in disciplines you have never heard of) you might wonder how they could ever distribute any money.

Put as simply as possible their purpose would appear to be to share fees for the use of copyright material out to the rights holders, and if you are “randomly selected” then ‘your staff will be required to follow two very simple procedures’ (sic), for which they require the name of the SLP (Schools Liaison Person – of course, you knew that!) – And you must tell ‘your receptionist’ that their “Royalties Officer” will be calling.

Mind you they say, “This is not a policing exercise”, but (this bit heavily underlined in the letter) “your Royalties Officer will clarify which licenses additional to your CLA licence will be included in this exercise.” Since it would appear that almost anything that is truly useful is excluded then (if you are copying from newspapers for instance) they will doubtless be seeking more revenue from you for a licence covering that.

To Satswana this all seems very heavy handed and we are sure it will be a most unwelcome intrusion on the time of schools. We assume (but it is not made clear) that the CLA require a data logging exercise over a defined period, from which they will produce their figures based on a statistical sample. We despair at yet another unremunerated demand on the time of a schools administration.

Did we say that DfE pays? Not really, County apparently de-delegates (which we understand means keeps) funding from your initial allocation to cover the cost of 'Licences & Subscriptions'. Since their charging basis is totally opaque you may want to check that you are not paying too much.

7 Using a “Sandbox”

Originally a military term where a box of sand was used to contain (hopefully!) the explosion of a grenade or such like that had become unstable; the word has been adopted to describe a safe environment in which you can test files without blowing up your PC.

Windows 10 Pro offers a version but it has to be turned on by searching for “Turn Windows features on and off” and should be restricted to competent users who will establish that it creates a unique virtual machine that is apart from the rest of the PC.

A specific use is to check an unknown or unrecognised USB stick, since it is a favourite criminal trick to leave one lying on the ground for the unsuspected to pick up. The natural action then is to try and locate the owner by checking the content – then wham, you have a virus! Open it in a sandbox please.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

C Easter update 2020

Contents

1 ESFA Complaints procedure

We do constantly stress that we learn from you regarding this job, and then seek to share the lessons. What you may ask has the Education and Skills Funding Agency got to do with Data Protection?

It proved to be an alternative route that a Parent used to attack a School where various access requests had been refused. We will not go into the detail, but of course we thought the refusal legitimate and expected them to complain to the ICO, and that we would then have to justify our action.

Instead they made a complaint to FESA claiming that "they have been unable to complete the published complaints procedure". The Complaints Manager of FESA wrote to the school to advise that "Our role is to consider whether the academy followed the correct process. We will not investigate the academy's decision". If it changes nothing, then any victory would appear to be pyrrhic, but that is not the point of this note!

It is to bring your attention to the possible use of this procedure, and to advise you to ensure that you do not fall foul of any of the "process" aspects. Somewhat starkly the letter advised that "Academy complaint processes must adhere to Part 7 of The Education (Independent School Standards) Regulations 2014. Failure to do so could constitute a breach of an academy's funding agreement."

To our reading Part 7 is not clear, it is certainly not even approaching a template of requirements for a complaints process, indeed 33 (d) promotes the initial use of an informal basis. If the parent complains about the response, then (f) requires a hearing before a panel consisting of at least three people who were not directly involved in the matter, but (g) requires an independent member if there is a panel hearing. Just one more thing for busy people to deal with we fear.

2 It can happen to anybody

The announcement below was viewed with a certain amount of schadenfreude by most who read it, a Regulator having to report itself to a Regulator!
https://www.fca.org.uk/news/statements/fca-data-breach
It does demonstrate how easy it can be to make a mistake, and how perfection cannot be legislated for.

3 Six phone apps for toddlers

We can hear the 'tuts' of disapproval, but it seems that the latest advice is that toddlers should be indulged instead of having their phones dragged from their fingers. DfE have now approved six educational apps which academics said would improve literacy, language, communication and handwriting.

Lingumi (2 to 5) uses speech recognition games and video games to help grammar and speech.
Kaligo (3 to 5) is a digital handwriting exercise book using a stylus and tablet.
Phonics Hero, for children who have started school, takes youngsters through 44 phonetic sounds.
Fonetti describes itself as the first listening book shop.
Teach your Monster to read helps literacy through games.
Navigo focuses on skills that underpin reading.

Quite a change from the days of early morning runs followed by a cold shower!

4 The most successful fraud

Before you read on, please think to yourself what the most successful online fraud might be, we would bet that many would think that it was credit card cloning or

faking bank documents, something like that. Thus I am sure you will be surprised to learn that Business Email Compromise (combined with email spoofing) is by far the leader, harvesting a value for a criminal that is 30 times larger than credit card fraud.

Our advice has to be never to trust any online request for payment, even if it appears to come from "the Head who has rushed on holiday and forgotten to pay a critical invoice". An infiltrated email account will be monitored, perhaps for years, waiting for the opportunity, knowing when the Head has gone on leave, learning the style in which an email is written. The hackers are capable and patient professionals. You must assume the request is faked until you have proved otherwise – and if you cannot contact the person to do so, wait until you can!

Also never accept instructions to change bank account details, that request is almost always a red flag. Check and double check before doing so – and delay anyway. The person you talked to on the phone to confirm the instruction may have had a knife at their throat. Yes, it can be that dangerous.

5 References

Did the CEO of the Trust who faked all his references and qualifications get away with it because, for a period of time, we had to disclose what was said under a Subject Access Request? Not so under DPA 2018, what you say is now protected from disclosure

Under the *Data Protection Act 1998*, references given by an organisation were exempt from disclosure on receipt of a SAR.

The exemption only applied to references given by the organisation. This meant that the exemption could only be used by the provider of the reference, and not a recipient.

The *Data Protection Act 2018* has removed this distinction so that any reference provided in confidence is exempt from disclosure under a SAR. This means that if an organisation receives a subject access request, confidential employment references about the individual making the request, whether created by that organisation or received from a third party, will be exempt from disclosure.

6 Face recognition technology

We are keeping an eye on this in the belief that it is likely to play a major role in the use of artificial intelligence in schools as essentially it is "intelligent" CCTV – in that you not only can see a person, you know who they are, and that can be managed by a program.

There was a very negative report regarding the use of the technology to identify criminals in London that, if true, just means that the supplier is dreadful. It is a very different story in China, where – as a consequence of Coronavirus – they can now identify people when masked. Cynics may say that they can also then track democracy activists in Hong Kong – they are claiming 99.9% accuracy, that being the feared "big brother" aspect.

However, the flip side is that in Wuhan they felt safer because "outsiders were identified coming into an isolation area, and they could stop those from leaving who were infected". One fears it is a privacy debate that has already been lost – not least because history would indicate that once something is technologically possible, then it will be adopted. And Cressida Dick (Metropolitan Police Commissioner) pointed out that many of the people objecting to the use of facial recognition were the same people who were happy to allow Facebook to use their image to connect with friends.

The genii is out of the bottle, this will be coming, and if you reflect for a second then you will want to use it exactly as it was applied in Wuhan. All schools wish to ensure that only authorised personnel enter the premises and nobody leaves when they should not. How many hours are spent guarding doors at the moment, and is that a good use of time? The answer is a clear no, and anyway it is imperfect, you cannot be everywhere all the time, a camera and computer can be, the alert can be precise and immediate.

Which brings us to two further issues, one being the call for consultation on changes to "Keeping Children Safe in Education 2021" – and we link that with proposals for legislation to force businesses and institutions to create provisions to protect personnel in the event of a terrorist attack. Satswana can see these two being combined and becoming yet another responsibility placed on schools whose personnel are stretched to the limit.

Intelligent recognition technology will have to be deployed and will become ever smarter in recognising risks. You may consider that an appalling invasion of privacy, but you will not be able to come up with an alternative that is as effective. Please take a seat Mr Orwell.

Gosh, did we forget to mention that the Wuhan cameras also had infrared technology to take temperatures so that they could identify sick people?

7 Biometrics

Schools adopt biometric identification for lunch systems in order to provide a secure system that avoids the apparent risks of bogus transactions from some other control methods such as PIN numbers, or indeed pupil names.

Where this is adopted the school has a “legitimate business interest” as a basis for consent to collect the “personal data” represented by a fingerprint in most cases. If a catering company is involved, then you probably have your contractors noted on your privacy policy as organisations that you share data with.

Despite this clear basis for consent one particular father took exception to his child having their fingerprint taken and claimed that the school had no consent to do so. We can only speculate why he became quite so emotive regarding the subject and it is always to be regretted when “Mr Angry” fails to manage their opinion in a reasonable manner.

However, as with facial recognition technology, it is now a reality that such systems have to be embraced as schools are increasingly required to do more with less. A fingerprint is simply and solely a secure means of identifying an individual and it is used on an entirely closed system basis within the environment of a school. It is not published anywhere, nor of any use anywhere else.

Thus Satswana contends that there is no basis for an objection to the collection and use of biometric information for school security purposes.

8 Disposing of computers

Did you know that within the second hand computer market (and indeed any intelligent device) there is a thriving trade in scanning disks and memory for any residual personal information – particularly stored login details?

It is not enough to simply erase your personal files as this does not actually delete the data; it just deletes the index to it, so that it cannot be found by the program that was using it.

The only way to guarantee that data has been removed is to overwrite the drive, and there are specialist firms that can do this for you, but you can do it yourself. Other machines and Macs have similar options, but with a Windows (we hope you are all on Windows 10 by now) machine first go to Settings. Select the Update and Security area. Select Recovery, then Reset this PC, choose the option to “remove everything”. During the reset you will be presented with the option “Remove files and clean the drive” which fills all but the section containing the system with digital noise, it may take an hour or two.

Make sure you have taken copies of any data you need in future, there is no way back!

9 Reports to Governors

There are a number of organisations that seek to make a living by providing training courses in aspects arising from GDPR, and we regret that many of them use scare tactics to sell their products.

One course is making the claim that Schools must provide a report to governors on an annual basis.

There is absolutely no statutory basis for that, though of course it is good practice to keep your governors advised of your progress on what we always describe as being a journey, and not a destination. We also constantly point out the difference between the words "must" (where there is an absolute statutory requirement) and "should" which tends to be a matter of opinion – usually as a consequence of gold plating the regulation.

Satswana submits that there is nothing practical to be gained from adding yet another burden onto your administration by requiring a specific report. We would welcome it if you shared our updates with governors, so that they are also aware of what is an ever changing and evolving scene. We believe that might be much more practical information for them.

10 Covert recording

This issue comes up quite frequently. Fundamentally a recording that is made secretly will never be admissible because they are regarded as being too easy to fake. "The Transparency Project" suggests that if a party requests that a recording be made, then it cannot be objected to, but the counter party should then also record the discussion so that it can be authenticated.

There is also the question of the consent of the parties. As stated above, this cannot really be withheld if requested, but if the recording is covert then under "Protection of the rights of others" it would be exempted on the basis that the persons present would not have expected their conversation to be disclosed.

11 Ransomware

We provided the following advice to the school that was affected by Ransomware

1 Search Internet for release keys from sites such as this https://www.ifsecglobal.com/cyber-security/rundown-ransomware-master-keys-released/ there is a reasonable chance that it might be an inside job, in which case the encryption may be amateur and you will recover the data

2 Whatever you do, there is no question of paying, and not just for the moral reason that you cannot allow crime to pay. Most criminals just pocket the money and do not provide a release (even knowing that they might makes them a target – or it would if the Police were any use.) Then you have no data and have also lost your money.

3 From login files establish where the infection got in, there is no point in rebuilding files if the infection source is not remediated.

4 Set to and rebuild your data, the base Pupil records will be available from the LA, parents, students, teachers, contractors etc., they will all have bits and pieces. Auditors are likely to have copies of finance files and DfE reports will also build a picture. It will not be perfect, but it is the best you can do.

5 Take a monthly totally separate archive file. You will lose several days data, but it is easier to rebuild a few days than a total history. Make sure none of the archives have the infection

12 Ofsted on GDPR

We are often asked what Ofsted's views are on GDPR, and the general expectation is that they might well examine your compliance with the Regulation, therefore we were very pleased to be able to capture some comments from a recent inspection that we will reproduce below. May we comment first however that if you have carried out the following work then it is felt that you would be considered to have done everything necessary?

a) You are required by law to appoint a DPO, and thereafter under the Regulation ensure that you seek their counsel for any planned changes in your data handling, including of course taking on further software. There are still many schools that have not made an external appointment, and if you genuinely have a staff member who has absolutely no conflict of interest with management, then that is OK. However, we do suggest that might be difficult to prove to the satisfaction of Ofsted. As with us, a full time DPO does nothing other than study the subject and so we also suggest that they must acquire a competency level that will exceed a part time role.

b) The DPO must have conducted an Impact Assessment with you and provided staff training and guidance on a plan that leads to "privacy by design and default".

c) Almost the first line of the recommendations will be to ensure that your data is encrypted wherever possible, this being the strongest available protection that you can adopt.

d) You will have published a privacy policy on your website.

e) Also adopted a strategy for retention and deletion of data.

f) We would also expect them to consider the physical security of the school (access etc.) as well as both digital and secure paper storage.

This might all be regarded as basic common sense management, and matters that the education community have always taken extremely seriously. In the particular instance referred to the inspectors had very little to say on data, with only three matters coming up that might come under that heading.

1 Of course they had a strong concentration on the Single Central Record
2 They questioned the "acceptable use" policy
3 They asked how the school managed photos, the policy on devices used, and their deletion

Our thanks to the school that provided this information

13 Chess anybody?

Garry Kasparov, possibly the greatest player in history, has complained that he is the first knowledge worker whose job has been threatened by a machine!

