satswana

Company registered number 09329065 www.satswana.com

Satswana Limited
DPA GUIDANCE MANUAL

Version 4.0 17th February 2021
Replacing Version 3.0 10th January 2020
Replacing Version 2.1 27th February 2019
Replacing Version 2.0 dated 3rd September 2018

Specific Notes for Version 4.0

With the passage of time almost everything we originally published has advanced or been changed and so this manual has to change with it. A great deal will either have been removed or truncated and elements you may have referred to previously may not be there now. If in any doubt, please contact us since that will enable us to subsequently identify anything missing, and add anything that is required.

We would restate that most Satswana customers will be in a confidently compliant position, with four major areas that we must concentrate on – but on the basis that this is a "journey", not a destination. We are keen to stress that (even if you still use paper records) nothing is actually "broken". The first is to ensure that we have embraced encryption wherever possible, this being the single most effective defence we can implement for digital data. Secondly we must start to come to terms with the deletion of data that we do not need to keep, and that will involve support from software suppliers – we will not develop solutions overnight. Thirdly we must wean ourselves off email in favour of the use of collaboration systems where the data never leaves our control. Finally we must demand that systems providers provide comprehensive and less expensive support solutions. Satswana are continuously promoting this objective and you will hear much more about that from us.

This document is the collation of the various elements of the GDPR journey, compiled into one searchable reference manual. This version reflects the post 25 May 2018 position, but as revised in January 2021, and provides guidance on how we at Satswana Limited will work with and support our customers.

Our assumption is that you have already sought to comply with DPA and our aim is to guide you to best practice through our ongoing support and expertise. If you are not already compliant, we will act quickly to assist you commence the journey.

Don't be daunted by the size of this manual it is structured, indexed, and it is searchable!

To search, select CTRL+F and enter the word or phrase you are looking for

satswana

Company registered number 09329065 www.satswana.com

Index

1 MEETING YOUR GDPR REQUIREMENTS

1.0 Introduction

Satswana are privileged to have been appointed to provide Data Protection Officer Services to a wide range of schools and parish councils, for the purposes of achieving compliance with the General Data Protection Regulation and Data Protection Act 2018, find the complete Regulation here https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

We look forward to the opportunity of meeting with you for a proper consultation, since we respect the individual personality of each School, and indeed have a responsibility to ensure that the personalities who create that identity "buy in" to the benefits we perceive.

Meanwhile, there is some information that we would like you to have straight away in order to help you check your compliance, and to ensure that you do not have any anxiety regarding the work that is required to achieve that compliance.

We ask you to accept this guidance briefing, together with "generic" solutions that have been garnered from experiences with other customers. We know there will be exceptions and differences, but you will have demonstrated massively more compliance than many other organisations.

1.1 What you should have in place as a minimum - just four things

1 We recommend that you include a privacy policy on your website, as found at Appendix K, together with a statement also included in Appendix K.

2 Please make a list of your Processors and analyse their state of compliance by reference to our Processor list. (Since this is a document that is frequently updated, please request that separately)

3 If not already in force, you should adopt and deploy encryption, both for data at rest, on any transportable medium (especially USB Sticks) and for sensitive emails.

4 Please note that there are certain places that you must publish who your DPO is, on your website for example. For those purposes the DPO should be Satswana Ltd, with email of info@satswana.com ; telephone number 01252 516898, if you need an office address as well it is Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

1.2 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.

1.2.1 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!

1.2.2 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!)

1.2.3 The SLT briefing

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

a) No fear

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

b) Return on investment

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

c) Breaches

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

d) Subject Access Requests

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

e) Processor agreements

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

f) Retention policy

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

g) Policies

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

h) Encryption

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

i) Myths

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

j) You are the Boss

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

1.2.4 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.

2.0 About the Impact Assessment

This is a generic Impact Assessment, its purpose is to transfer the knowledge gained from working with hundreds of people in order to arrive at as compliant a state as possible in the shortest possible time.

It does not replace the essential personal communication that leads to a meeting of minds and an understanding of any special conditions, but that can follow when we meet.

Within the consultation we will hope to meet the people who do the jobs we describe below, and seek to impart the value of GDPR as being a Regulation that returns the ownership of personal data to the individual. We have not yet met anybody who does not approve of that! What we then discuss is the impact of that ownership change to the organisation.

We go to great lengths to reassure everybody, to stress again that this is good law, that Schools are generally compliant, and that you are not the target. Providing you have set out on the path to meeting the requirements, you should not be criticised, even if you are seriously breached.

Our final introductory point is that we expect you to use GDPR as an opportunity to embrace change that you probably have in your mind anyway, but are lacking the impetus to enforce it. Most people we have worked with feel that they have actually had a good return on their investment, and that GDPR compliance is just a side product.

At Appendix I, we provide a list of processors that will not be inclusive for you but may contain much of what you would expect to see. Your SL/DSL and SENCO particularly will have many unique relationships that must be captured as a processor - please create your own list. We also supply a processor guide and a range of policies that may assist you in having something to adapt, rather than write from scratch.

Satswana will be providing customers with a list of approved processors.

2.1 The consultation phase

If you are not already a customer, as soon as possible we hope to arrange a date with you to discuss these matters personally, but since we have done that with many others we believe that we can suggest some of the lessons that may be learned.

a) IT Manager

We will ask about your current structure and your views on a future direction of travel.

You will either have an on premise server environment, or be using a cloud based environment, or a hybrid of the two, all three work, and can be continued under DPA. Our major recommendation will be to adopt encryption of data at rest, which can normally be achieved at minimum cost.

However a clear direction of travel has emerged, with most organisations adopting Microsoft 365 (or the Google equivalent) for its collaboration tools and encrypted email option. We expect the increasing emergence of cloud based versions of Schools Information Management Systems. The reason is the greater control, resilience and broad range of security options with a stronger level of support than can ever be afforded in house.

That is absolutely not mandatory, but we would be surprised to find an in house solution in ten years' time.

b) Admissions and data manager

The important point here is to ensure that any Admissions Form, Data capture sheet, or supplementary information form, carries a DPA compliant statement so that you are gathering consent from new information immediately. You should have a current Data Protection Act statement; if not, we suggest you review it.

As a guide only, we produced the following form of words – you can adapt as you see fit. *"The 'Generic' Academy is compliant with the Data Protection Act 2018 which means we seek your specific consent to use the data we are collecting within this Admissions Form (data collection sheet, or supplementary data sheet?) for the purposes as detailed within the Privacy Policy on the School website. We request that you sign this form to confirm that you are giving us your specific consent for the use of this data for the specific purposes outlined only."*

Please note that we are suggesting you refer to a privacy policy on your website, which means that the policy must cover all your uses of data, and hopefully our draft will help you there. As a caution, other schools have tried sending out a form with multiple questions and tick boxes with the best of intentions, but very variable results. You start with a distribution issue, do you hand deliver via a pupil, email, or write a letter? You almost certainly know the snags with all three options, but the reality is that you will not get a one hundred percent return.

Then there is the confusion in response, if a box is not ticked have they actually opted out, or misunderstood? Can you have one pupil in a class doing maths homework online, and another not? You know that some of your parents may not be comfortable with filling up a form at all. Thus we suggest the broadest possible approach, reflecting that there will always be the odd person without access to the website – but we believe that to be the easiest snag to overcome.

A major subject is likely to be your future retention policy. Whatever you have done in the past there will be a drive now to reduce the paper files you keep - that will be less welcome for some, than for others, but is an inevitable aspect of progress. This will need to be considered, and put into effect as soon as possible. We can provide a much more in depth paper on retention, which remains the hardest subject to actually implement

c) SENCO or Inclusions Officers, SL & DSLs

This group will have extraordinarily sensitive data that they necessarily share with a very wide range of third parties that are normally a surprise to the school itself! The assessment normally benefits more than most from the reassurance that the consultation provides, especially when discussing the future problems of references in a safeguarding environment. Please note that we have specific documentation to support you in the event of an access request where very often your position is protected.

d) Finance Officer

Most of the work of the Finance Officer is covered under statutory provisions, but we will need to cover the management of school meals, payment for school trips, and the organisation of your payroll provisions for staff.

e) Exams Officer

You will be sharing data – perfectly properly – with a range of exam boards who are nevertheless processors within GDPR.

2.2 Further information provided

i. First, please find attached at Appendix A, a generic “Discovery” document derived from the analysis of data sets, principally in a Primary School. A Secondary will be more complex but follows the same basics. In time we will ask you to consider the personal detail that applies, but for now this should cover 80% of the requirement to analyse your data.

ii. Second, below you will find an outline format "Impact Assessment" which, with the expanded sections at Appendices B & C, does cover the expected environment in a Secondary School, so many of the comments are likely to apply in due time. To some degree you can start to consider the ideas immediately if you have time. This is a redacted version of a real assessment, so please note that we are happy to consult with other parties than indicated above. Please note the guidance notes provided as to how to read that document.

iii. Thirdly we will provide you with draft policies as contained within Appendices K to Q

iv. Please note that there are draft processor agreements at Appendices G & H.

2.3 OUTLINE FORMAT OF IMPACT ASSESSMENT

Impact Assessments are important in that they reflect the work undertaken and the compliance to date along with the action plan moving forward.

The assessment is presented in four parts:

- **Part One** is an outline and executive summary as in "Quick Read, the main points". An example is shown below.
- **Part Two** are notes from the individual discussions within the Academy. The outline of a suggested timetable is shown below with the more detailed notes included at **Appendix B**
- **Part Three** contains generic headings that are intended to assist with "best practice" issues that are not necessarily absolutely tailored to your needs, please review and apply as you see fit. See **Appendix C**
- **Part Four** contains appendices such as the processor guidance and policies

Example Impact Assessment for xxxx School, Address, post code, date commenced

Attending - Xxxxxx and xxxxxx , for the School, and xxxxxxxxxx for Satswana

PART ONE

1.1 Outline

Describe the School in outline
School number

ICO Registration number or reason for exemption
OFSTED rating

1.2 Quick Read, the main points

An executive summary that may be along the following lines:

Xxxxxx School is very well managed by impressively capable people who all embraced the opportunity for change represented by GDPR. The School would be considered fully compliant with any reasonable analysis of private information. The only requirement for change is dictated by the specific legislative impositions of the revised Regulation.