D Satswana Summer update

Contents

1 Encrypt, NOW – please!

Last month we spent considerable time dealing with the consequences of two failures to encrypt data on servers. In both instances the management were extremely experienced, the most serious was a data processor – and as a

consequence one of our Directors is engaged on checking our list to ensure that Category A organisations are encrypted, or they will be downgraded.

The other was where trust in a person who had administrative access turned out to be unwarranted – which is perhaps the most difficult situation of all for management to deal with. The fact is that an internal attack is one of the most common, so creating the additional protection of encryption adds something to your security – it is another hurdle for somebody wishing to compromise your protection to jump over.

The real problem, with any data compromised due to the incompetence of a processor, is that it remains "out there" forever, and none of us can know either when, or if, a criminal manages to create an exploit by connecting say your bank account details with a future post on the Dark Web of something else. For that reason anybody compromised might have a claim for compensation if it should lead to a loss. Sadly we simply cannot know what the implications might be.

What we must point out is the critical need to take data security seriously. I know none of them personally, but would assume that the staff of the Processor concerned will have been perfectly decent people, coming (as they did) from a former local authority environment, running a business doing various functions that used to be centrally controlled. The trouble is that sort of culture will not "be told", they "know their job" and indeed "know best". Most sadly for them that cosy attitude will have meant that their world has now imploded due to a failure to execute the most basic of data security recommendations, namely to encrypt data at rest. Fingers will be being pointed and attempts made to shift blame, but it is all too late, because it is an institutional corporate mistake that every level and layer of "management" is responsible for.

Can they survive it? The brutal answer is probably not, though the same institutionally arrogant assumption of entitlement that caused the problem in the first place will probably mean that they are not even asking that question of themselves yet. They will be busy "putting it right", investing heavily in the changes that – had they been embraced in the first place – would have meant that the exploit would never have happened. They will assume that they can recover the reputational damage with their customers and "get back to normal", meaning an uninterrupted earnings stream into the future. If the ICO fine them along the same lines as the mega penalty charged to British Airways, and if their customers seek compensation for the data loss, then they may simply find that they do not have the strength to continue.

Thus their world collapses, one day respected citizens with a good job in a sound business, the next ruthlessly exposed as negligent in their duty to their customers - due in the first place entirely to criminal action. Do we feel sorry for them? On a

human basis, yes, of course, nobody would suggest that they were “bad people”, but they will now be out of work, branded failures due to an unlucky roll of the dice.

The margin between survival and failure is thus impossibly small. We do not intend to be rude but must point out that however fancy the title you may have, if you think you “know best”, and thus cannot be prepared to listen, and learn, be prepared to accept and adopt change, then just such a trip wire as this firm has experienced may be waiting for you just around the corner. Please make it a resolution that this consequence will not apply to you!

Prior to this problem the following article had been written on the subject, we hope you find it relevant and useful now in the context of the above imperative.

2 Securing your computing environment

This paper is designed to provide positive action to be taken by both our schools and local authority customers towards securing their computing environment. It is all a part of the Data Protection Act objective of “privacy by design and default”.

We suggest the most complete adoption of encryption as being the first line of defence, and the single most effective tool you can use to protect yourselves. Encrypt PC’s, servers, phones and USB sticks, then it you are hacked the breach does not have to be reported to the ICO.

Once you have done that the next most important issue is to rigorously challenge who has access rights within your network, with special attention being paid to anybody who has the elevated “administrator” access.

As we move towards the more collaborative methods of working represented by the cloud based Microsoft 365 the file access rights, “permissioning” to use another term, will become absolutely critical to both your control of data and its security.

It will also become a management challenge, both maintaining the system and keeping pace with any changes dictated by a member of staff leaving and somebody else joining, for instance. You will need somebody appropriately skilled to manage the entries within Active Directory – which generally speaking works across the Microsoft eco system.

In the old days it was fairly common for system access to be set so that all parties could see all files, meaning that there was no internal security at all – if you were logged on as a user, you could read and do anything. That should no longer be regarded as being acceptable, indeed the policy should be one of granting “least privilege” and if that means that the finance files cannot be seen by all and sundry, that is not only probably a good thing, it also means that fewer user profiles are

quite so vulnerable to phishing attacks, business email compromise, or indeed the loading of ransomware. Those are the three major threats that we are faced with.

If access rights now establish a greater importance, absolutely the most important of all is the level of "administrator" that allows somebody to make changes to your system. Recent Microsoft research has determined that in the case of the Explorer browser 100% of the critical vulnerabilities were connected to Admin rights and 80% within Windows 10, dropping to 79% in servers.

The raw fact is that people are the weakest link, so restricting the ability of individuals to cause an issue has to become a prime consideration.

To make this advice straightforward to follow we therefore have three jobs to do. If you do not know how to do them yourself, then of course you may need some support in implementation, but the first is to make sure that your files are protected by encryption. The second is to apply restraints on any universal access to files or areas of the network that are appropriate to the user. The third is to challenge why anybody has administrator access, make sure you know who they are, and confirm that they are competent to be given that trust. Make sure also that any logging is enabled so that you can audit who has done what, and at what time!

In the past we have trailed the idea of "zero trust" whereby multi factor authentication techniques absolutely confirm the identity of the person accessing your system. We are still working on that, but your advisor may wish to consider MFA for any administrator, given that the role carries such a serious risk. We will cover that in a future paper.

3 Bett Community online resources

A spin off from the Bett show was the gathering together of a host of online resources to support remote teaching, including our personal favourite, being The Khan Academy, it is worth checking out.
https://www.bettshow.com/bett-community-hub?mkt_tok=eyJpIjoiTTJZMU56ZGtNalk0TmpNNCIsInQiOiJKTkthSmxXZGpYNGY0QnBDSk1ZQitMK0lyckRsdGY3OUk5c2ppdjFzblB2UlV3Q3RjSGxpZ2ZqXC9EN29yYlVHdk5sa3hqcTY1NU92ZFU3ekYwbVJRTEZORmJIR1VZbitDdGxmZGZ0THByNWk0VUdFWTlaYkJYN00wVnB2dTdUK1IifQ%3D%3D

4 Microsoft Licensing?

Whilst Microsoft are making 365 and much of their Cloud platform free to education, it seems that historically you will have purchased a "Client Access Licence" for your servers and local operation, and the pricing has apparently risen by 40%. The school that raised this with us were facing a bill for £4000, which appeared to be an

overcharge in the first place and their IT supplier immediately suggested that it could be reduced, despite the price increase. May we recommend that you review carefully what your actual needs currently are with your IT provider and consider whether by using Microsoft 365 the bill can be reduced?

5 Ricoh Photocopiers

We have covered this issue before but it has come up again and it seems that Ricoh continue to seek to charge customers a fee for "cleaning" the copier of all personal data when it is returned. The Satswana argument is that as a processor it is their obligation to protect personal data as if they were a controller, and if they know that it is prejudiced when the copier returns to them, then they are obligated to clean it, and not charge for it.
The discussion is ongoing, and doubtless Ricoh are not going to give up a "nice little earner" easily. However, we believe they have compromised their own argument in the literature they produce, in that the free basic service they offer (DSSD) does not have the box ticked "Machine fully cleansed to meet Data Protection Act 2018 and ISO 2700 / GDPR – ISMS". The chargeable "Secure 30" service does! Case proved we think m'lud! It is further proved by our understanding that all copiers now being shipped operate in a manner that immediately deletes data, once again (we think) proving the point.

6 Chinese initiative!

We were amused to read that school children under quarantine in Wuhan, China spammed a homework app with one star reviews in the hope it would be removed from the App Store.

Apparently tens of thousands of one-star reviews for the Alibaba-owned app DingTalk were submitted to the App Store in the hope of knocking it offline.

The coordinated campaign saw the rating for DingTalk fall from 4.9 to just 1.4 stars. However despite the effort, the free remote working app remained available for download.

On Chinese social media, DingTalk reportedly made a plea for users to stop the bad review campaign. It wrote: "I'm only five years old myself, please don't kill me."

7 Zoom

How exactly did Zoom become the de facto go to video platform of choice? Why was it not Skype, Facetime, Google Hangouts, or even Teams? I suspect because it was free, uncomplicated, and just works. It clearly had initial security issues, but these have now all been fixed in record time – all clearly communicated to customers.

Now that we have used it “in anger” what a marvellous boon it is, to the point that Satswana will be using it whenever and wherever a “meeting” is called for, but we are unable to visit personally.

If you wish to study what they have done, then the Zoom blog is the best place to start, but you will find most of the detail you will be interested in within the attached appendix to this update, being their post for Zoom in Education.

Our use of Zoom does not change our respect and recommendation for the use of Teams, indeed that is clearly superior as an internal collaborative communications medium, but the permissioning involved, plus the fact that it is not free to those outside education, makes it cumbersome and expensive for ad hoc conferences.

8 Types of attack

What exactly are you up against in cyber-attacks? Here are four scams to look out for. We are often asked whether we have a guide for staff on GDPR, and indeed we can offer some options, but it is sometimes better to put across a limited set of lessons to ensure better absorption. If you were able to bring these to the attention of your staff, then it would help all our security going forward.

a) **Purchase scams** offer protective equipment, sanitising products and other desirable goods for sale that you will never receive. Be careful paying for anything via bank transfer and only buy goods from reputable companies that you know and trust.
b) **Smishing** is sending text messages that appear to come from a trustworthy source like the UK government or even your own doctor which try to steal personal or financial information. If you doubt the text’s authenticity, don't click links. Visit www.gov.uk to check any information given. Verify an organisation’s phone number from their website or from old printed correspondence.
c) **Phishing** is sending emails which try to make you divulge sensitive personal or financial information. They may appear to be Covid-19 tax refunds, reimbursements from travel bookings, safety advice via email and even donation requests. Fraudsters will try to make you click on links that aren't safe. So think before you click. If in doubt, then don't click. And don’t open any attachments from senders that you don’t know. If you’re still worried, talk to family, friends or someone else you trust.
d) **Vishing** is unsolicited phone calls. Always be suspicious of ‘cold-callers’. Don’t be afraid to challenge them or hang up if you can’t verify the caller. Banks, police etc. will never ask for security information, so never give out personal details. If you’re concerned, call the organisation back on the number listed on their website, ideally on a different phone as criminals can sometimes

keep the line open. Or if it's your bank, use the number on the back of your card.

9 5 ways to stay secure whilst remote working

McKinsey are a vast consulting organisation and they have produced the five following points, which you will have heard from us before, but no harm in restating them! We have added Satswana comment.

a) Multifactor authentication

Having a strong password often isn't enough, for example, if your credentials are leaked in a data breach. Multifactor authentication involves an additional step to add an extra layer of protection to your accounts. The extra step could be an email or text message confirmation, or even a biometric method such as facial recognition or a fingerprint scan. (Satswana – this particularly applies to any administrator access you allow as discussed in 2 above.)

b) VPN encryption

Many people are familiar with using a Virtual Private Network (VPN) to bypass geographic restrictions on streaming sites and other location-specific content. VPN encryption is the process of securing the data within the VPN client-VPN server tunnel to make sure it can't be exploited by anyone. Basically, when you run a VPN client and connect to a VPN server, your connection requests are encrypted before they are sent to the server. (Satswana, actually we hope that your use of any form of VPN connection will be declining in favour of the adoption of secure cloud connections such as Microsoft 365.)

c) Mobile device management

The average office worker will probably have more than one work device, i.e. a laptop and a smartphone, especially during a lockdown! These devices are deployed across multiple mobile service providers and across multiple mobile operating systems, so can be little difficult to manage. A mobile device management (MDM) solution can be used to monitor, manage and secure employees' mobile devices. (Satswana, practically speaking your staff will be using their own phone to receive content from cloud based systems. You need them to implement three things, first that the phone is access protected [password, biometric etc.] second that the content is encrypted [this is often the case by default but can be accessed through 'settings'], finally that remote delete is enabled in the event that the phone is lost or stolen.)

Contents of this document are the Copyright of Satswana Ltd 2021 ©

d) Antivirus software

Although having a firewall is important, it's inevitable that online threats can get through. Good antivirus software can act as the next line of defence by detecting and blocking known malware. Even if malware does manage to find its way onto your device, an antivirus may be able to detect and, in some cases, remove it. (Satswana, a strong caution, because AV software simply cannot keep pace with the rate of criminal exploits – but you must keep it as protection from historical attacks.)

e) Back up your data

Data can be lost in a number of ways including; human error, physical damage to hardware, or a cyberattack. While hardware backups are still an option, one of the most convenient and cost-effective ways to store your data is in the cloud. Cloud backup services come with a wealth of options enabling you to customise your backup schedule and storage options. (Satswana, plus please also recall our suggestion that you take a totally separate "archive" copy of your data once a month and separate that entirely from your network. The reason is that if you should suffer a ransomware attack you have a reference data point to go back to, even if your online backups have been infected. You will have lost data, but not all your history. Please recall you should never pay a ransom, almost certainly you will both lose your money as well as your data!)

Appendix, Zoom for Education

Kaitlyn Guzman posted: "Remote virtual learning has become the new normal for many teachers, administrators, students, and parents. While the transition may not be easy, we want to provide resources to ensure users are creating secure and effective virtual classrooms using Zoom."

New post on **Zoom Blog**

Zoom for Education: Top 10 Frequently Asked Questions
by Kaitlyn Guzman

Remote virtual learning has become the new normal for many teachers, administrators, students, and parents. While the transition may not be easy, we want to provide resources to ensure users are creating secure and effective virtual classrooms using Zoom.

We collected the top 10 most frequently asked questions about using Zoom for virtual education and online learning. And before we dive in, here's a bit of inspiration for everyone doing remote schooling right now:

1. Should I use Zoom Meetings or Zoom Video Webinars to host a class?

Both meetings and webinars are great ways to connect and engage with large audiences and even collect valuable insights by requiring registration. However, meetings and webinars have key differences:

- Meetings are designed to be highly collaborative, giving attendees the ability to use audio and video, share their screen, and annotate in a live, interactive environment.
- Webinars give you more power to manage the audience. Instead of interacting over video and audio, webinar attendees interact with the host and each other via the Q&A and chat panel.