The very specific areas arising from this report that we would highlight might start with the requirement for a retention policy which favoured deleting and purging information rather than the very reasonable practice of continuously storing ever more history.

The second major point would be to deploy encryption wherever an exchange of sensitive information was required; an area that is likely to become ever more developed over time. It is recognised that not all parties can cope with this at present and they would have to be brought on-board as training and adoption becomes a matter of course.

Thirdly, a means of limiting the degree to which information is passed out to third parties is through the use of a document collaboration structure that maintains control of content within the organisation. Your adoption of 365 will facilitate this.

Finally, the whole question of the external sharing of data in the form of either references or the passing on of knowledge to other parties has to be considered against the new consent requirements of DPA.

We are all embarking on a journey where to date there is neither case law nor precedent, so this is not a destination but the first step in a long march.

PART TWO

2.1 Consultation

The timetable below is a suggested format which can be changed to suit the requirements of the Organisation. A sanitised example of an impact assessment timetable and initial findings reported to school can be seen at

Appendix B

09.00 Business Management

09.30 ICT Team

10.30 Marketing, Website, Appeals

11.00 Exams, Data Management/Reports

11.30 Safeguarding

12.00 Health & Safety Officer, Trips Co-ordinator

12.30 Lunch, Meeting with Principal

13.15 SEN, Admin, Communications/External/Parents

13.45 HR, Payroll & Pensions,

14.15 Finance, Contracts, Primaries, HR & Payroll, Trips

14.45 Heads PA/Clerk to Governors'/Parental Communication/Appeals Admin

15.15 Community Sports Centre

16.15 Re-Group

PART THREE

Part Three provides a range of generic guidance and best practice which is usually tailored for each customer. A sanitised example can be found at ***Appendix C***

PART FOUR

Part Four – various appendices, targeted to suit each organisation.

Two final points:

2.4 The role of the DPO at headline level

The role of the DPO is variously defined and is subject to contract. The full legal requirement can be found here
https://www.legislation.gov.uk/ukpga/2018/12/section/70/enacted

For Satswana, we state that we are your independent advisor in order to provide the air gap against any conflicted interest. We consider it is best set out as:

- Inform, advise, assist and update

- Monitor compliance
- Cooperate with the supervisory authority (Information Commissioner's Office - ICO)
- Act as contact point for / interface with the ICO
- Due regard to risk (understanding, priority of tasks)
- Support with data breaches, SARs & policy templates
- Assist with arising solutions, i.e. encryption & cyber security

A practical example of maintaining the air gap is that when SARs or data breaches occur, we do not wish to see any data unless we decide to request it, lest we inadvertently become data processors. We believe that we can assist you ably without sight of data in most if not all cases.

2.5 Lastly, we recommend showing the video Data to Go https://www.youtube.com/watch?v=_YRs28yBYuI. It is just short of 2 minutes in length. It has proven to be personal to all who have seen it to date and, we believe, that it is persuasive in gaining the buy-in of not just staff but all stakeholders into moving forward to achieve compliance. There is an excellent ICO video for schools here ICO information rights video for schools - YouTube

APPENDIX A
SATSWANA INFORMATION ASSET AUDIT
(Draft as a guide only)

Questions about your data asset	Yours answers to the questions about the data asset
What is the name of the information asset? (Please note that this is a general guide, filled in with many of the "normal" headings to assist you)	An information asset is a body of knowledge that is organised and managed as a single entity, such as a payroll. You may have others than those below, such as sports hall bookings.
Why are you processing the personal data in the asset?	Parental data – Contact details Pupil data – for returns for funding plus Contact database and permissions Staff data – Payroll, contracts, contacts, right to work in UK, references. SEN information + trip data
Who is the asset owner?	(Define the ownership, ie the Trustees of xyz school)
Are you the controller/processor or joint controller/processor?	Controller would be the normal answer
Whose personal data are you processing?	Parents, pupils, staff, who else?
Are you processing sensitive personal data?	Yes, within SEN and trip data Free school meals SL & DSLs
What are your grounds for processing?	SEN pupils requirements, medical and dietary information required for school trips
What permissions do you have for the processing of the data? Are there any Privacy Notices associated with the collection of the data?	Privacy notices for parents and staff as DPA. In future specific consent will be required for a specific purpose, as obtained on Admission forms or data collection sheets
Have you carried out a Privacy Impact Assessment (PIA) for this data?	Satswana have been instructed to carry this out
Where is the personal data stored?	Computers, (on premise or in the cloud?)

Questions about your data asset	Yours answers to the questions about the data asset
	Paper files Phone records CCTV recordings Video, photographs, audio etc
Who has access to the information asset?	Staff, current parents and pupils whilst at the school. Processors such as auditors, legal advisors, IT support etc. may have access (must be subject to a processor agreement.)
How is the information asset kept safe? (IT measures, but also including other measures)	Locked cabinets, locked offices, password protected IT, encrypted, backup (We will suggest encryption, access control systems and digitisation of paper, all recommendations subject to your approval)
How long do you keep the personal data in the asset? It? Is it up to date?	Staff six years (+2 years) and other assets as per legal requirements. (We will suggest implementing a retention policy that destroys paper records and also purges electronic records that are out of date)
What will happen if something goes wrong and there is a data breach? Is there a process?	Most schools will not have a current process, Satswana will seek to discuss creating one with you
Do you need the data? Why? What is your retention schedule for the data?	Data required for DofE funding. Contact details, contracts including pay. Other reasons?
Do you share the data with anyone?	DofE, local authority, SEN professionals, payroll contractor, Schools information management systems, exam authorities, travel agents, lawyer, accountant, SL/DSL/MARAC etc
Do your contracts reflect any arrangements you have made for sharing and storing the data?	Probably not at the moment, but in future wherever you share information you will require a suitable processor contract
Is any of the data collected data from third parties? Do you have the necessary permissions from them to process the data?	Admissions documents? SEN shared data. Legislative requirements?

APPENDIX B

REDACTED FURTHER EXAMPLE OF AN IMPACT ASSESSMENT TIMETABLE AND INITIAL FINDINGS REPORTED TO SCHOOL

09.00 Business Management

We discussed the program for the day and were provided with the schedule which was to start with the IT Team. Xxx and xxx would both be supervising the consultation throughout the day and we would sign off at the end. The purpose of this consultation phase is to enable Satswana to perform a "know your customer" learning session, and to directly brief the members of staff regarding DPA. Our aim is always to listen to compliant ideas suggested by the various specialists themselves, which always proves that they have "got it". We are happy to record that we feel the day was very successful in that regard.

09.30 ICT Team

The excellently managed on premise IT infrastructure, being a secure environment that was as self-contained as possible. For the purposes of this Assessment we will concentrate on your proposed direction of travel rather than commenting at length on the existing system. That is not to suggest that there is anything wrong with the existing system but all present expressed the wish to go forward to the next stage.

Specifically, this involved the use of Microsoft 365 and the deployment of Onedrive to provide a shared/collaboration area for future interchange of information where you would deploy locked down PCs and retain all documents and files on the server.

We discussed encryption extensively and it was agreed that this should be deployed wherever possible and practical.

As with all headings we discussed retention which must be the subject of your policy with the requirement to actively purge data. It was noted that currently SIMS are working on a capability to facilitate this. (Note that we have a specialist paper on the subject)

You were fully aware of the possibilities within a Cloud future, especially as regards backup.

We discussed the potential challenges of IP Phone systems that were designed many years ago.

It was agreed that Pen Drives should be discouraged wherever possible, that cameras should be used for taking photographs and then the SD card deleted. You explained the risks inherent in the use of mobile phones as a camera by parents.

You considered that you could arrange for a single sign-on environment to satisfy the requirement for complex and changing passwords.

10.30 Marketing, Website, Appeals

Xxxxx manages the work experience for Year 10 with up to 200 employers. Much of the information is entered by the students themselves into the employers system so that is not retained by the school system. Frequent reviews are conducted of your data sharing agreements. Xxxxx also looks after the Health & Safety requirements of the organisation. Much of the information provided to the Local Authority falls under the statutory requirement to comply with the September Guarantee. We discussed the issue of references generally.

11.00 Exams, Data Management/Reports

As an Assistant Head teacher xxxxxx has a pastoral and safeguarding responsibility. You noted that paper reports were held digitally and the paper shredded. You advised that you had undergone a xxxxxxxx Improvement Audit. Xxxxxx oversees the Single Central Record. You use an electronic system for internal referrals which is encrypted. You use a program called Capture for online record keeping and input to both SISRA and Fisher Family Trust.

11.30 Safeguarding

Xxxx is also an Assistant Head teacher responsible for pastoral care and the well-being of children. We had a considerable discussion regarding referrals and references covering the impact of DPA on established practices.

12.00 Health & Safety Officer, Trips Co-ordinator

Xxxxxxx gathers information for risk assessments for trip requirements including medical and dietary needs, plus their mobile telephone numbers for parents. They are retained on paper for the period of the trip and destroyed afterwards. Personal information is retained in a protected shared folder.

12.30 Lunch, Meeting with Principal

The Satswana Team were very pleased to have the opportunity to meet the Principal and spent five minutes discussing the major points of DPA.

13.15 SEN, Admin, Communications/External/Parents

We were advised that xxxxxxx was the SENCO and that xxxxx was responsible for additional needs while xxx was a support officer responsible for health care plans and additional support plans. You conduct an annual review of the documentation and liaise with the Local Authority using CAMS. We discussed adding parents' consent to routine forms and noted that electronic mail sent to the Local Authority was not encrypted.

13.45 HR, Payroll & Pensions,

The major purpose of this discussion was to understand the role the School performed in providing both internal payroll and external processing for two primary schools. We discussed the way data was incepted and the personal details form plus the application form that were entered into SIMS and Sage. Other matters arising were the use of SAMS for absence management including the recording of sick notes, with the Single Central Record maintained on spreadsheets. Once again the subject of references came up in the context of being required to give mortgage information to a bank. The major recommendation that was considered was to replace paper payslips with electronic payslips.

14.15 Finance, Contracts, Primaries, HR & Payroll, Trips

Accounts are managed using the xxxxxx financial package and it involves all aspects of billing for trips, catering payments, school accounts, input and output from SIMS and pupil premium.

Xxxxxx is a catering package provided by xxxxxxxxx which can operate on a biometric input which is part of the Induction Pack for new students.

Required reports for the Local Authority are sent through secured xxxxxx . xxxxx records who has paid for their school meals.

14.45 Heads PA/Clerk to Governors'/Parental Communication/Appeals Admin

This consultation session served to reinforce four consistent themes that had arisen in earlier discussions, the first being the general requirement for the School to establish a retention policy. Secondly, whilst your current Induction processes and paperwork were excellent it was recognised that they should be changed to comply with the new consent requirements of GDPR. The third major point was to make greater use of document collaboration services with the very considerable range of correspondence required between parents and Governors. Finally, GDPR dictates

reconsideration of the whole question of references in light of the right to be forgotten and the necessity to obtain the specific consent of an individual.

It is perhaps worth noting the very considerable range of subjects that are captured with information of a personally identifiable nature. They are responsible for all calls, recording of absences, pupil communications, letters to parents, typing requests, Census completion, liaison with reception, ingoing and outgoing post, attendance registration, the updating of personal information. We discussed the inevitability of traditional paper input for these purposes and the need in future to consider how they can be digitised. In particular you were to establish whether the data collection sheets were subsequently destroyed.

15.15 Community Sports Centre

Xxxxxxxxx runs the Sports Complex Limited Company that manages the Sports Complex. Substantively the data consists of booking forms that are entered from her PC onto the School server. All documents are maintained in a cabinet in a locked room. It was agreed that the cabinet should be locked as well.

During this discussion the subject of CCTV came up which is covered in Part III but briefly signage should ensure that you are not exposed to onerous demands from subject access requests.

16.15 Re-Group

We reviewed the main points that had been discussed throughout the day with the additional identification of information required to be held for the Teachers' Pension arrangements. We also discussed peripatetic teachers especially in the context of music exams that we gather are conducted at the xxxxx Music Centre.

APPENDIX C

IMPACT ASSESSMENT PART 3 (REDACTED)

3.1 IMPACT ASSESSMENT PART 3 (REDACTED) – Generic notes

3.2 Notification of DPO

Where appropriate, within your policies, website, or any relevant literature you must transparently advise that Satswana performs your function as Data Protection Officer and provide a means for a 'natural person 'to contact us if they have any issues with your security procedures or performance.

3.3 Commentary on Processor contracts

Satswana will be pleased to check the compliance of any Processor you use and provide you with a consolidated list of approvals

3.4 GDPR versus DPB

Throughout this assessment we may refer to GDPR, being the General Data Protection Regulation originally adopted into European Law in April 2016 and intended for universal adoption in a standard legally enforceable form across all Member States

Brexit required English Law to replicate the requirement, or adopt changes and that is the Data Protection Act 2018 , replacing the current Data Protection Act, but also being substantively aligned to European Law to comply with the Brussels requirement for a common data landscape. Two distinct changes were to reduce the student consent age from 16 to 13, and to protect the provision of references from disclosure in Access Requests.

After we have left, any use of data that involves a European resident means that the Institution is subject to European Law in the handling of their personal data, so if you have one student from France, then you must comply. Finally, please consider the issue on social grounds. GDPR is good law, and as such is likely to be adopted as the privacy standard internationally – though the United States have a problem reconciling it with their First Amendment – all other Countries are likely to conform, not least because of the second requirement above.

Thus we promote a broad international view of regulation in this instance.

3.5 Data Protection Manager

You will appreciate that the Regulation requires you to appoint a Data Protection Officer, and that appointment is constrained by conflict of interest provisions. Satswana prefers to promote its role as a fractional service provider based on the belief that it is not a full time job, that it requires a broad range of expertise and that few within the organisations we work for would have the time or inclination to take on the task.

However the Article 29 Data Protection Working Party issued guidelines that (perhaps surprisingly) confirm that DPO's are not personally responsible in cases of non-compliance with GDPR, and confirming that "it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24 (1))."

The DPO does have other defined duties and responsibilities, but under Article 30 (1) and (2) it is the controller or processor (not the DPO) who is required to "maintain a record of processing operations under its responsibility" or "maintain a record of all categories of processing activities carried out on behalf of a controller".

The recommendation therefore is that an organisation should appoint a Data Protection Manager – who might well be the same person who might have been originally registered with the Information Commissioners Office as the DPO under the older Data Protection Act.

3.6 Encryption

We will consistently throughout our advice recommend that you deploy encryption wherever possible and practical. Whilst it can be an expensive solution, it can also very often be a no cost option, and on something so easy to lose as a USB stick, it is an absolute essential. (Please note, it is not just the physical loss of the stick, but also losing track of what may be on a device, they can only be viewed if used and will not have a table of contents!)

We are aware that there is a stratum that argues that encryption is "not the answer" because it can be broken, that agencies can read the data anyway, and that if you know a user password you can get into it regardless.

First point, modern encryption cannot be broken in all reasonable circumstances. It has to be true that any mathematical construct can be analysed, but the computing power necessary to do so is mind boggling, and is not going to be applied to Johnny's homework. We accept that in the US, agencies do require a "back door" in some circumstances, which is one reason why the US is not an acceptable server location

under European Law. The major point being that agencies are not where our risk comes from, it is from the criminal community that generally speaking they are seeking to protect us from. Finally yes, if you lock your house and leave the key in the door then your lock is useless. That is simple stupidity and has to be covered under code of conduct or acceptable use provisions; it is not a reason to fail to fit (metaphorical) locks.

The fact is that encryption is likely to give you extensive protection, probably much beyond an 80:20 ratio, and that is recognised by the ICO to the point that if you are breached but encrypted it is not a reportable event.

3.7 Software options and upgrades

One of the conditions for review of GDPR/DPA is in the event of any change to your software or working practices, and it may be that you are forced to change if a processor cannot meet your requirements, or their servers are not located within an area approved by the European Union.

It is not easy for an institution to adopt change. Most will stick to a dominant provider that is likely to fail to deliver leading edge solutions, despite the availability of leaner, cheaper and more effective options. "Nobody ever got fired for buying IBM!". But GDPR may just be a reason to focus on whether you have the best product.

In which case please be aware that you should judge them on the manner in which they approach "privacy by design and default", because embedding security in their process must lead to making your compliance easier.

3.8 Access control

Most organisations will deploy a physical, sometimes paper, often electronic means of controlling access – some of which can be extended to further restrict specific responsible persons to areas or files, or both.

Despite the cost, this is a subject that should be continuously reviewed. Do you have the very best option available for your environment and does it do everything you require of it? Is the supplier also a processor with access to data?

Very specifically you should challenge the supplier to explain to you how their system is designed to counter unauthorised access, and to identify any means whereby it might be hacked or misused. You must recognise that for some people , any security is there to be bypassed or overcome, and only by starting with the

assumption that they might succeed will you apply sufficient rigour to your system to be sure they cannot.

3.9 Voice Systems

As with access control systems above, many schools will have chosen telephone systems that reduce receptionist workload and can provide answering services. Many of these work on an IP basis, and some embrace VOIP.

Two points, the first being that you must challenge your provider in the same way as described above, because a phone system has a long life cycle and may have been designed years before modern vulnerabilities were recognised. Does the generation you have expose you to risks, and in that case can they be patched? If they cannot then you must record that and document your path to overcome the risk. That may involve a necessary delay for budget to become available, in which case the ICO can take that management observation into account if it should ever become necessary.

The second point is that any answering machine message becomes "data" that may on occasions have very sensitive connotations. What is your deletion policy, and can anybody unauthorised overhear the message on playback? Do you record conversations as part of a safeguarding policy for staff, and in which case how do you retain abusive examples as evidence (for example), when are they deleted and who might you share them with (the Police?) Who else might have access and are they appropriate?

Do not leave messages on an answering machine that might be heard by an unauthorized person.

This may well prove to be one of your potentially most vulnerable areas that will have the least support and could be the most expensive to fix. Solutions will have to emerge, but any disruption and change will not be welcome.

3.10 Clear desk policy

It must be considered a contribution to security if papers are not left out and any electronic access devices are logged out of (and screens turned off) when a user leaves their desk. It is recognised that there is a practical balance to be struck between convenience and an ideal, but it is a reality that an unattended desk with a logged on PC – or open file – can be the most exposed circumstance for any data. Very short absences might be acceptable if the room can be locked securely and nobody else has access, but any person working in an open area has a responsibility to ensure the protection of information under their control.

3.11 Photographs policy

The use of images generally becomes a more complex area. It is recognised that there are a number of occasions where identity is an issue, on an admissions form for instance, and thus there is an absolute requirement to receive and store a picture of the person. Similarly staff must be able to recognise pupils that may be at risk or subject to special needs, so their images may be properly displayed so that they may be identified. The corollary is that identification may also result in exposing sensitive data, thus the placement of images has to be carefully considered. If in a reception area (a logical place) can you be sure that only staff can see the images, and that they are inaccessible to casual visitors?

A similar challenge exists in the use of a single picture, or a recording, of individual or group action. In one sense it is a modern joy to record events, and the use within a marketing environment is also part of modern society. But we also have to be aware that there are circumstances where those very benefits can be misused and incorrectly applied.

It is inevitable therefore that a school must adopt a policy to obtain specific consent to the use of images for a specific purpose, and maintain evidence that they have done so. It is to be hoped that in doing so account can be taken of Recital 4 "The processing of personal data should be designed to serve mankind". Images are a delightful record of personal history and joyous events, thus worth preserving and not surrendering totally to the threat of misuse.

Satswana can provide you with an Images policy.

3.12 Use of a portal for data

Society has enjoyed the benefit of ubiquitous communication via email, but in the current security landscape the distribution of content that this methodology represents has to be reconsidered because the sender loses control of the use and destination of the shared information.