Meetings can be useful for a hands-on, collaborative classroom environment where students can engage directly with the content being shared and with each other. Webinars are great for online lectures where students can listen, view content, and submit questions via the Q&A feature.

To help you decide which is better for you, check out this side-by-side feature comparison of our licensed meetings and webinar accounts:

2. What are best practices for setting up a virtual classroom?

Here are some recommendations to help you create a secure and productive virtual classroom:

- **Require passwords:** Create a meeting or webinar password and share it with your students to ensure that only guests with the password are able to join your virtual classroom.
- **Require registration:** For both meetings and webinars, you can require registration to see who has signed up to join your class. You can also manually approve each registrant to help evaluate who will attend your class.
- **Enable Waiting Rooms:** Waiting Rooms prevent participants from joining a meeting automatically are enabled by default for those enrolled in our K-12 program. You can admit each participant individually or all participants at once. You can also allow students who are signed in via your school's domain to skip the Waiting Room, while attendees that aren't part of your school's domain must be admitted individually.
- **Disable screen sharing:** For education users, the screen sharing settings are defaulted to allow only the host to share a screen. This prevents attendees from sharing unwanted or distracting content. To allow your attendees to share content, you can adjust this setting or toggle in-meeting sharing in the Security icon.
- **Disable private chat:** The host has the ability to lock the chat so attendees cannot privately message each other. Students can still chat with the teacher.
- **Manage participants:** If an unwanted guest has joined your class, remove that participant with controls in the Security icon. Get additional insights for managing participants, including the ability to mute participants, stop their video, and restrict renaming, on our support page.

- **Lock your meeting:** You can also lock the meeting right from the Security on to prevent other attendees from joining once the meeting has started. This feature not only keeps out unwanted guests, but it is also great for enforcing a tardiness policy.

3. How do I ensure my classroom is secure?

There are a number of features and settings that are enabled by default and can be utilized on the fly to ensure your Zoom classrooms are secure.

Within your meeting, the Security icon is your all-in-one place to quickly find and enable security features. This feature allows a host or co-host to:

- Lock the meeting
- Enable the Waiting Room
- Remove participants
- Restrict participants' ability to screen share, chat, rename themselves, and annotate

As an additional layer of security, Waiting Rooms and meeting passwords are enabled by default for free Basic and single licensed Pro accounts, and accounts in our K-12 program. The meeting password requirement cannot be changed for those K-12 accounts. We invite you to check out our recent blog on securing your virtual classroom for additional tips.

4. How do I take classroom attendance?

One way to take attendance during your online class is to require registration so you can review the registration report to see who registered and who actually attended. Another way to take attendance is by launching a poll during class. You can later export that poll report to know who attended your class based on who responded to the poll.

5. How do I see all my students on video?

With Zoom you have the ability to see up to 49 people on video in Gallery View. Simply enable this feature in your video settings. Have more than 49 students? No problem! View up to 1,000 thumbnails by clicking the right or

left arrows in Gallery View to show another 49 participants.

6. How do I set up breakout rooms?

Breakout rooms give you the ability to split your class into as many as 50 separate sessions, which are great for group-based activities or assignments. Within each breakout room, participants have full audio, video, and sharing capabilities. Each room can also alert the host when help is needed, and the host can visit any of the breakouts to assist and answer questions.

To use this feature, be sure to enable breakout rooms in your meeting settings. Then, you can either pre-assign or auto-assign students into groups. (Here's how.)

7. How do I share my screen?

Screen sharing allows you to share slides, videos, and other valuable content with your students. You can also give students access to screen sharing so they can present their own work. To share your screen, just click the green "Share Screen" icon and select what you would like to share. If you are sharing a video, be sure to click the "Share Computer Sound" checkbox.

Screen sharing also allows you to share a secondary camera in a Zoom session. This means you can share from a doc camera, which is similar to an overhead projector. Check out our integration with Kaptivo, which allows you to capture and share content on a physical whiteboard digitally.

8. How do I annotate? Who else can annotate?

When you are sharing your screen, you have the ability to draw, type, and add stickers on to your shared content. The host also has the ability to allow participants to annotate on their screen. This is a great way to engage and collaborate with your students.

When sharing your screen, you can also share a whiteboard. This is just like a whiteboard you would have in your classroom, this shares a blank digital

page that you and your attendees can use to work on problems together.

9. What features are available on a Chromebook?

Hosting and joining meetings on a Chromebook gives you access to most of the features you would have on other devices. All you have to do is join your meetings via the Zoom application found in the Chrome web store. The main differences with a Chromebook are that polling, whiteboard, annotation, and remote control are unavailable. Learn more about using Zoom on a Chromebook.

10. Can I host and join meetings on a mobile device?

With Zoom, you have access to the same reliable and seamless meeting experience on your mobile device as you would with other devices. However, some in-meeting controls such as creating and launching polls, starting breakout rooms, and controlling who screen shares, aren't available on a mobile device. The Gallery View is also limited on smartphones and tablets.

Start Zooming today

Want a little more help getting started? You can walk through these top 10 questions with a Zoom expert in this on-demand webinar:

Watch the webinar

Or check out some of our additional resources on setting up and securing your virtual Zoom classroom.

Kaitlyn Guzman | April 24, 2020 at 1:45 pm | Tags: zoom for education |

URL: https://wp.me/p3BrMJ-6yF

Unsubscribe to no longer receive posts from Zoom Blog.
Change your email settings at Manage Subscriptions.

Trouble clicking? Copy and paste this URL into your browser:
https://blog.zoom.us/wordpress/2020/04/24/zoom-for-education-top-10-frequently-asked-questions/

E Satswana Summer holiday update, 2020

Contents

1 Recording video meetings

Except in the most exceptional circumstances where you believe you might have to retain a recording as evidence that cannot be supported otherwise, our strong advice is that you should not record video meetings.

Of course you can find other advice, but in our opinion it has not been thought through. It seems that the suggestion is that because you **can** record the meeting, then you might as well do so, and then if there is any discussion or debate over what was said, then you have the evidence.

The first and most basic point is the GDPR principle that "it is the data that you do not keep that is the safest". We say that if it was a normal meeting then it would not have been filmed (and probably not even voice recorded). So why because the meeting is on film do we suddenly say we have to record it?

Secondly you are faced with all the retention period issues, once you have decided to make a record, how long do you keep it for. Furthermore who then has the duty to remember to delete it at the end of the period, and how long does that take? It all adds to a work load and risk that you will forget, adding to the risk that it might be unlawfully accessed. You will all have read about the medical notes that were released accidentally.

Thirdly this is rather easier to do than you might think, not least because lay people are working with new technology that – because it is new – may have undiscovered flaws. That created a nightmare for one of our customers when she sent it to what

she thought was the secure part of Microsoft Streams. She didn't see one of the check buttons so accidently shared the recording publically. Of course we would say that should not have been possible, but apparently the "default" is public, so you have to state if it is private. Now just how many undiscovered traps are there like that within the various systems we are using?

Fourth, are we sure we have consent from anybody involved to retain their images?

Finally there is the question of the minefield that Subject Access Requests can be. These are hard enough to deal with in a straight administrative sense, taking a lot of time and often creating considerable stress. If you retain recordings then very possibly they will have to be disclosable, meaning extra work as a minimum, and the risk that you are passing something that can be taken out of context and capitalised upon by the sort of vexatious litigant who too often seems to make these requests.

Hence our advice, a video meeting is merely a meeting that is held via video. Stick to your normal tried and tested procedures for recording the minutes, where required, and do not record anything at all if that would have been your usual practice.

2 Exam Board results leading to Subject Access Requests

We have shared information on this matter separately and at the time of writing this are really no further forward. The commentary below is extracted from an article published by TheExamsOffice.com referring to AQA, the ICO and Ofqual, from whom apparently confirmation is still to be received as to whether or not you can release individual grade and rank order information, meaning really that we are no further forward.

Given the emphasis below on the work of the DPO, we hope to be able to give you absolute advice closer to the date!

"Last week, in an email update to exams officers, AQA stated:

Exam scripts are exempt from subject access requests, but centre assessment grades (CAGs) and rank orders aren't. This means students are allowed to ask to see their CAGs and rank orders, but please remember, CAGs and rank orders cannot be given to students before results day.

The *Information Commissioner's Office* has issued the following guidance in relation to requests for grade and ranking information from students:

The ICO has received a number of queries about whether the exam scripts exemption will still apply in these unusual circumstances.

The answer is yes, the exam scripts exemption will still apply to the information used to award students' grades.
This allows for longer response times for requests for access to pupil assessment information if they are received before the official results are announced.
Requests made after the results are announced need to be dealt with as a normal subject access request.

It seems that providing students with access to the grade awarded by the teachers is acceptable, however, if students are informed of their rank order, then via a process of elimination they could deduce the rank order of other students, and therefore, would this contravene Data Protection regulations?

Whilst confirmation is received from Ofqual on this issue, *The Exams Office* asks all members to consider the following steps in relation to requests from students for access to their centre assessment grade and ranking:

• All enquires **MUST** be dealt with by the individual in your centre who has been appointed as the Data Protection Officer (DPO)
• Any advice or guidance provided in relation to a student's data must be given by the DPO as the individual who is responsible for monitoring compliance with the GDPR and other data protection laws, and devising your centre data protection policy

3 Clearing out Primary School files

As we constantly confirm, we absolutely welcome questions from our customers since that becomes the best way for us to learn what you require, and also means we have to find the answers. Recently there have been a number of queries regarding when Primary School files can be deleted or destroyed and we were able to reply to one as follows below. The statutory requirement link was a particularly useful "find" and will also assist any Secondary having similar questions. We were also intrigued to learn of the "lost pupils" database (that you probably knew about!)

"You are perfectly at liberty to destroy all files that have been transferred via CTF to a Secondary School

The statutory requirement will be found here
https://www.gov.uk/government/publications/common-transfer-file-19-specification (and useful further guides)

This only applies to the maintained sector, though others are encouraged to use the system

If no destination is known there is a provision to send data to the "lost pupil's database which could be a convenient means to ensure it has been "passed" somewhere

I extract and copy below something that might not apply, but you should be aware of from a safeguarding point of view

As I read it, despite the lack of real structure to do so, schools are encouraged to provide data to any further school, including in the independent sector

Thus in the vast majority of cases you should be able to pass the documents on, and then dispose of any remaining files

If you are concerned about any that are left, then your idea to contact the parents is a good one, though I would point out that there may be times when information should not be passed to Parents, within certain safeguarding files perhaps?

I think I might make liberal use of the lost pupil's database, especially if the parent did not respond."

(EXTRACT) Circumstances when it is not considered appropriate to pass on information about a pupil via a CTF might include:

•a family escaping a violent partner
•the family is in a witness protection programme
•adoption

In the first two examples above it may not be desirable for the "old" school to know where the pupil has gone to ensure this cannot be accidentally divulged. If a family is in a witness protection programme the "new" school should also not know where the pupil has come from as this could enable the pupil to be linked back to his or her previous identity. It is important that an adopted child cannot be identified through his or her school history and so a new school should not know the previous school an adopted child attended and vice versa.

In each case the "old" school needs to be involved in deciding what to do because it is that school's responsibility to send a CTF to

•the next school that a pupil attends or
•the Lost Pupils Database (LPD) area of the S2S secure transfer site when they do not know which school the pupil will next attend
• The DPO, in conjunction with your Head of Centre, must be the individual who makes decisions relating to data handling and sharing in line with official guidance and the centre's Data Protection policy

• Centres should be aware of the severe penalties which can be imposed for incorrectly disseminating, sharing or withholding data

Effective protection of data requires a thorough understanding of data protection regulations, and therefore, unless you are the appointed DPO, we strongly advise all members to forward any data related enquiries to their DPO and not to take it upon themselves to share data upon assumptions or advice from non-data specialists.
If your DPO is unclear over any of the regulations, or requires advice, they should contact the Information Commissioner's Office, Ofqual, JCQ or the relevant awarding body.

4 Taking on new software or administrative processes

We are similarly delighted to hear from you when you are considering taking on new software or changing your processes. We can check out the supplier for you and add them to our Processor list and share it with everybody. That is absolutely the function of the DPO, as is any related impact assessment. The specific question then was what was required as an impact assessment and we advised as follows:

"The assessment can be a totally internal "risk" discussion. The assessment is for you, not any external party.

Basically the question you will be asking yourself is "what is the impact on our data practices of adding (the new software) to our systems"?

And the answers are likely to be:-

1 We now have a separate software suite to record data on
2 That will need consideration as to who has access, to be limited to those who "need" access
3 How is the data secured (encrypted) and backed up so that authorised persons can obtain access
4 Are there any other issues we have to consider, such as who might be entitled to be told what is on the new database

So actually it is only a common sense approach, but it is sensible that you do perhaps discuss it formally at SLT

If you feel that Satswana can assist at all in that discussion we are very happy to join any meeting via Zoom"

5 Backing up your systems

We have also received questions on this subject from a number of you and the security and reliability of any backup system is also related to your ability to recover from any disaster situation or criminal attack with ransomware, so it is important. Link that to the failure of one particular County based provider to even encrypt the data they held and the quality of the organisation also becomes important.

So when we discover one that is experienced at supporting schools and also answers all the questions we could put to them, we feel we should bring them to your attention. May we stress please that Satswana has a policy of never getting involved with "partnerships" or having any conflicting commercial return that might affect our duty to you.