An alert regarding the availability of information can still be sent in an email, but retain the actual message content in a single accessible source, that may be either open, in the case of website pages, or protected behind a requirement to login to a document collaboration area, such as Sharepoint.

3.13 External connections

The desirability, indeed often necessity, to "work from home" is recognised in the schools environment. For this purpose a dedicated, locked down access device should have secure access to working files that are maintained within the schools

server infrastructure, not on a local drive. All accesses should be logged and reviewed.

Ideally no data should leave the schools control, but if there is no other option consider the use of encrypted USB sticks. In no circumstance should you allow the use of unencrypted memory devices, or mixed personal and business use.

3.14 Tablets

In the absence of paper an alternative means must be provided to view and review relevant information. It is suggested that the adoption of tablets or similar devices for the use of staff would be a suitable alternative. They should be dedicated to school use, locked down and use encryption – being accessible by a single individual via a password access. A central register of passwords must be securely held by administration to ensure relevant management access to the tablet, in the event that a user leaves for instance and the device must be redeployed.

3.15 References policy

It has been the historical practice of schools to generously respond to information requested by other schools, employers, local authorities and other similar official organisations.

It was an advance within the DPA 2018 that references are protected from disclosure within a Subject Access Request.

3.16 Shredding

We believe that all paper should be shredded at the first opportunity following its use, which includes the casual use of paper such as the scribbled notes you might find a receptionist has used to remember the name of a phone caller, visitor or phone number. We note that many organisations use contractors for this purpose and they comment that a Teacher's time is not best spent shredding paper.

We have a concern over the long term use of contractors, and feel it is only a matter of time before a white bag finds its way into a black bag environment, or the processor suffers a human or deliberately criminal failing that compromises your data.

3.17 Training

Compliance with GDPR requires the continuous identification of either new processes or new participants, both of which require structured training and

awareness of their security connotations. Satswana are always happy to discuss requirements that normally will fall within your current contract.

3.18 Paper files

We have all grown up loving the convenient access to information represented by paper, but in security terms it is the most portable and readable of any form of data and thus must be retired wherever it is possible to create a digital alternative.

3.19 Locked cabinets

It may seem very obvious, but if you are relying on keeping paper files, keep them in an environment where they cannot be readily seen, and which can be locked.

3.20 Email

Email is a hugely useful and ubiquitous means of communication. It is also insecure, the subject of frequent attack, can be misused with open address lists and you have no control over content – in that it can be forwarded and shared without your knowledge.

Recommendation

If you do have to send specific information out to a third party by email which contains sensitive information, use an encrypted email service. Please note that at the very minimum there are solutions (in Outlook for instance) that are free to use, though the password must be communicated to the recipient, and if SMS is used for that purpose you are exercising the additional security of two factor authentication.

Wherever possible do not send content within email, but use it as a prompt for the recipient to access the information by another means. This can be by looking at an area of the website, either on an open page, or behind a privileged login. Alternatively use a document collaboration service, Sharepoint is likely to be convenient for staff users of 365, this way you control access and control the content, going forward.

3.21 Smart Phones

The synchronisation of data between devices is both wonderful and dangerous. It is fantastic that our files are always up to date; regardless of the manner in which we access and work with them, but it also means that a copy of what might be extremely sensitive content might also be on our mobile phone. In turn that can be lost, stolen, or played with by a family member – three scenarios that create risk.

Recommendations

If a phone has dual private and business use (and realistically this is the only practical option), then it must deploy strong password access and any encryption available, plus have the remote delete option enabled.

It must be controlled according to your code of conduct and in line with your acceptable use policy, meaning that children do not play games on a phone that has a business application, for instance.

3.22 Policies

Schools generally deploy a number of policies which very sensibly and effectively provide a "rule book" for many aspects of life – all appropriately published.

Within GDPR/DPA this principle can be adopted and extended to seek specific consent on a website with the addition of appropriate phrases to other content. For example if a parent is signing up online for a school trip, then the addition of "by completing this form you are giving us your specific consent for the use of this data for administration, dietary and health information related to the trip" is the specific authorisation that is required.

Transparently published policies can also assist in many other areas, such as in freedom of information responses and subject access requests.

Recommendations

To review your code of conduct in light of GDPR and adopt changes as required reflecting the requirements of security and data privacy. (To be extended to third party contractors.)

Similarly to consider how an acceptable use policy can be aligned to suggested changes in the use of digital data.

You should review your privacy statement in line with the change in data ownership to the individual.

You should publish and implement a policy on both staff and pupils bringing their own device into the school.

It is suggested that you identify and review your retention policy, especially in light of the anticipated cull of paper. (Satswana can provide further details on this.)

Your CCTV policy should be created to minimise any work demanded through a subject access request (We have a new Images policy available).

3.23 The right to be forgotten

When considering this heading any paper files can be considered a disastrous liability that dictates the digitisation of records. There are conditions where data cannot be removed – indeed there is a current problem with software used by education in that it was never designed to facilitate deletion.

Recommendation

Techniques for the obfuscation of data exist that allow you to retain a record but not make it available ever again. These must be adopted in a manner that ensures that the data is indeed "forgotten" and made permanently inaccessible in the future.

3.24 Website

Continuously review the content of your website to identify any personally identifiable information. It may be appropriate to publish names and qualifications of staff, Governors and marketing information, but in each case you should hold the consent of that person to publication.

Please consider whether there are any aspects whereby data is shared with an external party within any part of the website, and if so include them on your processor list.

3.25 External Online Educational Sites

There are a number of online educational sites. You will wish to ensure that all such advanced teaching options are available but it is recommended that you carefully check what data they are using, how they process it, and who they might share it with. It is likely that you will decide that you must enter into an appropriate processor contract with them.

3.26 Breach response

It is technically extremely challenging to identify a breach, not least because the criminal does not wish to advertise their presence. There are instances of exploits being undiscovered for a number of years. The ICO do recognise that considerable attempts to penetrate your network are likely to be continuous and at some stage one might succeed. We recommend as follows:

Recommendations

a) If you are breached notify us immediately so that we may support you and advise the ICO
b) Prepare a reaction plan in advance, you need two things. The first would be web pages that you can instantly (via a DNS change) switch to giving information on the issue
c) The second requirement is a spokesperson who is trained in media relationships and who has an appropriate script prepared beforehand. Both these instant reactions will portray competence and confidence to the public. (Please recall the relative chaos of the Talk Talk breach where the Chief Executive was hung out to dry by the media.)

3.27 Subject Access Request

We expect properly constructed policies and an active engagement with external parties to minimise the likelihood of aggressive and litigious SAR's, but if you do get one please contact us so that we can provide support in response.

3.28 CCTV

We established that you had a CCTV system. There are differing views regarding what constitutes processing within a recorder. We do not subscribe to the view that the recording alone becomes a process. We state that only if human use of an electronic function has taken place does it become actionable in any sense, meaning that we will not trawl through CCTV to provide copies for access requests if they have never been viewed.

Recommendations

a) Please consider your site signage providing transparent information to the public regarding your use of CCTV
b) We suggest that your policy should be to state that you only review images in the event of an incident, otherwise they are not viewed. That will limit the response required by a Subject Access Request
c) If you do review an image, then you should keep a record of it according to your retention policy.

3.29 Use of Social Media

The use of resources such as Twitter are of benefit to the School but careful control should be exercised over what is published, who controls the account, and having

procedures in place to remove the privileges if an operating member of staff should leave.

Recommendation

Maintain an appropriate register with log in details so that a School controlled account (or accounts) on social media can be handed over or otherwise managed.

3.30 Encryption

Notwithstanding your current use and adoption of encryption, we would like to ensure that we cover some general points within this assessment. The first point is that you do not have to report a breach to the Information Commissioners Office (ICO) if the data is unreadable because it is encrypted.

The second point is that it is very often either a no cost, or very low cost, option that is selectable in many programs. We believe it would be good practice to always encrypt data if you have the option of doing so, particularly in the case of any device that is taken off premises.

Which brings us to USB sticks, ideally please do not use them at all, but if you must never take anything off site unless protected.

With email, once again please do not send content, refer back to data in a cloud source. (Dropbox was developed by a guy who kept forgetting his USB stick!) If you really must send sensitive data out of your control, then use whatever form of encryption is available to you, please!

3.31 Summary

In summary, Satswana found that xxxxx School really is compliant in terms of DPA 2018. Indeed, with every head of department we had the pleasure of talking to, they had a good understanding of what was required of both the school and their own areas of expertise, in terms of remaining compliant.

Satswana found that the vast majority of any personal data collected was digitised, stored safely and encrypted.

The adoption of Google's applications (Or Microsoft's as applicable) throughout the school is impressive, as it enables smooth collaboration, ease of access and safety of storage.

The majority of physical copies of data within the school are locked away safely.

In general, the recommendations made by Satswana have been minor, as the general data protection practices of the school are excellent. It has been a pleasure to get to know the staff and we will certainly look forward to working as a peripatetic member of their team for the future.

APPENDIX D
DATA PROCESSOR GUIDANCE

***Satswana note. Much of this guidance will not be of concern to you if we are qualifying your processors for you. However there will be some instances where you may wish to manage the agreement yourselves, so some of the technical content may still be of value to you.**

If not already in place, please create a list of the "Processors" you are dealing with, referring to the check list document contained in **Appendix I**. Please note that we are continuously capturing uses from schools, so many of the headings will not apply to you, simply ignore them please, and adopt those that do.

Similarly, there will be other specific processors that only apply to your organisation. This will be particularly so in the case of both your SENCO, the organisers of your school trips, and possibly your school meals provider, for instance. Please also read the Guide to Processors that follows!

1 Satswana Processor Guide

This guide is intended to assist Data Protection Managers within customer organisations that have contracted with Satswana for their fractional Data Protection Officer Service. The concern is that the Controller retains absolute liability, even if the Processor is at fault, so the contract that is entered into has to include all the elements within the Regulation.

- We are seeing a wide range of claims and a huge variety of approaches, some good, others either fake, naïve or deliberately fraudulent. This guide seeks to provide customers with benchmarks against which to judge the protection a contract affords.

2 We will approach this starting with ….

What does the General Data Protection Regulation actually say? The information can be found in Chapter IV, starting with Article 24 where the responsibilities of the Controller will be found. However, the "trouble" starts in Article 28, paragraph 1 *"the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation…."* Recital 95 places a duty on the Processor to help you do that.

You can read on within the Regulation, or cut to the attached **Appendix E** where we have listed the questions that you have to ask a Processor. They are not very

difficult to answer, so in Appendix B we have what we believe a model answer to the questions should look like.

Providing you are happy with the answers you receive, then you can agree a contract and the ICO have provided a model option that is reproduced at **Appendix G**. Clearly for any UK organisation it must be based on the appropriate UK law (English, Scottish, Northern Ireland or Welsh.)

3 So what are the problems?

a) It starts with the fact that many organisations, critical to your operation have either not produced a Processor contract, or it is hopelessly non-compliant, of which more below. Technically you should stop using them, but in practice that is likely to be impossible - but be clear that these organisations are exposing you to risk.
b) Others have chosen to present their agreements in a different form, referring to a policy held on a website for instance; or perhaps related to a service level agreement, offering you a variation on an existing contract. Those are fine if they answer properly the questions you have to ask in **Appendix E**. It will be a tedious exercise for a Controller to have to check, but we might assume it is a onetime exercise. If they do not, then however fancy and clever the documents look, and however big the organisation is, we stress again that they are not the organisation at risk, you are. We respectfully suggest that you cannot afford to let them bully you into submission. Write to them formally and record your objections, then you have evidence for the ICO if there should be an issue.
c) We have seen a professionally produced contract that requires the signature of your DPO. That is fundamentally misconceived, since it is the Controller who retains liability, not the DPO. You can appreciate the level of underlying issue when organisations are selling incorrect documents.
d) As to the issue of non-compliance, we have seen statements such as "We are GDPR compliant". They may be, but only if they can provide you with the aforementioned *"sufficient guarantees"* a totally unsupported statement cannot be relied upon, and cannot provide a basis for signing any form of evidential contract with them.
e) Similarly organisations claim compliance under the EU/US Privacy Shield. Ultimately the decision has to be yours, but we explain our objection to that option below.
f) One Processor contract we saw ran to 22 pages of dense legal language. We were convinced that the intention was to pull a fast one, but got lost in the verbiage and could not determine what was hidden and where, we were just convinced something had to be wrong. We can see no reason for the statements required going beyond two pages, nor for them to be any less understandable than the Regulation itself – which is pretty straightforward.

We recommend you reject any such impositions on your time as a matter of principle.

g) Recently any reader of this document will have found their email full of varying forms of entreaties to review your relationship with them under GDPR. You will have noted that some were properly written, requesting your specific consent to the specific use of your data. (Most you ignored and were delighted to see the back of!) Others were totally non-compliant, ranging from the "you do not have to do anything" to the bad old days of assuming an "opt in". The point is that a range of organisations have taken different approaches, some reasonable, others opportunistic, yet others frankly illegal. We fear that the same thing will happen with Processor agreements, coming from the same range of organisations – from the honest to the criminal. With an email it may just be annoying into the future, with a Processor contract – if it does not provide the *"sufficient guarantees"* – then your organisation is at risk. Hence our concerns to provide you with this guide, providing a bench mark, taken directly from the Regulation.

4 Can you rely on the EU/US Privacy shield?

The short answer is no, and it was specifically outlawed by the European Court of Justice in July 2020, but it must be your decision whether or not you accept the assurance by some US companies. The reasons for our point of view are:

a) The first point is the whole purpose of DPA. It was to create a common data landscape across the EEA so that data could be safely transferred between the Countries, relying on a common framework of law. From the Brexit point of view it has been mirrored as the Data Protection Act 2018, but if you have one EU national within your data, GDPR applies. As such it has become an Internationally accepted standard for data privacy, like ISO 27001 and similar standards apply all over the World. If a server is held within Europe, then a data controller must comply with GDPR: a Regulator in each Country that will enforce the Law (Chapter VI!)

b) At the same time as Europe was producing versions of the first form of the Data Protection Act, America produced the Safe Harbor Privacy Policy. This was abandoned following claims that it offended the Fifth Amendment of the US Constitution, and was replaced in 2016 by the EU-US Privacy Shield. We had three problems with that.

1 As we forecasted Privacy Shield suffered the same challenge as Safe Harbor and has been declared non-compliant.

2 It relied on a US Company "self-certifying" its compliance - and simply do not believe that can be trusted. Of course honest companies will be fine, but the risk comes from dishonest companies which will have no problem lying.

3 If the Server is within Europe, then you have the protection of a Regulator, whereas in the US a European Company would have to seek redress under US law. We believe that would be expensive and subject to considerable hazard.

c) Our simple conclusion, is why take the risk? If an honestly structured US based business wants European clients, then all they have to do is locate their server for that purpose in the EU, or appoint a European Representative. Our concern if they will not do that is that their financial model relies on selling the data they harvest for advertising or other purposes to generate their revenue. That takes us back to the very objection to the corporate misuse of personal data that gave rise to GDPR in the first place.
d) We have identified one provider that uses Fulton County in the State of Georgia as its legal jurisdiction; another stores data on secure servers world-wide. In both cases, there is a question of security and compliance that would need investigation.
e) We stress it remains your call!

4 Creating your Processor list

This is a list of anybody you share data with, and we suggest you record this on a simple spreadsheet so that you can monitor their compliance, Satswana will be happy to do the leg work for you and provide you with their prior approved list.

5 Dealing with minnows

We suspect that Processors will fall into three categories. The macro version will seek to dictate how they present the agreement, a take it or leave it attitude. They must not be allowed to get away with that for two reasons. First, as previously stressed, it is the Controller that retains the liability, so if a Processor does not do the job properly then it is not them that will suffer, it is you. We must demand that they answer all the relevant questions to your satisfaction. Secondly, they are not allowed to create circumstances that deny equal access to services. It will be annoying to those large corporates with huge legal departments – but GDPR means that they actually have to answer the requirements of their customers. It will be a new experience for them. Another category will be those who are cooperative, helpful, well briefed, and they will be easy to deal with. Hopefully as time goes on more and more will fall into this category.

But the final category is likely to be what we are calling the minnows, those that you share data with but who have no real resources to meet challenges such as this. Within the academic world we are talking about the connections for special education needs, speech therapists for example. Within local authorities it may be

clubs and similar organisations that rent facilities from you. Corporates may have an association with charitable interests. They may all be technically Processors, but they need help to meet your requirements as discussed in this paper.

We have three suggestions.

a) Where a local authority or the NHS is involved (or similar bodies), who may make services available to you, ask them to perform the role of Processor, with the individual then becoming a Sub Processor.
b) If you contract an individual directly, consider "adopting" them within your structure. If that means them coming under your DPO contract with us, we would ask that if they are dealing with any other customers, that when they list us as their DPO they add "sponsored by the xyz organisation" so that we know who they come under.
c) Finally, and especially in the case of b) above, do not share data with them at all, but make available a document collaboration area within your Sharepoint (or comparable) central server where their files etc., can be managed within your infrastructure.

We respectfully suggest that any other organisation that similarly supports Sub Processors in that way should also adopt document collaboration structures. There remains a case for email, but only if it is encrypted when dealing with sensitive data. We are seeking to meet the requirement for "privacy by design and default".

We believe that by supporting "minnows" in this way you will make your own Processor agreements much simpler to complete, whilst at the same time removing considerable stress from a sector of the population who do not have access to a fraction of your resources.

6 Third party services

Satswana has seen offers from other organisations offering to manage Processor contracts on your behalf. Whilst such an approach could clearly work if everybody had the same relationships, we respectfully submit that most of our customers will end up managing a huge range of organisations they share data with that are unlikely to be covered by a third party supplier. You have unique relationships with Auditors, Lawyers, HR Consultants, Debt Collection agencies, not to mention any sensitive data sharing arrangements in the area of special needs, for instance. The fact is that you cannot relieve yourself from the liability that attaches to a Controller, thus whilst third party support may be superficially attractive, they only have to make one mistake and it is your reputation that suffers. Since they cannot be experts in the unique circumstances that make up the associations within your organisation, we suspect that this is one management liability that should not be delegated.

7 Summing up

The purpose of the Regulation in creating the relative responsibility between a Controller and a Processor is quite clear, but we fear that interpretation (and possibly deliberate obfuscation) is going to make it very difficult for a Data Protection Manager to manage agreements and ensure that they are not exposed to risk.

To assist you in your determination we have gone back to first principles with the requirements within the Regulation, and then "turned that round" into what the answers should be.

We very much regret that there will be many examples of "fake compliance" presented to you. If you are in doubt, please ask us.

Appendix G provides a model agreement from the ICO, indicating that you do not have to be long winded. But please note that other documents may be referred to generally such as a webpage, a supply contract or a service level agreement.

Finally, to be as constructive as possible, at **Appendix H** we copy (rather poorly, the gaps in the document are embedded and we have not been able to remove them) a redacted document that we did find helpful and to be compliant. It is perhaps longer than we would like to see, and it refers to supplementary documents such as a Service Level Agreement, but we cannot reject all approaches, providing they answer the critical questions that the Controller must ask.

Final word, it is you, the Controller, who must be satisfied that you have received "*Sufficient guarantees*" from the Processor.

APPENDIX E
DATA PROCESSOR QUESTIONNAIRE

Please note that it should not be necessary for you to use this, but we have preserved the information in case you have an application that Satswana cannot process for you

Data Processor Questionnaire

This document is provided by a Data Controller to a Data Processor to comply with the duty of the former to assist with definitions and duties as defined in Recital 95 of the General Data Protection Regulation, with comprehensive coverage within Chapter IV.

Its purpose is to assess the level of compliance within your organisation and to address any areas that require attention following the legislative changes on 25 May 2018. It may assist you to review as a starting record the compliance that data processors will be required to cover under article 28.