Three things impressed us about https://www.directcloudbackup.com/. The first was that the data they handle is encrypted at every stage of every process. Secondly, and this really impressed us, they have an ability to check every backup you do to see whether it may have been infected with ransomware, and if it has they stop the backup and check with you. As many of you will be aware our biggest concern is that a criminal will wait until your historical backups have been infected before declaring their hand, so you cannot recover.

In that regard we hope you recall our advice to retain an "archive" copy of your information somewhere entirely off your network, so that even if you lose a lot of recent data you do have "something" to go back to, because we must repeat that you should never pay a ransom demand. That is not simply because you would be supporting criminality, but for the practical reason that they almost certainly will just take the money and run. You have then lost both your data and the money!

So the third thing that impressed us was this company's attitude to archiving, not only giving you historical data to get back to, but also reducing the cost of the data that is largely static – but which you have to keep for a set period of time.

A final credit to them was their very personal response, with their Director making the effort to get back to us. We acknowledge that there are massive international organisations that specialise in this area, but we think you will like an equally competent, but UK based and approachable concern.

6 Financial strength of processors

Which brings us to another consideration that we are increasingly finding it sensible to include in our processor evaluations and that is their financial strength, since the raw fact is that if they are underfunded they might say all the right things, but simply not have the resources to support them. It is also a reality that an entrepreneur

Contents of this document are the Copyright of Satswana Ltd 2021 ©

might be exceptional at delivering a service, but have virtually no IT training. So how do they know who to hire, can they afford them, and can they trust the result?

With organisations as large as British Airways being found seriously wanting we will have to find ever more ways of assessing their capability.

7 Track and trace risks

It is really sad to have to report that society remains at risk through the use of technology where security flaws should have been fixed years ago. We can have sympathy for officials who thrash around and make mistakes when faced with an entirely new challenge, but it is unacceptable that their political spokespeople cannot admit to their errors and do nothing to correct them.

The latest confidence trick arises from the ease with which a telephone number can be "spoofed", meaning that a crook can pose as a track and trace caller using a call centre number – which incidentally will not accept incoming calls so you cannot call to confirm. They call and claim that you need to buy a test because you have been in contact etc., you can see how people will fall for that, especially the elderly. (Please spread the message the tests are free.)

But even more troubling is that our entire banking industry remains a cynical conduit for criminal funds. The criminals require access to a bank account or credit card payment system in order to receive any money, and almost every citizen will have experienced how difficult it is to get an account these days. So how do the crooks always seem to have a means of taking your money? How come they are not instantly closed down when the very first complaint is received?

One answer exposes the utter incompetence and ineffectiveness of the reporting process, starting with "Action Fraud". We can perhaps forgive the Police themselves for not being cyber experts, but when they set up something to be expert, then you expect it to work! To be fair we know they are overwhelmed, so what has actually happened is that the bankers have sat back and let them take the flak.

The banks could stop a great deal of the fraud tomorrow, if they worked at it and (heaven forfend) actually spent money to do so. Furthermore the international telephone community could stop lining their pockets with the income from the criminal calls and do something about spoofing.

That they do not do so means that we have to warn you of risks that you should not be exposed to. The next time you read how much the directors within those two sectors get paid, please reflect on that.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

8 Phishing

This is simply out of control, with ever more sophisticated ideas from the criminal community that are designed to persuade you to click on a link and after that ideally to disclose information on a form that looks like the real thing, but is fake.

First, do not click on the link, even if you think it is a genuine mail.
Second, we are going to have to come up with new rules for the use of email, particularly where attachments are concerned, more on that below.

Third, be aware that this also applies to the sort of fun email that you receive from friends – and that is going to be hard to do because we have all shared jokes, cartoons, and perhaps short videos that we find amusing, or which creates empathy amongst connections that are easily lost otherwise in a busy world. The problem is to ask where the content came from in the first place. Criminals have cottoned on, create a funny, embed a viral link, and send it out – somebody will forward it in all innocence and Bingo.

What to do? Ideally use an entirely different form of document collaboration, but if you must use email first use a means of transmission that authenticates sender and receiver, so that you know absolutely that you are talking with the person that the address claims to be. The easiest way to do that is to use an encryption service such as Egress, or Outlook 365. Secondly only send information whose source you can unequivocally vouch for. If you have the slightest doubt regarding who produced it, and what hands it might have passed through, do not forward it.

Very sadly we have to find a means of replacing email, it is probably too flawed to ever "fix".

9 County Council use of email

Our apologies if this is becoming an all too familiar theme, especially as we recently covered the subject in respect to communications with the NHS, but it seems that certain Council departments will simply not get the message that it is essential to protect sensitive communications that they share with schools. We do understand that it adds "friction" to the exchange, sorry but that has to be true of all features that add security, and we know they are busy – we all are!

Clearly it does not pay to "go to war" on the subject, these are people whose support we need and rely on; we want great relationships with them. What we would ask is that you tell them that your DPO has insisted that all sensitive emails have to be encrypted, so blame us, but get the message across.

We do not want to wait for a serious breach to hit the headlines before we take it seriously.

10 Broadband for Schools

A useful guide from DfE to be found here

https://www.gov.uk/government/publications/choosing-the-right-broadband-for-your-school/broadband-for-schools-introductory-guide-for-senior-leaders

We would encourage you to talk to experts about your broadband provision; perhaps there is somebody within your Parent group who has specific expertise? It may be possible to obtain a direct fibre link, and if you are in a poorly serviced area you can not only underwrite the cost, but possibly contribute to your budget by providing a localised wifi service.

Many of you will be enmeshed in what was originally a local authority provided infrastructure, and you may be perfectly happy with that. But there are options, and we forecast that those structures will eventually disappear.

11 GDPR leaving checklist. For Staff Leaving the School.

At the end of summer 2018 a school produced this check list for staff leaving, and since it would appear that the end of the term is often a staff change time it is reproduced again, we hope you find it helpful.

1. All school documentation which identifies any individual (staff and pupil) stored on home devices is permanently deleted or personal identifiers removed: names DOB e.g. class list, planning, assessment spreadsheets.

2. All school documentation which identifies any individual (staff and pupil) on a portable device e.g. USB /phone is permanently deleted or personal identifiers removed: names, DOB e.g. class lists, planning, and assessment spreadsheets.

3 Hard copies of school documentation are returned to school and shredded or all personal identifiers: names, DOB etc. are redacted.

4. Staff email containing any information/documents which identifies any individual (staff and pupil) is not forwarded to personal emails. Please note that access to staff email accounts will cease on last working day (if earlier than termination of your contract).

5. (XYZ) Church of England School logins will not be used to access any websites or Apps e.g. Education City, The Key, etc. Please note that all access to school systems will cease on the

last working day (if earlier that the termination of contract). E.g. Website, KLZ, Maths No Problem, Cornerstones, Pupil Asset.

6 Copyright restrictions will be adhered to e.g. no duplicating any copyright resources e.g. cornerstones, Maths No Problem.

7. Resources or equipment belonging to the school will remain on site unless agreed with the Head teacher.

8. Electronic devices belonging to the school e.g. laptop or iPad will be returned to the school office on your last working day. All school documents on these devices either need to be saved onto the school server and/or deleted.

9. All school keys held are returned to the school office.

10 I understand that professional confidentiality applies in relation to all staff and children at the school beyond the termination of contract to ensure continued safeguarding and adherence to General Data Protection Regulations.

8/7/20

F Satswana – A future view

Predicting where we are going with education, with a specific focus on the privacy of data.

In producing this prediction we recognise that there is so much more to "school" than learning. Arts, culture, sport, manners, pastoral care, social interactions, belief, somewhere to belong, not to mention the essential contribution to the economy that enables parents to work whilst their children are safe and looked after. Whatever changes, those values will remain regardless.

Contents

1 Where next?

Much is talked about the "future", but it is only ever a logical progression from the past, and is only delivered by those with the vision and drive to create it, nothing happens in isolation. The purpose of this paper is to examine what is likely to be the future direction of education, within the specific subject area of personal privacy and protection of data. The context of privacy "by design and default" being the objective of current regulation. As such it is intended to assist an increasingly aware and competent population within the sector to decide on their strategic direction.

2 Who will benefit?

It is worth asking this question because the vast majority of the population never seek change and do not welcome it when it is forced upon them. Ask them with hindsight whether they would wish to return to how it was before and the answer is usually "no", they accept the development and enjoy the benefit it brings because they have got used to it – very few would abandon smart phones to return to BT call boxes!

Of course the point is that if your natural tendency is to view forecasts with cynicism and to reject and resist change, then this paper will be less compelling for you. That is not intended to be a critical comment, quite the reverse, society needs personalities of all sorts, and too high a percentage of "disrupters" would rapidly become chaotic rather than creative. But to be able to take a reasoned position within the discussion readers must be clear on their personality orientation towards the subject.

To do that may we call attention to the Herrmann Brain Dominance Instrument? In his brain dominance model, Herrmann identifies four different modes of thinking, and we would ask you to consider which most suits your personality?

- A. Analytical thinking

  Key words: logical, factual, critical, technical and quantitative.

  Preferred activities: collecting data, analysis, understanding how things work, judging ideas based on facts, criteria and logical reasoning.

- B. Sequential thinking

Key words: safekeeping, structured, organised, complexity or detailed, planned.

Preferred activities: following directions, detail oriented work, step-by-step problem solving, organization and implementation.

- C. Interpersonal thinking

  Key words: Kinaesthetic, emotional, spiritual, sensory, feeling.

  Preferred activities: listening to and expressing ideas, looking for personal meaning, sensory input, and group interaction.

- D. Imaginative thinking

  Key words: Visual, holistic, intuitive, innovative, and conceptual.

  Preferred activities: Looking at the big picture, taking initiative, challenging assumptions, visuals, metaphoric thinking, creative problem solving, long term thinking.

Clearly a type D personality is going to be more likely to be delivering a future strategy, but it will never be implemented without types A and B, and type C will analyse how we did!

3 Age groups

One final bit of "scene setting" is to establish some year groups for those being educated. Now this has been done before, in a number of areas, with different objectives. Our purpose in coming up with this specific definition is to provide analysis break points for where the approach to education will change according to the maturity of the child. We claim no particular science behind the choice, but are using a senary (base 6) approach to break age into six equal parts of six years.

Incidentally, to insert a slightly lighter element for a second, are you aware that base 6 was used by the ancient Egyptians, and that we all use their system to this day? How many degrees are there in a circle, how is longitude and latitude measured, how many minutes in an hour, hours in a day, how many pennies made a shilling in pre-decimal days? What other examples can you think of? They counted by calling the first one digit, and then adding five fingers! Of course all you mathematicians knew that!! (We also use base 2 in binary.)

Thus we arrive at the following, which hopefully will inform some of the projections to come:

a) 1-6. The nurture years, where infants are wholly dependent on care and compassion
b) 6-12. Prime development, acquiring all the basics of life within numeracy and literacy
c) 12-18. The formation and development of independent thought and character
d) 18-24. Identification and acquisition of key life skills
e) 24-30. The establishment years, finding their place in society
f) 30-36. Productive years, a time of peak performance

Why are we defining this, and specifically, why are we looking so far forward, to age 36? The answer is that we forecast that education will mean something entirely different to these year groups, so we cannot suggest a one size fits all solution. If we are correct we believe that society will increasingly value "education" right up to and including a time of peak performance, and that there will be an increasingly specialist approach to "teaching" at different levels.

Does it mean that there is no hope for you after the age of 36? No, absolutely not, clearly there is a time when wisdom and experience starts to impact as much as learning and education, and those inclined to continue to develop new skills will do so. But most people will have arrived at a form of apotheosis at that age, so the work of the education community will be complete.

4 The recipe

Clearly the major purpose of the regulation is to preserve and protect personal data from criminal exploitation or unwarranted disclosure. As such our concentration on future handling should be on the technology employed, on the base assumption that the original management medium of paper will be replaced by automated processes.

That is fine for the executive control functions, but if the education content is increasingly delivered digitally then it massively increases the interaction between data connections, meaning a greatly increased risk of penetration and exfiltration of personally sensitive data. So we have to regard the future educational landscape as one large system, and privacy has to be front and centre of everything we do.

It is for that reason that we have broken our thoughts down into a senary presentation; because we think that the systems are going to be fundamentally different as the person receiving the education gets older. Let us cease the preamble and get to the forecasts!

5 Core technology

We cannot tell you where the initiative for change will come from, but what we can say unequivocally is that almost every element of the technology that you are currently using today is compromised, incompetent, overly expensive, not fit for purpose and must be replaced wholesale.

If enough IT managers got together to ensure it happened, or an entrepreneurial group decided that it was the future for them, then it could all be delivered in a very few weeks – and if this paper acts as a catalyst for that consideration, so much the better.

Not that we are being clever in forecasting the future in this regard, all we are saying is that the principles behind the systems that power world commerce (and increasingly governments) be applied to the management of education.

Whether you call it supply chain management (SCM) or customer relationship management (CRM) – actually two halves of the same thing – business would not contemplate managing multiple databases. They demand an integrated information system that seamlessly manages production, sales, accounts and reporting – producing all the answers, all the time, and on time. Targets and budgets are constantly updated; managers react to exception reporting, with an increasing use of artificial intelligence handling the routine.

Schools could start to build such a system tomorrow. Begin by adopting QuickBooks as your accounting software and then add the associated Method CRM package to customise all your requirements.

That is just one route, with both Microsoft and Google providing an increasingly comprehensive suite of services to education, especially collaborative tools, both those armouries would be able to offer you suitable weapons.

In fact it would be better still if the supporters of the Open Source community – which would accord with the ethical beliefs of many in education – used not only the available options within free software, but also the development expertise that can be harnessed there.

Satswana says that the entire investment in almost every piece of software used in education today represents “yesterday’s men” and that none of them will be around in their present form in ten years’ time. You are paying too much, for too little, that requires too much training and dedicated attention, tying staff down who could be doing something far more useful.