It is our belief that you are a Processor who handles personal data of individuals on our behalf, and as such we are required to enter into an agreement with you. Prior to that we have a duty to ensure the processor's security arrangements are at least equivalent to the security that we are required to have in place as if we were processing the data ourselves. Please refer to the full requirements that we will be asking of you within Article 28 of GDPR. In this regard please refer to the model form attached as **Appendix G**

Please provide the following information on your organisation for record purposes

Organisation name
Address
Post code
Contact person
Email address
Telephone number

Please advise whether you have a Data Protection Officer, if so supply the following details

DPO Name
Email address
Telephone Number

To assist us with our own compliance responses, please provide the following information.

1 Define where the Data is stored (Please set out details of the database and filing systems containing personal data for the storage of information on behalf of the Data Controller)
2 Advise who has permission to access the data, both internally and externally
3 How is access to this data logged and controlled?
4 How and where is our dataset backed up
5 Is the dataset encrypted on your servers?
6 If so, when is it decrypted?
7 Please advise whether you apply anonymisation or pseudonymisation
8 Do you have a retention policy? How long do you keep personal data?
9 Are you able to restrict the purposes for which you process the information?
10 How often the personal information you process is updated?
11 Is any information you process known to be incomplete, outdated or wrong?
12 Is there any mechanism for data subject to access the data, and if so can they correct it?
13 Do you sell, rent, or by any means disseminate the personal information to third parties?
14 Do you have any mechanism to check the accuracy and completeness of data?
15 Do you have a process to update, correct or delete data?
16 Do you operate any regular or automated process to 'clean' your data?
17 Does any dataset include personal information on subjects under the age of 16?
18 Could the personal data ever get transferred to another party?
19 Does the dataset include recordings of video or sound that includes the public?
20 Do you maintain a record of processing activities that is frequently reviewed and updated which can be demonstrated to the Data Controller?
21 Please confirm that information (digital and manual, and especially special category data) is only stored in your organisation. If a third party (a Sub-Processor) is involved please provide full information.
22 Do you separately handle and store any special category data?
23 Where is archived information stored, in what format and medium? Please provide details of any Sub – Processor as in Question 21.
24 Describe the physical, administrative and technological security procedures in operation to keep all information secure.
25 Does anybody within or outside your organisation have access to the personal information of the Data Controller? If so, who authorises such access?

26 What policies and procedures do you have for detecting and dealing with breaches and can they be identified and reported to the Data Controller within 72 hours?
27 What data audit facilities or controls are in place to ensure that there is no internal unauthorised access to personal data?
28 How is personal information, including backups and archives, destroyed if you are instructed to do so by the Data Controller?
29 Who authorises the destruction and who carries it out?
30 What happens to the data at the end of the contract period?
31 Are you required to transfer data between departments or to third parties? If so how is the data transferred and what encryption or similar security is deployed?
32 Please confirm that no data including archives and backups is transferred outside the UK and EEA.
33 Do you have a privacy policy?
34 Please confirm that you are prepared to enter into a contract with us as required by GDPR as reproduced below:

28(3) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed, and the obligations and rights of the controller. The contract must stipulate that the processor will:

28(3)(a) process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);

28(3)(b) ensure those processing personal data are under a confidentiality obligation (contractual or statutory);

28(3)(c) take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;

28(3)(d) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;

28(3)(e) assist the controller in responding to requests from individuals (data subjects) exercising their rights;

28(3)(f) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);

28(3)(g) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);

28(3)(h) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.

(Numbering refers to the Sub-Articles in the General Data Protection Regulation)

APPENDIX F
DATA PROCESSOR CUSTOMER CONTRACT

As with Appendix G, this would only be relevant if Satswana cannot manage the process for you

Data Processor Customer Contract

This document is provided by (Name of Data Processor) a Data Processor under the terms of the General Data Protection Regulation (to become Data Protection Bill when passed), to our Data Controller customers to comply with our duty to assist with definitions and duties as defined in Recital 95 of the General Data Protection Regulation, with comprehensive coverage within Chapter IV.

Its purpose is to define the level of compliance within our organisation and to address any areas that require attention prior to May 2018. It may assist you to review as a starting record the compliance that data processors will be required to cover under article 28.

It is our belief that we are a Processor who handles personal data of individuals on your behalf, and as such we are required to enter into an agreement with you. We have a duty to ensure that our security arrangements are at least equivalent to the security that you are required to have in place as if you were processing the data yourselves. Please refer to the full requirements that we will be satisfying within Article 28 of GDPR.

We would advise that for these purposes our Data Protection Officer support is provided through Satswana Ltd. who can be contacted at …. Reference Processor DPO.

1 We would advise that your data is stored within systems provided by us under the terms of our commercial contract with you, available as a separate document.
2 None of our staff has permission to access the data, either internally or externally
3 Access to this data is logged and controlled (via a login register…?)
4 Your data is backed up as per the requirements in your commercial contract referenced in 1 above
5 You have opted to have your data encrypted on our servers
6 It is only decrypted when accessed according to your policies.
7 We do not apply anonymisation or pseudonymisation - that is under your control if required.
8 The data retention policy is set by you. We immediately delete all data if our contract with you ceases.

9 We do not process your information in any form.
10 We are not involved in any manner in which you update personal information.
11 We have no means of knowing whether any of the information that is processed is incomplete, outdated or wrong. That is a matter for your control.
12 We offer no mechanism for a data subject to access the data, and thus they cannot correct it. This control is solely through your access.
13 We do not sell, rent, or by any other means disseminate the personal information to third parties.
14 We have no mechanism to check the accuracy and completeness of data, which is solely under your control.
15 All processes to update, correct or delete data are under your control.
16 We do not operate any regular or automated process to 'clean' data.
17 If any dataset included personal information on subjects under the age of 16 then we would have no means of knowing that, all data classification is under your control.
18 Personal data would never get transferred to another party by us.
19 We would not be aware if any dataset included recordings of video or sound that included the public.
20 We maintain (what?) records of processing activities that are frequently reviewed and updated which can be demonstrated to the Data Controller?
21 We confirm that information (digital and manual, and especially special category data) as provided by you is only stored in our organisation. No third party (Sub-Processor) is involved except as provided for within our commercial contract referenced in Point 1.
22 Any separate handling and storage of special category data is subject to your decision and your policy.
23 Archived information is stored as agreed within the terms of our commercial contract referenced in Point 1.
24 Please find at Appendix tbn attached the physical, administrative and technological security procedures in operation to keep your information secure.
25 Nobody within or outside our organisation has access to your personal information.
26 We have policies and procedures for detecting and dealing with breaches which can be identified and reported to the Data Controller within 72 hours. Full details are contained in Appendix tbn.
27 The data audit facilities and controls that are in place to ensure that there is no internal unauthorised access to personal data is described in Appendix tbn.
28 Our process for the destruction of personal information, including backups and archives when instructed to do so by the Data Controller is described in Appendix tbn.

29 You authorise the destruction, which is executed as in 28 above.
30 At the end of the contract period all data is destroyed as in 28 above.
31 We are not required to transfer data between departments or to third parties?
32 We confirm that no data including archives and backups is transferred outside the UK and EEA.
33 We have a privacy policy as published on our website.
34 We confirm that we are prepared to enter into a contract with you as required by GDPR as below:-

a) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:
b) process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
c) ensure those processing personal data are under a confidentiality obligation (contractual or statutory);
d) take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;
e) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;
f) assist the controller in responding to requests from individuals (data subjects) exercising their rights;
g) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
h) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);
i) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.

APPENDIX G

MODEL PROCESSOR AGREEMENT FROM INFORMATION COMMISSIONER'S OFFICE

Please discuss with Satswana if you feel you need to use this form

Model Processor Agreement from Information Commissioner's Office

Agreement entered into between _____ (hereinafter referred to as "the Data
Controller") and _____ (hereinafter referred to as "the Processor")

1 Whereas the data controller has entered into a contract with the processor for the
management of a system/rendering of a service;

2 Whereas sub-article (2) of article 25 of the Data Protection Act ("the Act") provides that the relationship between a data controller and a processor shall be regulated by a contract in that "the carrying out of processing by way of a processor is to be governed by a contract or other legally binding instrument in a written or in an equivalent form";

3 Whereas the parties wish to regulate this relationship, the data controller is binding
the processor, and the processor undertakes, to act in compliance with the provisions
of the Act, to act in conformity with any directive, order or request for information from the Data Protection Commissioner, and in particular:

a to act only on instructions received from the data controller in terms of article 25 of the Act;

b to take all the necessary measures referred to in article 26(1) of the Act namely
to:-

"implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to the:

(i) Technical possibilities available;
(ii) Cost of implementing the security measures;
(iii) Special risks that exist in the processing of personal data;
(iv) Sensitivity of the personal data being processed."

The Processor binds himself to use personal data solely for the purposes of this Agreement and will not make copies, or otherwise reproduce personal data processed
on behalf of the data controller, unless this is necessary for the purposes of this Agreement;

Whereas article 26(2) stipulates that the controller shall ensure that the processor can
implement the security measures that must be taken, and that these measures are actually implemented as indicated by the controller;

a. The processor undertakes to respond immediately to every request for verification submitted by the controller in relation to processing of personal data regulated by this agreement and to inform immediately the controller with:

(i) Requests for personal data regulated by this agreement, by individuals (right of access requests) and also from third parties, including requests from law enforcement authorities;

(ii) Any accidental loss or unauthorised access to personal data regulated under this agreement and any legal proceedings initiated on the basis of an alleged breach of the Act.

To be signed and dated by both Data Controller and Processor

APPENDIX H
SAMPLE DATA SHARING AGREEMENT

As with Appendix G, please discuss with Satswana before entering into a data sharing agreement

DATA SHARING AGREEMENT

This Data Sharing Agreement ('the Agreement') is made xx April 2018 (the 'Effective Date') between the following parties:

Parties

"An Educational Organisation" **(The Data Controller)**

and

"A Data Processor" (The Data Processor)

Together and hereinafter referred to as 'the Parties'.

Background

The Parties are entering into this Agreement to enable the Data Processor to deliver the agreed support services as per xxxx's Support Service Level Agreement and Service Level Agreement (together hereinafter referred to as 'the SLA').