We do recognise that there are barriers to change, not least the interface with data connections to local authorities and the Department for Education, for instance.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

Similarly there are vested interest groups that depend on having access to your data for a specific purpose, supporting further education objectives for example. Indeed if we return to our Herrmann categories, then there are going to be personalities that are dedicated to preserving the status quo and managing it well.

But we say that in ten years' time it will all be gone. It was never built in an adequate manner with privacy in mind, and many of the programs fail totally to deliver a proper log performance to determine whether there has been an exploit, and if so what has been compromised.

Perhaps the most telling reason why they will go however is that they are not making enough money, meaning that they are also not investing in future change.

Is this a clever prediction? No, it is an inevitable analysis, and if you want to see where change is already taking place then check out Catholic Education in Western Australia who presented at the (virtually ignored) Microsoft strategy session at Bett 2020. Some may run, but they will not be able to hide.

6 Connectivity

The distribution of schools nationally provides an ideal network for terminating a fibre backbone with diverse back up routes. That could then deliver local "high speed Internet" as a community service, and at the same time provide the school itself with peerless connectivity.

If that was to be State sponsored, then Satswana believes that would be a good use of infrastructural investment, but if not we can obtain a commercial provision quote for you. It could possibly create an additional income stream. However it happens, we forecast that all schools will have a direct fibre termination meaning that access speeds to "the Cloud" would never be a problem.

The cloud has to be considered part of the answer to protecting data because the organisations managing the service can afford the staff and investment to continuously keep abreast of breach threats. It is not the total answer however, and even the most passionate supporters of "cloud" have come to accept that a hybrid solution, with a local server for specific applications, will be with us well into the future. (Print server, CCTV storage, biometric identity etc.)

Satswana forecasts conceptual development of this local server with an integrated "next generation" firewall holding threat intelligence tables and predictive anti cyber threat software such as is produced by Dark Trace. It may well be remotely managed

by a specialist IT organisation, but we do not see any future for the organisations that define themselves (for instance) as “Grids for Learning”.

We understand their origins, and their wish to retain central services that are then contracted for, but see their holding of data as being an additional weak point that provides no benefit for the school. The fact that one such “managed service provider” disgraced itself this year by failing to protect their unencrypted data (how come?) from an attack demonstrates that they have run their course.

Future schools will have unmatched connectivity and speed, not least to deliver networked educational resources that we cover further on.

7 Messaging

As brilliant as email has been as a communication tool over the last thirty years its security was flawed at the first design stage, we do not expect it to exist at all in thirty more years. It will be replaced by message structures that are totally encrypted (thus protected) that are delivered directly to the recipient, probably involving multi factor authentication of the sender and content, as well as providing an acknowledgement from the receiver so that a complete audit trail is available. Messages will be auto filed by content and subject to planned deletion timescales. There will be both call and video options to the text of the message.

8 Personal data

Perhaps the biggest revolution we forecast is that individuals will retain total possession of “their” data and only consent to its use for a given period of time, and in defined situations. This has massive implications for circumstances where the State determines that there is a statutory requirement to have access to personal data, and injects complications into the design philosophy behind the provision of a single incidence of information within a database.

However it makes sense that those who now have the right to ownership of their data also accept the responsibility to look after it, relieving any institution of any sort from the risk and liability of keeping the information safe within their own software. Of course they must still have appropriate access to data that is required for statutory purposes, such as employment, tax, or indeed school admissions, but it can only be used for the purpose for which it was provided.

Organisations are already working on a control structure to provide a solution, and early versions are likely to emerge this year, making a re-think of current legacy systems even more urgent. The assumption that a system owns and controls all its data in a central environment has become so embedded that there are very few examples of anybody thinking outside that “box”, but actually it has become more

pervasive than you might have imagined. How about all those "apps" that we are adopting on our phone that depend on the geo-location provided by our smart devices?

Just as you can turn off the consent for revealing your location, so will you be able to manage consent for the use of your personal data. Instead of losing all your data to a hacker as British Airways did, you will only allow them to access it for the purpose of the air passenger information you need to provide for a flight – and any other access or use is forbidden. It is true that will constrain a lot of misuse of your data, but isn't that the point?

It means that schools would no longer be liable for compensation for losing data that they had to control to manage their function. Both Government and local authorities would have to totally re-think the manner in which they control admissions, for instance. If there was a statutory requirement to retain access to information then the data owner would not be able to block consent for the required period, those issues will have to be managed, but it will mean that everybody knows who has access, for what and for how long. It is designing privacy into the system, and delivering it by default.

9 What is education?

Before we go any further may we go back briefly to definitions? Is education a business sector, or a social service? The answer is important if we are to forecast its future.

We suggest that it has to be regarded as a business, not least because all schools have to operate within a budget, and if you fail to balance income with expenditure then there are consequences – including bankruptcy for the private sector, something that may become far more prevalent after recent disruptions.

If that is so then a part of the future has to be consideration as to where the money is going to come from, how can you increase your budget, or alternatively protect it from being reduced? We have identified distributing high speed Internet bandwidth, what else might there be? As we go along we will seek to identify more ideas, but first, what about that aspect of being a social service?

Very many people in education will have entered the profession simply because it was not part of the cut and thrust of commerce, because they felt a degree of "calling", wanting to make a difference, and indeed a great deal of your time will be involved with the care and concern for your charges that goes well beyond the simplistic teaching of a subject.

In recent times your role in looking after children, and indeed ensuring that they are properly fed, has become more recognised, and it is Satswana's belief that the school of 2030 has far more to contribute in this area, and should be provided with an appropriate budget to reflect that.

It has relevance to one of the specific exemptions from GDPR, being the provisions of "Keeping children safe in education". Teachers will always be the first safety net for a child, or indeed at any stage of their learning, nothing else even comes close, and we suggest that role has to become more centre stage in the future.

10 Digital education

Three months ago this paper might have been very different, but the recent experience of the Covid 19 period has already challenged many cosy assumptions and forced us all on a path to change, together with many other aspects of society.

Dare we suggest that "chalk and talk" has gone for ever? If so, what does that mean for the charismatic communication skills and interpersonal ability represented by a "teacher"? Where will the motivation come from if you are just managing a timetable of resources, and what does that imply for future training requirements?

It is from this perspective that we wish to introduce our age breaks, since we see each having a different connotation, just as we see the pupil being in a different stage of development, so also do we expect the role of the teacher to be stratified accordingly, let us explain.

a) Age 1-6, care and compassion

This is the area where we see the least impact on change to the traditional role, but we do see the social welfare component needing more recognition, and also funding. We want children to be happy, learn through play and social interaction, so concerned and loving teaching staff will always be beyond price.

Where parents are at work, especially in a single parent household, you are possibly more "in loco parentis" than you ever planned to be, but even more important as a consequence, especially if you are picking up deeper problems.

If the Government are to review institutional behaviour under many subjects, then Satswana feels that the role of social services within local authorities are a suitable case for treatment. We forecast that teachers will be recognised as being better trained and better equipped to identify early stage dysfunction, with the skills to initiate remediation. If the tools for direct action are delegated to them to use, then there is less personal threat, not least to the information flow.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

In too many instances too much of what used to be the function of the family has become fractured, leaving children at a vulnerable age with an absence of guidance and direction. The school of the future must act as the safety net to protect and fulfil the promise of such children, and society must ensure that they are funded to do so. It has to be absolutely the best investment that we can make.

b) Age 6-12, prime development

Nothing will ever be the same again. We are not quite sure where the break point will be. We do not suggest that you go straight from care and compassion to red blooded force feeding of numeracy, literacy and all the other aspects of the curriculum, but we expect its presentation to have changed dramatically, not least because, for a period, parents had to take the role of teacher. OK, you supported them with advice and resources, but what else changed?

In terms of impact you cannot ignore the results achieved by platforms such as Seneca Learning (https://senecalearning.com/en-GB/) and there is going to be huge competition amongst providers to create the most compelling and memorable content. With great respect no individual teacher, with just their personality as a resource, will be able to compete with that, no school can employ sufficient teachers to cover the entire range, contentiously they may not need to.

So teaching will become a resource management role, ensuring that pupils concentrate on the material within a structured learning environment and providing social interaction regarding the content, but not delivering the prime lesson. That will be digital, and in the not too distant feature it will be enhanced by virtual reality. The future geography lesson will actually “go to” Niagara Falls, the history lesson will be present at the Battle of Trafalgar, goodness it will be exciting!

Perhaps not so much for the teacher, you have become a manager, though your social role will continue to be as demanding as ever. Will that give you time to be more creative, arranging school trips, developing beyond the school? We will cover that later, but in the meantime we suggest that you will always rejoice in seeing the fulfilment of your charges as you ensure they are equipped for a challenging future.

What about the educational record that we are building? We forecast that this will be more detailed than it ever could have been in the past, with subjects covered and achievements gained being recorded in an automated manner that would have been inconceivable before. It will be a constant measure by which to track improvement, and for you to change content and providers, ever seeking perfection. Experience will make you more and more expert; it will be a new world for you and your charges.

c) 12-18, Formation and development

When do they cease to be a child and turn into a young adult? Individuals differ, so there will be no rule, and in any event the set curriculum in the early years will mean a reliance on a digital learning medium and content presentation that will not be dissimilar from the Primary stage of their lives, similarly the teaching role will be the same.

Except that at this sort of age there are some even more brutal challenges for the teacher in your social role and it probably will not get any easier or safer. Drugs, bullying, gangs, peer pressure, social deprivation, mental illness, diversity confusion, puberty and denial, it has become a far more dangerous world fuelled by social media and mass instant communication of everything you can imagine, and more that you did not.

So is the teacher of the future a counsellor and friend, or a mixture of disciplinarian and police? Indeed, can they extend the use of digital information media to add social lessons to the essential subject learning, if so how? To save a child from skunk induced schizophrenia or the even worse tragedy of depressive illness leading to suicide was probably not what you came into the profession for, yet it could be your greatest achievement.

We reflect that two hundred years ago they would not have been in education. The lucky ones might have gone to sea as a midshipman; too many others would be condemned to going down a mine. Have we advanced?

To cease reflection, the law says that from the age of thirteen they are responsible for their own decisions regarding their personal data, whatever we seek to do with it requires their consent. Satswana thinks that sixteen would be a more appropriate age to assume that responsibility; will Parliament change its mind?

d) 18-24, key life skills

You may reasonably ask why we are including this age range in our forecast of the future, and the reason is simple. If education is to any extent a “business”, do you really want to lose track of one of your customers, or would they still contribute in some manner to your budget? In the alternative, is there an unrecognised educational imperative within this target range that can be identified for the benefit of society?

We further postulate that if the student has been used to learning through digitally inspired media since perhaps the age of 9, providing the resources are controlled, managed and presented to them to meet their learning objective, does this require the “label” of the XYZ school? Can anybody provide that resource, especially somebody that they know and trust from the past?

What seems very clear is that the role of the university is likely to be unrecognisable in two or three years, indeed it is surprising that their bluff was not called some time ago. To dictate that a degree course had to take a fixed term, at a fixed place at a fixed price, with only the occasional lecture to attend was surely always a confidence trick. It is recognised that perhaps "university life" was something entirely different, but since the writer joined the Army at 17 in order to have somewhere to live, that is not regarded with much sympathy!

We forecast that the role of learning, to change the word from education, will be very different in the next ten years. We use the word learning because those doing so must be personally motivated to acquire additional knowledge, and they must not be constrained by age, cost, or time. In a past life three of us were required to pass the Stock Exchange exam, a three year course. We all crammed for a week and passed.

With new tools, new approaches to courses, fresh attitudes, and our young people can afford false starts, try different things, put things down and pick them up again – not accept crippling debt. A three year degree course in a week, absurd you cry! Why? And what might be the role of an Alma Mater in assisting that?

We are not suggesting that there is no future role for universities, clearly there is for some subjects, and the pure search for academic development will always have a place and appeal. But we do say that many more people will have flexibility in what they study, with the acquisition of related qualifications, based on brilliantly presented learning material, and that both society and the individual will be the richer for it.

e) 24-30, finding their place

Substantively our argument for including this age range is the same as in d) above, except that we have gone a bit further on in life. We would continue to state that an Alma Mater could have a commercial role in ensuring support for any learning needs.

f) 30-36, the productive years

Perhaps the time when the past student can start to give something back, can you for instance contribute any resources towards the training needs of the organisation they are involved in? Can they contribute unique learning and experience? What motivation can they provide for a current teenage generation?

Our purpose has been to construct a forecast of what the future holds when education can be delivered in a perfect form, every time, at any time, no longer dependent on the one to one of a trained teacher. It will be different.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

11 Can we look beyond our immediate boundaries?

Now for a challenging statement, if within the era of digital course presentation teaching staff have become managers of resources and time, why should you be constrained by space and distance?

Can your teaching specialist institution, because that is what you have become, extend your writ to embrace – shall we say a remote African village school? If you can, and within the very near future we will be able to "be there" on video as easily as we conference today, what would be the value to you, your students and the remote pupils for such a relationship? Would it boost your budget?

12 In conclusion

The "local" school now has an international reach which is as far as the imagination can take you, taking achievement to new levels whilst doubling down on essential safeguarding and social concern with an essential safety net. Some of you will have an unimaginable impact.

About the author

Of course I cannot always be right, but I do claim to be a type D personality, and there are a number of things that I have been responsible for that you will take for granted.

With every one of them the "idea" was originally met with doubt, and in some cases derision, so I became used to cynics!

My first material "invention" was the electronic data collecting petrol pump in 1969, it was the foundation of all retail information systems and in 1976 we conducted the first ever online credit card transaction. It was at 200 baud, over an audio coupled modem, and had to include an OCR signature as bank inspectors stated they would never accept a payment that was not signed!