In the ordinary course of the SLA the Data Controller will provide information to the Data Processor to enable it to deliver the Support Services. Some of the information that is provided will be personal data (Personal Data as defined below) and will therefore require strict compliance with Data Protection Laws.

This Agreement is to define and govern the circumstances in which Personal Data can be shared between the parties and to grant the Data Processor and certain permitted third parties access to the Personal Data.

Agreed terms

1. Interpretation

The following definitions and rules of interpretation apply in this Agreement.

Definitions

Data Protection Laws mean the governing privacy laws of the UK from time to time.
Personal Data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data can include, but is not limited to, business, employee and pupil records to provide detail and context, full personnel files including the contract of employment, performance management records, occupational health (OH) reports, absence records, discipline and grievance

records, IT records, supplier contracts, accounting records and can include special categories of Personal Data.
Process/Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
SLA means the Supply Service Level Agreement and Service Level Agreement that are in place between the Data Controller and Data Processor from time to time.
Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric/genetic data.
In writing means communications via fax, email or letter.
Written notice means any notice given to a party under or in connection with this Agreement and shall be:
• Delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case).
Written notice shall be deemed received:
• If delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and

• If sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second day after posting.

2. Right to process Personal Data
The Data Controller hereby grants the Data Processor the right to Process Personal Data supplied by the Data Controller to deliver the support services agreed under the terms of the SLA.

3. Term
This Agreement will commence on the Effective Date and continues as long as the Data Processor provides a service under the SLA (or other relevant separate contract) and the Data Processor retains the Personal Data, unless the early termination clause is enacted by either party. If terminated early, the return or destruction clause (below) will apply as if the Agreement has reached its natural termination date.

4. The Processor's use of data

4.1 Standard of care
The Data Processor shall exercise at least the same degree of care as it uses with its own data and confidential information to protect the Personal Data from misuse and unauthorised access, disclosure and/or destruction.

4.2 Purpose

4.2.1
The Data Processor provides access to XX services, financial, legal and/or HR advice (either directly or through third parties) to ensure the Data Controller follows best practice and maintains employment law and financial compliance.

4.2.2
The parties consider data sharing (including sharing of Personal Data) necessary in order for the Data Processor to deliver the SLA.

4.2.3
The Data Processor agrees to Process the Personal Data in accordance with the Data Controller's written instructions, and only for the purposes of providing the SLA. For the avoidance of doubt, the Data Controller's written instructions already form the basis of the terms and conditions of the SLA.

4.2.4
The Parties shall not Process Personal Data in a way that is incompatible with the purposes described in the SLA.

5. Security of data

5.1
The Data Processor shall take such technical and organisational security measures as required by law and to meet the reasonable expectations or direction of the Data Controller.

5.2
Such technical and organisational measures shall include appropriate safeguards to protect the Personal Data from misuse, unauthorised access or disclosure. The safeguards will include but are not limited to:

• Maintaining physical security and access restrictions for any server or system on which the data is stored.

• Ensuring that all mobile devices (eg laptops, smartphones, iPads) are encrypted.

• To monitor and restrict access to data to maintain confidentiality and data integrity.

• Ensure all directors, employees, consultants, third party suppliers and representatives understand and comply with a duty of confidentiality.

• Taking any other measures reasonably necessary to prevent any use or disclosure of the data other than is allowed under this agreement.

• Only transfer personal data via a secure encrypted server.

APPENDIX I
SHARED DATA PROCESSOR GUIDE LIST

This list has been removed, copies of the most up to date available spreadsheet will be provided on request

Please note that the original Appendix J was also removed on review in January 2020

APPENDIX K
EXAMPLE PRIVACY POLICIES

Important Satswana note:

Below you will find two examples of privacy policies, the first would need revising to reflect the relevant clauses in DPA 2018 rather than GDPR 2016, though in practice the drafting is exactly the same. All of these policies came from an original reputable source, such as a Local Authority or the Department of Education and should be considered as being the best "guess" as to phrasing and needs – and in producing your policy it is perfectly acceptable if you do the same there is no such thing as a 100% perfect answer. Please bear that in mind when you are asked to review your own policies. If they can be obviously updated, then fine – please do that – but otherwise English Law is based on the outcome of actual cases creating a precedent which in turn becomes the law. Thus only if we have a precedent to go by can we suggest any future changes, which of course we will all do if that need becomes apparent. Our message is not to be concerned. Providing we are all using our best endeavours to present a transparent statement to the world, there is no further basis for criticism – unless a Court subsequently dictates that we must change.

Privacy Policy

Privacy Notice (How we use pupil information)

1. The categories of pupil information that we collect, hold and share include:

    - Personal information (such as name, unique pupil number, address and relationship to other pupils at the school)
    - Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
    - Attendance information (such as sessions attended, number of absences and absence reasons)
    - Behavioural information (such as positive or negative behaviour, exclusions, detentions)
    - Relevant medical information
    - Assessment information
    - Post-16 learning information
    - Special educational needs information
    - Biometric Data (we use an automated biometric fingerprint recognition system which is used to purchase items from the school canteen and in our library to loan books. The system takes measurements of the fingerprint; it

does not capture a complete image so the original fingerprint cannot be recreated from the data)

Why we collect and use this information

2. We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

3. On the 25th May 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR). The condition for processing under the GDPR will be:

Article 6

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 9

1. *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

2. *Paragraph 1 shall not apply if one of the following applies:*

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. The Education Act 1996 - Section 537A – states that we provide individual pupil information as the relevant body such as the Department for Education.

5. Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

Collecting pupil information

6. Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

7. We hold pupil data for for as long as we need to in order to educate and look after you. We will keep some information after you have left the School, for example, so that we can find out what happened if you make a complaint.
8. In exceptional circumstances we may keep your information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under the law.
9. We can keep information about you for a very long time or even indefinitely if we need this for historical, research or statistical purposes. For example, if we consider the information might be useful if someone wanted to write a book about the School. Please see our Information and Records Retention Policy for more detailed information.

Who we share pupil information with

10. We routinely share pupil information with:

- schools that pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- Careers advisors
- Medical practitioners and NHS staff
- Agencies involved in caring for and supporting pupils
- Parents and carers
- Exam boards
- Our catering companies
- External suppliers (e.g. travel companies or those providing off-site activities)
- Curriculum support providers (e.g. SAM Learning and My Maths)

Why we share pupil information

11. We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
12. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

13. We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

14. To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

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

16. This enables them to provide services as follows:

- youth support services
- careers advisers

17. A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

18. We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

19. This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

20. For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

21. The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

22. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

23. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

24. The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

    - conducting research or analysis
    - producing statistics
    - providing information, advice or guidance

25. The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

    - who is requesting the data
    - the purpose for which it is required
    - the level and sensitivity of data requested: and
    - the arrangements in place to store and handle the data

26. To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

27. For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

28. For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

29. To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

30. Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs I Begum, the school's Data Manager via Reception.

31. You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

32. If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

33. If you would like to discuss anything in this privacy notice, please contact:

(Satswana DPO information, normally placed on your website)

Please note that there are certain places that you must publish who your DPO is, on your website for example. For those purposes the DPO should be Satswana Ltd please, with email of info@satswana.com ; telephone number 01252 516898, if you need an office address as well it is Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

Review

34. Standard DfE Privacy Notice text adopted May 2018 with appropriate alterations made to reflect xxxx High School practice. The member of staff responsible will review this document every 12 months.

Website - Privacy and Retention

OUR PRIVACY AND COOKIES POLICY (Privacy Policy – draft suggestion for review and edit)

PRIVACY

The organisation (insert) is committed to respecting your privacy and the privacy of every visitor to our web site. The information we collect about you will be used to fulfil the services you might request and enable us to improve how, as a company, we deal with you.

Should you have a question about the data we store, our contact details are:

Contact name
Organisation
Address Line 1
Address Line 2
TOWN
Post code
controller@organisation.com
(Phone number)

The information that we collect about you will only be used lawfully (in accordance with the Data Protection Act 2018 and the General Data Protection Regulation). All data is retained exclusively within the United Kingdom (amend as required).

This information will not be disclosed to anyone outside (insert) or its associated companies, partners, and other companies with which (insert) has arranged services for your benefit.

We expect the information we hold to be accurate and up to date. You have the right to find out what information we hold about you and make changes, if necessary. You also have the right to ask us to stop using the information. To have your information removed, please contact us.

The type of information that we will collect on you, and you voluntarily provide to us on this website includes:

* Your name
* Address
* Telephone number(s)
* Email address
* Survey responses
* IP address

We may, in further dealings with you, extend this information to include your address, purchases, services used, and subscriptions, records of conversations and agreements and payment transactions.

You are under no statutory or contractual requirement or obligation to provide us with your personal information; however, we require at least the information above in order for us to deal with you as a prospect or customer in an efficient and effective manner.

The legal basis for processing your data is based on your specific consent that we will have requested at the point the information was initially provided, therefore we will not store, process or transfer your data outside the parties detailed above unless you have given your consent for us to do so. You can remove this consent at any time via the unsubscribe link included on all emails we send, or by contacting us and requesting that your details be deleted.

Unless otherwise required by law, your data will be stored for a period of 2 years after our last contact with you, at which point it will be deleted.

PROTECTION OF PERSONAL INFORMATION

(insert) takes precautions, including administrative, technical, and physical measures, to safeguard your Data against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.

(insert) uses industry-standard efforts to safeguard the confidentiality of Data, including encryption, firewalls and SSL (Secure Sockets Layer). We have implemented reasonable administrative, technical, and physical security controls to protect against the loss, misuse, or alteration of your Data.

COOKIES

This site uses cookies – these are small text files that are placed on your device to help this website to provide a better user experience. In general, cookies are used to retain user preferences, store information for things like shopping carts, and provide anonymised tracking data to third party applications like Google Analytics. As a rule, cookies will make your browsing experience better. However, you may prefer to disable cookies on this site and on others. The most effective way to do this is to disable cookies in your browser. We suggest consulting the Help section of your browser or taking a look at the About Cookies website which offers guidance for all modern browsers.