In the early 80's I was responsible for the upgrade within the City (leading the world) from video switch to digital dealing rooms, and then subsequently to founding the first electronic stockbrokers. In the early 90's I founded the first business internet service provider, now part of the biggest provider in the world, we pioneered early firewalls with Cisco.

Thereafter I worked in exchange technology, winning a worldwide contract to provide Nepal with its control software in 2006 and establishing commodities policies with UNCTAD. Satswana was founded to concentrate on cyber security, and

we are content and satisfied to provide our school customers with a very personal DPO service.

Thus a lifetime of creating digital change has come back to talking about it together! Like any chef, you are only as good as your next meal!!

G September 2020 Update

Contents

1 Audit data

For those wishing to ensure that they are up to date with all aspects of data protection we seek out audit options that you can go through. In truth, they often cover the same ground, but in a slightly different manner, and in any event they serve as a useful refresher exercise. This option comes from no lesser body than the National Cyber Security Centre, and whilst it is aimed at Governors and Trustees, it has equal value for anybody charged with the data protection task. The detail can be found here https://www.ncsc.gov.uk/information/school-governor-questions

2 Issues with Class Dojo

You may be aware that Satswana do not regard Class Dojo to be DPA compliant and The Times found that they were sharing data with 23 other organisations – presumably to give the investors who subscribed $65 Million recently a return.

Herewith a cautionary tale on the difficulties they make when you want to remove data.

We have to balance that with the school's finding that the product was extremely useful and helpful in a remote learning situation, and for that reason they will continue to use it. However over time they plan to consider alternatives.

A correspondent writes “A bit of an update. I have been having a bit of a back and forth with Class Dojo over the last week or so trying to get our children removed from their systems. They are not making life easy but I have finally had assurances that the process they have given me will remove the children's content, photos and details but it is ridiculously onerous.

They have said we have to remove every activity, child and class post individually which is very time consuming and although I have now managed it for my class and it has taken ages. However the main problem is you can only remove your own class posts so any photos any other staff have added need to be removed by them.

Therefore the only way we can remove photos on our class story will be for each individual teacher to go in and remove their own posts.

That means I am anticipating having to ask Y1 and Y2 teachers to go back and delete all their posts from this last year with children's photos in which is a long job (Y1 don't really need to do it this year but it might be a nightmare trying to guarantee staff are around to do it next year).

I have asked whether we or they can't just delete the whole class and all the content and they have said they can't do that but will put in on the development list to be discussed.

Just flagging this as this is going to be an issue every year (although more so this year with lockdown) and I needed a rant.”

3 Relying on US based servers, more on the subject

There are many glorious things to say about the United States, a Country which throughout our lifetime has been associated with our defence and protection.

However, their attitude to personal privacy has distinctly different origins, in their case enshrined in the First Amendment to the Constitution. Contrast that with what you might describe as the Napoleonic Law origins of GDPR.

Freewheeling do – as – you - like may have many benefits, as against legalistic prescription, but not we suggest when it comes to personal privacy, and we earnestly recommend that if the organisation that you are dealing with holds its data in the US then you discontinue a relationship. Please forget the honeyed words about EU/US Privacy Shield, unless you are prepared to overlook that each organisation certifies itself, and if you want to make an issue of it then you must use US Law in US Courts. Do you think that you are going to win, even if you can afford it?

When the option is to have the security of a regulator to fight your corner, and all any organisation has to do is to locate your data within one of the European Countries that support GDPR – which is almost 100% embraced within DPA 2018 – to give you protection; then why would they not do that? If they will not it is because they are making money out of your data, which is their business model, entirely acceptable in the US, but increasingly not here.

The point emerges again as we read that another half a million people have been hit by a cyber theft, with amongst others internationally the universities of York, Reading, Leeds, and Oxford Brookes, as well as charities such as Young Minds. An expert said that the data taken would make them all subject to phishing attacks, which in turn can compromise every server they rely on.

So how come these august organisations were relying on a company called Blackbaud? Some credit must go to the organisation for apparently frustrating a ransomware attack, but why was all this data allowed to be stored outside the reach of European regulators?

We accept that US companies offer great products and great services, that is why they are worth so much and people want to use them, but nevertheless if they refuse to support their European customers from a European based server – then you in turn should look elsewhere. If enough people demand that, then you will get good service and protection for your data.

4 Google for education

Comprehensive information from Google to be found here
https://teachercenter.withgoogle.com/

Candidly we are not fans of Google's approach to personal privacy, even in going to this URL we found we were tracked – clicked on the email and the address line had "campaign" in it, deriving petty amusement from clicking on another heading and then back to 'Home' to get rid of it. Finding jingoistic annoyance that they cannot spell properly, as in 'center', the trouble being of course that they do, because they can, and we are powerless to stop them.

And the reality is that they have some superlative products that have made a considerable contribution to society, to the point that we use the name as a verb. Google maps, with its satellite view and associated street view is just remarkable, as is their translation software – that does so much more than translate your documents – it can be embedded in development code so that you can market in any language. Will their software be driving us around in just a few years?

Education has to be the richer for having two behemoths fighting for the market, two immense development teams constantly aiming to be better, to increase protection – push back against the brilliance of a disenfranchised criminal community, who turn to exploitation when other legitimate paths to earning a living are blocked. What else do you do if you happen to be North Korean with a double first? Unconsciously they also contribute, why otherwise would we have levels of encryption that even state actors cannot penetrate?

So despite our preference for what we consider to be the more serious, disciplined and professional approach of Microsoft – not least because they have never made profits from selling your data – we must also set to and learn what Google can do for education. Because you will never stop learning this sort of resource is essential so that every individual can answer their own questions, proceed at their own pace. We do live in an amazing world.

5 ICO Guidance on AI and data protection

The ICO have requested us to give the widest possible publicity to their latest guidance on artificial intelligence and data protection, to be found here https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection/

Broadly speaking an impact assessment is required as for any other software innovation.

The ICO would specifically like to engage with any organisations adopting AI solutions to ensure their guidance remains relevant. Volunteers are invited to register.

6 Secure email

We found another important "thought process" paper here https://www.gov.uk/guidance/set-up-government-email-services-securely and we are currently seeking advice from the ICO as to whether a County Council should be obliged to use encryption to protect safeguarding data, a decision that we will publish when available.

It seems to us that the recommendation is clear, extract as follows:-

"As an information owner, you're responsible for managing your organisation's security risks. You should consider the protection of your data at rest as well as in transit. There is no standard list of approved, secure email domains for government. Your organisation must decide what assurance you need based on your own data and your own risk profile.

You need to understand possible risks when sharing information with other organisations and take steps to help protect your data. There are a number of approaches you can take to protect data including:

- checking to make sure the recipient has independent accreditation that shows good security practice such as Cyber Essentials Plus or ISO 27001
- asking the recipient organisation about their cyber security practices using the 10 steps to cyber security guidance
- creating a data-sharing agreement between your organisations
- relying on the reasonable expectation that the organisation you send data to will protect the data as required by legal or regulatory requirements like GDPR or the NIS Directive
- using additional encryption methods described above to protect the data in transit and at rest so you do not have to get any security information from the recipient.

7 Legacy networks

In conducting research on this topic we also came across the following advice here https://www.gov.uk/guidance/moving-away-from-legacy-networks
It seemed to be particularly useful at a time of potential change in the education sector, perhaps from on premise, or reliance on a formerly local authority provider, to either a cloud or a hybrid server structure. It is reproduced for your consideration, with the expression a "single source of truth" being particularly notable.

"You should follow guidance on moving to modern network solutions which are generally more flexible, current, cheaper and quicker to deploy than using bespoke services over dedicated networks. DO not use public service network psn
Work better across government by using commonly available tools such as instant messaging, voice and video messaging, secure file sharing, and the APIs that support these services

You should consider providing a digital service to give other organisations access to information rather than emailing attachments. This means everyone will have a single source of truth, which will improve cross-government collaboration.

This single source of truth will help to manage and control your data effectively and lawfully. Users in other organisations will then always be able to access the most recent version of any data record, rather than referring back to old copies in their mailboxes.

8 Minimum security standards

Similarly we discovered this site on minimum security standards
https://www.gov.uk/government/publications/the-minimum-cyber-security-standard
Four key words, Identify, protect, detect, respond, recover

9 Zero Trust

Consideration of these issues prompts us to continue to watch for the eventual adoption of Zero Trust that will also eventually offer passwordless access. Those wishing to study the subject may benefit from the following explanation.

Zero Trust assumes that nothing inside or outside of the enterprise perimeter should be trusted and the network must verify anyone and anything trying to connect before granting access. Connectivity is only granted after identity is authenticated, the security posture of the connected device is verified, and the user or thing is authorized to access the desired application, service or information.

First, a Zero Trust Secure Access solution must enable enterprise mobility to boost workforce productivity. This requires enabling visibility and compliance controls in a transparent way across different devices and operating systems. It involves simplifying the secure use of mobile devices by offering automated, self- service onboarding of devices – whether they are laptops, smartphones, or tablets – regardless of user location and device ownership.

Mobility enablement also requires the ability to ensure compliance by isolating work applications and data from private applications in BYOD scenarios. Lastly, a Secure Access solution must support always.

A Zero Trust Secure Access solution must also take into consideration users' consumer-based expectations for a simple, integrated user experience (UX). For example, end users want the convenience of Single Sign On (SSO) to applications across devices, operating systems and application infrastructures. IT administrators demand an intuitive and flexible way to orchestrate all elements of access security – freeing them from the need to correlate data and actions across multiple security systems and consoles. Additionally, a best-in-class solution will optimize the user experience by leveraging an integrated Application Delivery Control (ADC) solution, guaranteeing timely response to meet any demand, regardless of whether users access applications on site or remotely.

The increase in cyberattacks coupled with the move to hybrid IT environments means that a Zero Trust Secure Access solution must offer end-to-end hybrid IT security. Such a solution should combine SSO authentication with role-based and

device-compliant authorized access to applications, whether the applications are hosted in enterprise data centers, private clouds, or public clouds, or are delivered as SaaS. Software Defined Perimeter (SDP) offers a compelling, "Zero Trust" architecture that can be applied to new or existing hybrid IT deployments. SDP prescribes an "authenticate and verify first" approach that renders resources invisible or inaccessible to all users and devices until an explicit authentication, compliance check, and authorization have been completed. The overall result is a "dark cloud" where the attack surface of the network is diminished because hackers can't attack what they can't see.

The difficulties associated with multiple security silos can be mitigated by adopting a unified Zero Trust Secure Access platform

H Satswana October Update 2020

Contents

1 Privacy Notice Coronavirus Track and Trace

(Providing you with the legal support basis for responses)

The school has an obligation to respond to the Government's advice on Covid 19 and the development of the NHS 'Track and Trace' scheme is a key part of the Government's plan to manage Coronavirus.

It may be necessary for us to share the data we hold when requested to do so with the Public Health NHS (National Health Service) Track and Trace Workers.

We expect that we will be asked to provide details, including contact details, of any cases of Coronavirus (or a suspected case) that may arise within our school. We have an obligation to share this, and any other health data, as part of our Public Duty as set out below.

The law on protecting personally identifiable information (Data Protection Act 2018) allows Public Health England to use personal information collected by NHS Test and Trace.
(Originally Article 6(1)(e) of GDPR but Section 8 of DPA 2018) : "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 controller".

As information about health is a special category of personal information, a further section of the GDPR applies "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare".

Public Health England also has special permission from the Secretary of State for Health and Social Care to use personally identifiable information without people's consent where this is in the public interest. The law that applies here is Section 251 of the National Health Service Act 2006 and the associated Health Service (Control of Patient Information) Regulations 2002.

2 Providing References, a safeguarding option

Whilst on the subject of exemptions, may we stress that the content of references was specifically excluded from the DPA 2018. It used to be the case that the originator was privileged, but disaffected parties discovered that they could demand the content from the recipient. That distinction has now been removed and all references are exempted from disclosure following a Subject Access Request.

All the discussion of case law considers this matter under the employment heading, so where do we stand when a Head requests a reference on a pupil? We must advise that a qualified legal opinion came up with the view that consent had to be sought to provide it. Now clearly Satswana should not be disputing a qualified opinion, but we simply cannot see how that can work in practice, how can you ask for consent to provide information that you are not prepared to disclose to the consenting party? Every reader of this update will have experience of the sort of disaffected parent who has a totally different view of the child to that of the school, and it is almost certainly critical to understanding if the information is shared in an educational environment.

Three options follow from that. First you can seek the consent of the person responsible to provide a reference, secondly you can refuse a reference, or thirdly, you just "pick up the phone". Many of you will have opted for the last course.

However there may be circumstances in which you consider that you should pass information that has a safeguarding impact on the child, and then we contend that the GDPR/DPA 2018 conditions no longer apply. Indeed within the revised Keeping Children Safe in Education 2019 the expanded commentary on information sharing has moved this clause to 85. "The Data Protection Act 2018 and GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Before that Clause 82 has "Information sharing is vital in identifying and tackling all forms of abuse and neglect. As part of meeting a child's needs, it is important for governing bodies and proprietors to recognise the importance of information sharing between practitioners and local agencies. This should include ensuring arrangements are in place that set out clearly the processes and principles for sharing information within the school or college and with the three safeguarding partners, other organisations, agencies and practitioners as required. School and college staff should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to the local authority children's social care."

And 84 reads "Governing bodies and proprietors should ensure relevant staff have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the GDPR. This includes:

• being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as 'special category personal data'.

• understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows practitioners to share special category personal data. **This includes allowing practitioners to share information without consent** where there is good reason to do so, and **that the sharing of information will enhance the safeguarding of a child in a timely manner but it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.**

• For schools, not providing pupils' personal data where the serious harm test under the legislation is met. For example, in a situation where a child is in a refuge or another form of emergency accommodation and the serious harms test is met, they must withhold providing the data in compliance with schools' obligations under the Data Protection Act 2018 and the GDPR."

This clause concludes with "Where in doubt schools should seek independent legal advice" and we would not wish to counter this in any way, you will make up your own mind.

3 The growth of email

Covid has forced the pace of digital change, but it was a surprise to find that video meetings only came third in the growth stakes, behind live chat which was first and then the product most of us would consider to be an antique now in a strong second place, being email!

That means that there has been a great deal more dependency on a product that is fundamentally insecure and which is used far too much as a "filing system" in place of any other record, not least by this writer who knows that change must come, just not yet please!

We all should be considering deleting old mails and retaining essential history in an appropriate location, something that is easy to say and a challenge to execute, especially if society is placing more reliance on email, not less.

Requesting emails has become more and more a feature of subject access requests and even if there is no information that might be inadvertently disclosed within their content it is nevertheless a tiresome business going through them all extracting and then redacting. It is a principal of GDPR that "the data you do not keep is the safest".

The nuclear option – that we only recommend following extensive warnings and time being allocated to allow change – is to ensure that your system deletes all emails that are over 30 days old. If information should be kept then it must be "filed" (against perhaps the pupil or staff member record) - then it will be recognised and saved.

The result will be that you will always have the information you may need in a single place, and you will be able to respond to requests in the most satisfactory of manners, by stating "the school retention policy ensures that we do not keep emails beyond thirty days".

4 Launch of the Children's Code

The Children's Code came into force on the 2nd September, which triggers the start of a 12 month transition period for organisations to make any necessary changes.

All major social media and online services used by children in the UK will need to conform to the code.

https://ico.org.uk/for-organisations/childrens-code-hub/

5 Data matching exercise

Referring back to our covering email where we comment that Government can always excuse itself from complying with laws that it has passed, we find that schools are required to provide information on aspects of employment under the guise of ensuring that no fraud is committed. I fear that we found the following statutory support for this added imposition

"The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under data protection legislation or the GDPR."

6 Microsoft update of terms

We would not blame most of you if you just deleted the emails that tell you that a major corporate has updated its terms, after all – what could you change if you disagreed?!!

However, in the latest version there is one nugget of information that is worth noting; especially in the context of the Data Protection Act, and that is the legal location of the entity that you are contracting with, in this case in Ireland. This is what they say:-

In the Contracting Entity, Choice of Law, and Place to Resolve Disputes section, we've clarified that if you live in (or, if you are a business, your principal place of business is in) the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom, and you are using cost-free or paid Services, you are contracting with Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland (registered at the Companies Registration Office in Ireland under number 256796, VAT registration number: IE 8256796 U, with a registered address of 70 Sir John Rogerson's Quay, Dublin 2, Ireland).

Please also note the following in case it may have some relevance to you:-

In the Kids and Accounts section, we've clarified that by creating a Microsoft account or using the Services, you and your parent or guardian accept and agree to be bound by these terms and you represent that you have either reached the age of "majority" or "legal responsibility" where you live or your parent or legal guardian agrees to be bound by these Terms on your behalf.

7 Phone Privacy

Because of its security and privacy features we are fans of Mozilla Firefox as our browser of choice and we reproduce below some very useful thoughts they have provided on phone security, naturally promoting the use of that browser on your phone!

But remember please also the Satswana advice if (as we all will be) we are using a personal phone for "business" purposes. First, the phone should be secured with an access passcode of some sort, with many clever options such as a fingerprint being available. Secondly, the data encryption option should be selected. Many phones may have this set by default, so you may not even be aware that you have it, so do not be concerned by its use. Finally the remote auto delete capability should be selected within the "find my phone" feature, because if it is permanently lost or stolen, then you can erase anything sensitive. If your information is backed up "in the cloud" then any new phone you get should be able to recover the data.

Incidentally, we noted in the Press that Google have been asked by the Police to give them information on any phone use or presence close to a scene of crime at the appropriate time. We will not argue here whether or not that is a pragmatic and sensible use of Police powers, or a gross breach of privacy – it is probably both!

This is the Mozilla advice, together with links you can follow:

> **You shouldn't have to worry about your privacy**
>
> It would be great if the makers of your apps, favorite sites and devices had your best interests at heart — but unfortunately, most tech makers put profit over people. Controversial opinion: that's not ok.
>
> There are easy ways to put your privacy first. Start with your mobile device:
>
> **1. Adjust your phone's permissions**

Prevent apps from accessing your info, and stop your phone from giving it away.

2. Change your phone's name
Fellow cafe patrons (or nearby hackers) don't need to know your name.

3. Clean up your apps
Old apps don't need to hang out on your homescreen... or collect data without your permission.

And when you get online from your phone or tablet, use Firefox for Mobile to keep your web activity and personal info safe and private.

I Satswana Half term update

Contents

1 Privacy Shield invalid

You should all be aware of the monumental impact of the following judgement from the CJEU
"The Court of Justice of the European Union ('CJEU') announced, on 16 July 2020, that it had issued its judgment ('the Judgment') in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) ('the Schrems II Case'). In particular, the CJEU declared the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection provided by the EU-US Privacy Shield ('the EU-US Privacy Shield Decision') invalid, but found that nothing affected the validity of Standard Contractual Clauses ('SCCs') in light of the Charter of Fundamental Rights."

Regular readers of our updates will not be surprised to read this, since we have constantly said that Privacy Shield was only really a revamped Safe Harbor, which had been declared non-compliant in 2015, and its "self-certification" basis was clearly unsafe.
What it means immediately is that any software that you are using that relied on Privacy Shield to be GDPR (DPA 2018) compliant is no longer so and as a consequence Satswana has urgently started a review exercise of the status of organisations in our Processor list.
We believe that there are two arising practical realities that should suggest that we all take a calm and measured approach to a reaction, the first being that you must be given a reasonable time period following the judgement. You cannot be expected to change a software control process that you are reliant on overnight.
The second is that affected suppliers should be given a reasonable opportunity to respond with a means of becoming compliant, something that can be achieved by simply moving their servers into a European Country. You may recall that in our recent review of Microsoft's terms and conditions they had specifically stated that all contracts were placed with a registered entity in the Republic of Ireland which put them in a great position.
Thus we suggest we should not prejudge any position, all suppliers must be given a chance to put a remedy in place, and Satswana will be contacting all those that currently "fail" so that we can monitor whether they change or not.
It will be our intention to conduct this work over the next two months and provide you with an updated processor list in January with either an assurance that your supplier is working towards compliance, or alternatively with a list of organisations that are not cooperating and whose use you should review.

2 No deal?

Which brings us to recognise that at the time of writing we still do not have a "deal" with the European Union for the end of the transition period, meaning that "data" may yet be used as a weapon by politicians who make five year olds arguing in the playground appear mature and logical.
Three arising thoughts, the first being the absolute "equivalence" between GDPR 2016 and DPA 2018 should ensure that even if we leave on what they choose to call Australian terms, then it appears that "mini deals" will be done, and surely to create one of those with data will be the easiest possible immediate solution to avoid mayhem.
Secondly, even if one of the 27 really throws a tantrum, then in reality they will actually have materially less success than King Canute in actually putting a stop to the established data flows on the Internet, and they will discover that there is no point in a law that you cannot enforce.
Finally however, you should all be aware that Europe will continue to claim extra judicial control of the data of any Continental children that you have in your School. Can they do that? Of course only a real Court decision can answer that, but consider

the evidence for acceptance. Worldwide (except for within the US) GDPR has been accepted as being good and useful law, to the point that most countries accept its application – at least as far as European data is concerned, but in some cases effectively adopting the principles within their own law, or being considered as being equivalent (such as Canada.) It is not worth fighting over!

3 How do we define backup?

Having a background in cyber security, Satswana are constantly researching, listening and reading anything we can find on the subject to find new ideas, fresh techniques, analyse changing risks.
So it brought us up short when we realised that we were taking "backup" for granted in the sort of SAAS environment that we are increasingly relying on, whether that is Microsoft 365 or Google's G Suite, or any of the other applications that can be found "in the cloud".
What we discovered is that whilst all these organisations will store data for a period the techniques deployed do not fulfil the definition of a backup, which is to hold a separate copy of your data that is stored elsewhere. Indeed if we dig into the small print we find that Microsoft talk of a shared data responsibility, with "data in the hands of the customer". In other words, it is your duty to look after it, not theirs!
Your IT people can be forgiven for missing this, as we did, because of terms like unlimited archive, litigation hold and third party backup, but nothing ensures that your data is retained for legal compliance periods. If you suddenly find that you do not have your finance records going back six years it is you that will be in trouble, similarly where pupil data has to be retained until age 25.
So this is a subject for both SLT and Governor's agendas, especially where you are updating and upgrading your digital options – something that may have scaled significantly in recent months. Are we sure that in adopting change we have considered the basics, such as backup, retention periods, and disaster recovery? Furthermore are we getting the best service in that regard? Satswana were impressed recently by finding that a backup supplier automatically confirmed that there had been no unexpected changes before backing up the data, something that should catch a ransomware attack before it infects your historical records. That is really useful, especially as hackers often wait a few days to ensure that your whole archive has been infected before declaring themselves. We have offered consistent advice to take occasional backups onto media that you remove entirely from your network as a protection against having all your files encrypted by an attacker, because then you retain your history even if your most current changes become lost. Having a procedure attached to your backup that identifies the problem is even better.
We are proponents of change but recognise that it is not universally right for everybody. We have schools that still rely totally on paper for their records and their security issues are actually minimal. Do we rush into the cloud, or does "Office 2010"

still do everything you need? It appears there may be unexpected consequences of change, and as ever it may be better to "make haste slowly".

4 Controlling video reproduction

In this difficult period many Schools are creating videos to share with parents in the absence of parent's evening's etcetera, and one teacher was concerned that this could open the door to data being shared on social media. The original idea was that some form of disclaimer could be attached to the recording to the effect that it was not to be shared with social media, but we could not find any real legal basis through which a statement of any sort could be supported or enforced.
Our conclusion was to invoke Copyright in the following form: © 2020, this video is the Copyright of the producer and must not be viewed, copied, or provided to any other party other than the intended recipient to whom it was addressed, for which a record is held by the School. It may not be saved, downloaded, shared or posted to any form of social media or third party.
We think that means that if a parent should upload it then the platform is obliged by Copyright Law to remove it, and there is a basis for an action against the offender.
The "record" should be the email that will of course record the recipient(s).
We further understand that there is a means to record the copyright on the video itself, which would be a good idea if that is easy to do, but if not this statement accompanying its delivery would be hard to deny.

5 Staff suitability declaration

Recently we have had a number of questions regarding the retention period for your Single Central Record, and we have had to state that IRMS 2019 does not list it, probably because its origins come more from Keeping Children Safe in Education rather than GDPR. The best opinion we could get was date of leaving plus six years and we think that might be appropriate in the vast majority of cases. However, we would always qualify it with respect for any opinion that you might have, perhaps about a specific person, and know that in some instances details have been kept for far longer.
It brought to mind the document reproduced at Appendix A which was produced by one of our customers some while back and we felt that it represented useful "belt and braces", so reproduce it again.

6 Afterthought, does size matter?

Or in this case, can you even conceive of the size of matter? Apple has announced that they will be "the first to use the breakthrough five nanometre technology". The dimensions of computer chips are now challenging the laws of physics with transistor sizes measured in atoms. To put it in some form of context, they are 1000 times smaller than a red blood cell and 24 times smaller than a particle of Covid 19,

which incidentally would very easily pass through most current face masks or coverings!
Which is all very interesting, except Apple does not make a single wafer, its chips are made by the Taiwan Semiconductor Manufacturing Company – and it depends on your political view as to whether or not you regard that as being China. (Which we fear requires knowledge of both history and geography!)
Considering that the first transistor, invented in 1947 was the size of the palm of your hand it is almost incomprehensible how far and fast technology has come.

satswana

Company registered number 09329065 www.satswana.com

Appendix A

Staff Suitability Declaration

This form is to be completed by all new staff when they commence employment (including regular volunteers and students) AND completed by all staff on an annual basis

Name of staff: ……..

Name of Manager: ……..

Please answer the questions and sign the declaration below to demonstrate that you are safe to work with children. If there are any aspects of the declaration that you are not able to meet, you should disclose this immediately to the manager/senior responsible for your recruitment.

Please circle yes or no against each bullet point:

Have you been cautioned, subject to a court order, bound over, received a reprimand or warning or found guilty of committing any offence since the date of your most recent enhanced DBS disclosure?	Yes / No
Have you been cautioned, subject to a court order, bound over, received a reprimand or warning or found guilty of committing any offence either before or during your employment at this school?	Yes / No
Are you "Disqualified or would you be disqualified for Caring for Children": (to include) • Have you committed any offences against a child? • Have you committed any offences against an adult (e.g rape, murder, indecent assault, actual bodily harm etc)? • Have you been barred from working with children (DBS)? • Are you living with someone who has been barred from working with children (DBS)? • Are you living in the same household as someone who has been disqualified from working with children under the Childcare Act 2006? • Have your own children been taken into care?	Yes / No Yes / No Yes / No Yes / No Yes /

• Have/are your own children the subject of a child protection order?	No Yes / No Yes / No
Has your name been placed on the DBS barring list?	Yes / No
Do you have any medical conditions that could affect your ability to care for children?	Yes / No
Are you taking any medication on a regular basis or any other substances which could affect your ability to do your role in the Academy?	Yes / No

If you have answered **YES** to any of the questions, please provide further information below:
I understand my responsibility to safeguard children and am aware that I must notify my manager of anything that may affect my suitability.

I will ensure I notify my employer of any convictions, cautions, court orders, reprimands or warnings I may receive.

I am aware that if I am taking medication on a regular basis I must notify my employer, and must keep the medication in a safe place, out of reach of children.

I will ensure I notify my manager if I experience any health concerns which could impact upon my ability to work with children.

I give permission for you to contact any previous schools, local authority staff, the police, the DBS or any medical professionals to share information about my suitability to care for children.

Signed: …… Date: ……..

Manager / Senior Signature: …… Date: ……..

Manager / Owner

Please record follow-on action taken, where relevant:

_____
_____
_____
_____

Sign:…… Date action taken: ……

'I understand the requirement to inform the school immediately of safeguarding issues relating to any personal circumstances that the school should be aware of as part of contextual safeguarding and safeguarding culture'.

J Satswana final update 2020

Contents

Appendix A

Advance briefing for Schools prior to a formal impact assessment.

1 Role and duties of a Data Protection Manager

Originally under the Data Protection Act 1998 the Data Protection Officer of an organisation was its Principal. However GDPR 2016 – which is almost 100% embraced within the Data Protection Act 2018 – introduced a "conflict of interest" test in that the appointee (who could be shared with other parties) must not have any duties which conflict with their monitoring obligations. This was held to include their legal advisers who may represent the organisation in legal proceedings.

However the GDPR also stated that the DPO is not personally responsible for any non – compliance, though of course they remain liable with general employment contracts, civil and criminal rules.

A review body known as the Article 29 Working Party recognised that it was necessary to have a person with full time operational and practical responsibility for data security and introduced the role of Data Protection Manager. Very substantially it is this appointment that undertakes the day to day implementation of the Regulation by the Controller – as the data holder is described.

The relationship between the Controller and the DPO is defined within Articles 70 and 71 of Part 3 of DPA 2018, to be found here https://www.legislation.gov.uk/ukpga/2018/12/part/3/enacted.

Rather than reproducing these clauses we invite you to look them up, not least because the original GDPR was most elegantly drafted and is unlikely to be improved upon in reproduction! However please note 70 (3) (c) which protects the DPO from dismissal, and (perhaps more importantly) 70 (5) which requires that they report "to the highest management level of the controller".

The Part 3 referred to is also an important study area for anybody involved in data security, but especially the Principal and Data Protection Manager, since it covers the scope, definitions and principles applied – as well as the rights of the subject, together with the role of the controller and processor, all within a few pages that are surprisingly easy to read. You may only ever have to do that once, but it is valuable to be able to find this information and confirm your understanding.

The most material point is the manner in which the original GDPR returned rights over the ownership and management of data to the individual, which in turn placed a responsibility with the controller to look after something that does not belong to them. Whilst that introduces a new liability to an organisation, many will applaud its intent from a personal perspective.

2 Future Technology

Talk to anybody in commerce, tell them how many software contracts you have for multiple disconnected applications, and they will think the industry has lost its senses. If you also tell them that you pay other companies (some with very doubtful finances) to access your data and provide it to another company, and they will be sure that you should be certified.

You would have to respond, look it works, and everybody is trained to use it that way – besides nobody has the time to change it, even if a modern option was available to us.

But the risk they would say, and all the extra work, the additional training needs, the cost of pulling information together from disparate sources, not to mention the expense of maintaining so many contractors. Indeed, are you sure they can survive as suppliers with such a narrow market focus?

However you look at products and features that were originally written decades ago they cannot make sense in 2021 – even though we will continue to use them. There are moves afoot for change, and it cannot come soon enough.

They say that there are two good times to plant a tree, the first being twenty years ago, failing that, start now. We should do that with our technology.

3 Relating data, what does that mean?

If you know what a relational database is, or a relational database management system, (RDBMS) then you do not need to read this. If you do not understand the term, please do read on, because Satswana suggests that any future software solution for education should be based on a relational structure, and we would like you to understand why and how it works.

Can we start with history, because all early programs were created with what was called a hierarchical database model? Now, in computing we always use plain English words to describe things, so the word means what its definition is, namely a hierarchy, with data stored as records which are connected to one another through fixed links that are created by the programmer. (The first "bug" in computing was actually a moth that got caught in the guts of an early machine and shorted the contacts – the expression stuck for any problem!)

These programs can run extremely fast and thus are essential for applications such as banking, but in 1970 a guy called EF Codd working for IBM decided that they could relate bits and pieces of data to each other in any number of ways. This had the advantage that you only needed to record a bit of information once (your name, or your address, or your date of birth – for example) and yet you could use it countless times by "relating" to it. You could use it to write a structured program that followed a required routine, but you could also ask it ad hoc questions that you had not thought of needing in creating the code, something that is impossible with a hierarchical database. So if you needed to know how many students are learning Latin and doing Biology, then you could "structure a query" and it would come back with an answer. This led to "structured query language", often shortened to SQL, and we are sure you have heard of that!

It is not a problem that would ever impact the sort of computing speeds demanded within education, but because the relations have to be set up every time any aspect of the code is run, and they cease to be there once the next stage has been calculated, a relational database is very slow in absolute computing terms. If we were a bank needing to access the statements of ten million people in a nanosecond, then we would be stuck – but for the admission records of a few hundred pupils, no problem.

4 Embedded accounting

An example of how a relational structure would be massively more competent in supporting the management of schools is that you would never again have to enter anything into your accounts, beyond the initial capture – let's say a till entry from your meals provider. That single entry would update every area where the number was required, from the parent account, through to the sales ledger, in turn updating the performance against budget, whilst creating an invoice and adding the details to the contractor's accounts as well.

Your reaction now may range from "gosh this is scary" to "why have we been maintaining multiple databases all this time when we don't need to?" If the former then we understand that change is normally not welcome, but if the latter you will be reflecting that this is what commerce has come to expect from several decades ago.

It is time to plant that tree.

5 Processor Agreements

This discussion has a direct bearing on the work that we have been doing for the last few months in re-evaluating the processor contracts – very substantially with software providers of a specific application that ought to in the future be consolidated into a single structure.

In conducting our analysis we realised that it was all very well ensuring that a provider was GDPR compliant, but given the extreme sensitivity of the data they were handling did they have the technical competence to actually control their infrastructure in the required manner? One key to that question was to consider their structure and accounts, and to our horror we found that all too often they were single director managed organisations with a negative net worth.

Quite simply if they were not making money as a lean operation now, how were they going to survive in a future where further investment was required? And worse, could they actually afford the essentials for security today?

For this reason, and also because we are writing to those who have "failed" in order to give them a chance to correct their position, we will not issue an update until the New Year – by which time we hope it will have meaningful data.

6 Deduplication problems with SIMS

It is perfectly sensible to provide routines within code that ensures that duplicate records are not obfuscating any search results, but they are only as good as the definition and process. If that goes wrong then you end up with an incorrect record when importing the applicant file, meaning in the case of one of our customers that emails were being sent to the wrong party.

As you can imagine that involved some serious head scratching, and no resolution of the issue until it landed on the desk of a 2nd Line Support Analyst that we had better not name, but we were really grateful that she came up with the answer.

She advised as follows. "When going through the process the system indicates that there is a match of contacts and the user is given the option of either creating a new contact or matching the two, which is what has happened in this instance. In order to avoid this situation in the future please go to Tools | Admissions | Defaults | Section 5. In here you can select what criteria should match when importing applicants. When I ticked postcode and house number and imported the applicant file the issue did not occur as the contact was imported as a new contact."

We are most grateful to her for actually solving the problem.

7 Understanding Cyber Risks

What are they really all about, and how likely are you to be hurt by an attack? We hope to explain the answer in a non-technical manner that you can understand easily, and which then helps you to avoid the risks.

There are probably three levels of likely exploit, we will cover all three but you are really only likely to experience the first two. We will also seek to make it more interesting with some true stories!

Email

Electronic mail has been a blessing for society, but also for crooks, in that when it was designed by the early originators of the Internet, in the 1970's, they really only thought about the value of communications and connectivity, at the time they did not seriously think that security was a problem. As a consequence there was originally no protection to ensure that you were who you said you were, or where you were, or what you said, it was all in open text.

There have been moves to improve this situation, not least by adding encryption as an option to messages, but since you will hardly ever use that, the risks remain.

Fundamentally a crook gains access to email through one of two means, the first being an old fashioned confidence trick – called "phishing" nowadays – but it is an apparently genuine email that persuades you to click on a link, and that is actually a Trojan horse attacking your system. Ideally you should never click on an attachment in email, if you need a file think of another way of sending it, because these criminals are seriously brilliant in thinking up ways to make you lower your guard! Having said that, we will still use standard email, but you must be mega suspicious, even if it appears to come from a close friend or contact.

The second method is to divert your email traffic through their server which allows them to read all your mail. This is known as a "man in the middle" attack and can be very dangerous because they can appear totally genuine if they comment on something you have just said. They capitalise on this in two most frequent ways, the first is called "Business Email Compromise" (BEC) and is the most common exploit on the Internet. It normally takes the form of an instruction to pay an invoice "urgently" to a given bank account. The second option that is similar to this is the diversion tactic, telling you to pay an invoice to a different account – theirs of course. You should never accept an instruction to change a payment method without multiple authentication of the identity of the requestor, and even then leave it a week!

Perhaps the simplest "con" is to get hold of your address and send you a threatening message – usually suggesting they have turned on your camera and filmed you doing something that you know you haven't done, but asking for money (Bitcoin almost invariably) to delete it. These can be safely ignored and deleted.

If they do manage to create a presence in your email they may use your server to broadcast other compromising emails to all the addresses in your contact list as if they had come from you. That is not only really embarrassing, but means they in turn infect all your friends and expand their network still further.

Please never use a public Wi-Fi connection, as in a coffee shop, because the "free" connection that you are so pleased to find may be the person at the next door table harvesting connections rather than the shop provider. There is a tale that an enterprising crook used a drone to create a connection on the roof of a bank. Where was the boardroom? On the top floor of course, and the Directors blithely logged on to the strongest signal, there were many embarrassing outcomes from that.

The network attack

Many of the confidence trick style attacks require little if any technical skill (they can download instructions from the Dark Web) but they can also be entry points to access your network and create a hidden presence. There are two major risks from that, the first being that they will copy any valuable information you might have in

your files, perhaps to be used for blackmail. But the most damaging is to encrypt your information so that you cannot access it, and then demand a ransom to release it.

Ransomware, as it is known, is very damaging, not least because again they are very clever and do not tell you straight away. They will wait several days until they are sure that all your backups are likely to be infected too. Three points, first, never pay the ransom – not just because you are complicit with criminals if you do – but because they are criminals they will be most likely to take your money as well as your data and disappear. Indeed they take a risk if they did come back into your network with a release key, they can be tracked.

Second, we recommend always having a historical backup that you keep off network. Even if you only do it every three months, you have something to go back to, your original history – even if all your current data has to be re-created. Best though is the third option and that is to choose a backup provider who checks for any changes in file structure that might indicate an attack, and then stops to check before going ahead. (Do please call us if you get a ransom demand, there are other things that we can do.)

The macro attack

Individuals, schools, local authorities and SME's are most unlikely to ever experience a macro attack because you are simply not worth it. For the same effort the attacker can make possibly billions, not a few hundred pounds. These exploits come from either extraordinarily well resourced criminal structures, or may be actually State sponsored entities. Are these all either Asian or Russian? No, one of the most famous (Stuxnet) was actually alleged to have been built by US and Israeli intelligence to penetrate Iran's nuclear programme.

Protecting data from a macro attack is a science on a totally different level, but as far as possible your IT provider will employ many of the tools to also protect you. You will have heard of antivirus software, but the next generation firewall that contains threat intelligence profiles and limits the range of "the Internet" that is allowed to talk to your server will be constantly monitoring for new risks and trying to keep you safe.

Encryption

If there is one single protective element that you can embrace it is to make your data unreadable without authorised access with a technique called encryption – actually the very attack mechanism used by Ransomware, except that in this case you always have the key.

If I tell you that encryption cannot be broken then we risk the wrath of a million or more “experts” who will claim that it can, but let us tell you why they have all been victim to one of the most brilliant intelligence secrets of all time.

First, let us explain how encryption works. Simplistically because all data is binary, then it is all numbers. If you multiply each number by another very big number then the data becomes incomprehensible until you divide it again, when it becomes unencrypted and readable again – only when you use your user name and password to authenticate the access.

Second, in theory, if you had a fast enough computer that can compare every combination of numbers with your data until it was interpreted, then you could find the key. But hang on, this is a huge processing task, and even the projected (but not currently available) speed of Quantum computers would take ages to derive just one key. For your database it is simply not going to happen!

So where did the myth come from? Once again, from western intelligence agencies who operated the most astonishing confidence trick you will ever hear of, this time developed by America and Germany in the form of a company that sold cipher machines to governments under the guise of a Swiss company called Crypto AG. It is a tale worthy of a James Bond film and from a UK point of view meant that the UK had full access to Argentinian traffic in the Falklands War.

How to explain the leaks? You will see that it had to be put about that with a really powerful computer encryption could be broken, and we all believed it. Today it would have to be a huge prize to make it worth it, and there are indications that the Swift payment network might have been vulnerable at certain times, but for all normal purposes, encryption cannot be broken!

8 Brexit

Thanks to the excellent sharing of information by Andrew Hall’s Safeguarding service we thought we had some Government information that might help at the end of the transition period, notably regarding the recruitment of teachers from overseas. Sadly he advises that the references have been removed, so apologies, but we are all in the dark regarding what the kindergarten politicians will deliver at the end of this month.

Appendix A

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!

Contents of this document are the Copyright of Satswana Ltd 2021 ©

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.

Contents of this document are the Copyright of Satswana Ltd 2021 ©

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.

Contents of this document are the Copyright of Satswana Ltd 2021 ©