GOOGLE ANALYTICS

This website sets “first party” cookies through its use of Google Analytics. We use Google Analytics to provide us with non-personal site analytics, which in turn help us improve this website. Google Analytics tracking uses cookies in order to provide meaningful reports about web site visitors’ but they do not collect personal data about you. Google Analytics sets or updates cookies only to collect data required for the reports. Additionally, Google Analytics only uses first-party cookies. This means that all cookies set by Google Analytics cannot be altered or retrieved by any service on any domain other than dpocentre.com. Further detailed information on Google Analytics cookies can be found here.

https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

If you have a concern about how we handle your data, or you would like to lodge a complaint, you may do so by contacting The Information Commissioners Office.

Retention Policy

It is the policy of (insert) that personal data should not be retained longer than necessary, in relation to the purpose for which such data is processed.

(insert) will provide individuals with access to information regarding their personal data that we hold on request.

The Executive of (insert) has responsibility for the management of personal data. (insert) complies with all compliance requirements of GDPR including the right to erasure of personal data if the data subject withdraws consent.

In the latter event, data may be anonymised by one of the following methods

- erasure of the unique identifiers which allow the allocation of a data set to a unique person;
- erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
- separation of personal data from non-identifying or
- aggregation of personal data in a way that no allocation to any individual is possible.

APPENDIX L

EXAMPLE ACCEPTABLE USE POLICY

Acceptable use policy. This example was originally drafted for the Janet educational network and is designed for data use. A School may have other reasons to use a AUP within their standard discipline structure, and you will note that in the JANET case they do refer to other documents

Introduction to this draft document

An **acceptable use policy (AUP)**, is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used. AUP documents are written often to reduce the potential for legal action.

AUPs are an integral part of the framework of information security policies; it is best practice to ask new organisation members to sign an AUP before given access to IT.

This document focuses on education, so should be amended for local authorities or commercial organisations. Please amend in a manner that suits your Organisation. We suggest replacing “Organisation”, then read again to ensure it imparts intended meaning.

IT Acceptable Use Policy (AUP)

What you may and may not do when you use the Organisation's IT systems, and the consequences of breaking the rules.

Introduction

It is the responsibility of all users of the Organisation’s IT services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This AUP is intended to provide a framework for use of the Organisation's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.2 Policy

This AUP is taken to include the JANET AUP and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service. The Organisation also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

1.3 Scope

Members of the Organisation and all other users (staff, students, visitors, contractors and others) of the Organisation's facilities are bound by the provisions of its policies in addition to this AUP. The Organisation seeks to promote and facilitate the positive and extensive use of IT in the interests of supporting the delivery of learning, teaching, and innovation to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the Organisation.

1.4 Control of Data

Information must be retained under the control of the Organisation at all times. You are not authorised to copy any data to any other device other than storage provided by the Organisation, including, but not limited to, local drives, USB Sticks (unless provided by the Organisation and encrypted) and remote document storage areas. Where information is synchronised to another device you must inform us and enter into an agreement for its remote deletion. You must not take photographs except using equipment provided by the Organisation, and any images must be immediately deleted after uploading to the controlled environment. Sensitive data should not be sent by email unless encryption is used and wherever possible names should be anonymised.

2 Unacceptable Uses

a) The Organisation Network (Network) may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited "nuisance" emails;

4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the Organisation or a third party;
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings the Organisation into disrepute.

b) The Network must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other Organisation resources;
2. corrupting, altering or destroying another User's data without their consent;
3. disrupting the work of other Users or the correct functioning of the Network; or
4. Denying access to the Network and its services to other users.

c) Any breach of industry good practice that is likely to damage the reputation of the JANET (or other) network will also be regarded prima facie as unacceptable use of the Network.

d) Where the Network is being used to access another network, any abuse of the AUP of that network will be regarded as unacceptable use of the Network.

e) Users shall not:

1. introduce data-interception, password-detecting or similar software or devices to the Network;
2. seek to gain unauthorised access to restricted areas of the Network;
3. access or try to access data where the user knows or ought to know that they should have no access;
4. carry out any hacking activities; or
5. Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3 Consequences of Breach

In the event of a breach of this AUP by a User the Organisation may in its sole discretion:

a) Restrict or terminate a User's right to use the Network;

b) Withdraw or remove any material uploaded by that User in contravention of this AUP; or

c) Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the User is also a member of the Organisation community, the Organisation may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Charter, Statute, Ordinances and Regulations.

4 Right to Monitor and Access Emails etc

The company and its management retain the right to monitor and access emails of employees. This applies when it is necessary it is necessary for business purposes.

5 Definitions

Organisation Network – all computing, telecommunication, and networking facilities provided by the Organisation, with particular reference to all computing devices, either personal or Organisation owned, connected to systems and services supplied.

APPENDIX M EXAMPLE TAKING, STORING AND USING IMAGES OF CHILDREN POLICY

This appendix has been removed. Please request a copy of our updated and integrated "Images" document in its place

The Appendix N consent form has also been removed, see our Images policy please

APPENDIX P EXAMPLE CCTV POLICY

This policy has been retained for those locations that may have a very significant CCTV structure, and where you feel that the clauses within our Images Policy are not sufficiently comprehensive.

CCTV Policy

Dated: xx xxx 2018 Review: xx xxx 2022

Introduction

1. The School uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to provide a safe and secure environment for its pupils, staff and visitors, and to prevent loss or damage to school property and surrounds. This policy outlines the school's use of CCTV and how it complies with the General Data Protection Regulation; it is to be read in conjunction to the School's data protection policy.

   a. The system comprises a number of fixed and dome cameras.
   b. The system does/does not have sound recording capability.
   c. The system is/is not linked to staff or pupil attendance records.
   d. The system is not linked to automated facial recognition or number plate recognition software thus all individuals' images are anonymous until viewed.

2. The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team / Business Manager.

3. The CCTV is monitored securely from the Security/Business Managers/Admin office. The school server stores the images and is retained on-site. Access to the images is controlled by the Business Manager, or in his absence, The Senior ICT technician and is password protected.

4. The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community.

5. The school's CCTV Scheme is included in the School's registration with the Information Commissioner as a data processor.

6. All authorised operators and employees with access to images are aware of these procedures that need to be followed when accessing the recorded images. Through this policy, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The school's 'Data Controller' (Head Teacher Title NAME NAME) will ensure that all employees are aware of the restrictions in relation to access to and disclosure of, recorded images by publication of this policy.

Statement of Intent

7. The school complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure that CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

8. The School's CCTV surveillance cameras are a passive technology that only records and retains images. They are not linked to automated decision making or facial or number plate recognition software. Transmission is by cable direct to the server.

9. CCTV warning signs are clearly and prominently placed at the main external entrance to the school, including further signage in other outdoor areas in close proximity to camera positions. Signs will contain details of the purpose for using CCTV (**see Appendix Q**). In areas where CCTV is used, the school ensures prominent signs are placed within the controlled area.

10. The recordings will be filed with accurate metadata noting the camera location and time of the recording.

11. The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting the Cameras

12. Cameras are sited so that they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated.

13. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which includes outdoor/indoor areas. The system design is sympathetic to the privacy of surrounding public and does not monitor public space outside the legitimate areas of interest for the School.

14. CCTV will not be used in classrooms but in limited areas within the school building that have been identified by staff and pupils as not being easily monitored at all times.

15. Members of staff will have access to details of where CCTV cameras are situated with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

16. It is not the school's policy to conduct 'Covert Monitoring' unless there are 'exceptional reasons' for doing so. Any such monitoring would be temporary and be justified as 'exceptional'. The covert surveillance activities of public authorities are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. Such type of recording is covert and directed at an individual or individuals. The school may, in exceptional circumstances, determine a sound reason to covert monitor via CCTV. For example:

a. Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

b. Where notice about the monitoring would seriously prejudice the reason for making the recording.

17. In these circumstances authorisation must be obtained from a member of the senior leadership team and the school's 'Data Controller' advised before any commencement of such covert monitoring.

18. Covert monitoring must cease as soon as necessary, such as following completion of an investigation.

19. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

Storage and Retention of CCTV images

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

21. All retained data will be stored securely at all times and permanently deleted as appropriate / required.

22. Recorded images will be kept for no longer than 3 months, except where there is lawful reason for doing so, such as discipline investigations. Images are deleted from both the server and back-up server.

Access to CCTV images

23. Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

24. Access to stored images will only be granted in the case of an incident. To be viewed in the course of the incident's investigation.

Subject Access Requests (SAR)

25. Individuals have the right to request access to CCTV footage that constitutes their personal data, unless an exemption applies the General Data Protection Regulations.

26. All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

27. The school will respond to requests within one month of receiving the written request and any fee where disproportionate effort is required to adhere to the request.

28. Disclosure of information from surveillance systems must be controlled and consistent with the purpose(s) for which the system was established. When disclosing surveillance images of individuals, particularly when responding to subject access requests, the school will consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration will be given to the nature and context of the footage.

29. The subject will be supplied with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply. The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort, whereby the disproportionate effort may incur an administration fee.

30. Further guidance on SARs is within the Data Protection Policy.

Access to and Disclosure of Images to Third Parties

31. There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

32. Requests for images and data should be made in writing to the Head Teacher.

33. The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

34. Data transfer will be made securely and using encryption as appropriate.

Complaints

35. Complaints and enquiries about the operation of CCTV within the school should be directed to the Head Teacher in the first instance.

36. Further Information can be found at www.ico.org.uk

APPENDIX Q
EXAMPLE CCTV CHECKLIST AND SIGNAGE

*As with Appendix P above, this document is retained for the benefit it may bring to

the larger user

CCTV Checklist

This CCTV system and the images produced by it are controlled by the Business Manager who is responsible for how the system is used under direction from the schools 'Data Controller'. The school notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose.

The School has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of the school's community. It will not be used for other purposes. The school will conduct regular reviews of its use of CCTV.

	Checked (Date if appropriate)	**By**	**Date of next review**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	Yes.		
There is a named individual who is responsible for the operation of the system.	Yes.		
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	Yes.		
Staff and members of the school community will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.	Yes.		
Cameras have been sited so that they provide clear images.	Yes.		
Where possible, cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes.		
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	Yes.		
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Yes.		

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Yes.		
Except where individually authorised, images have not been provided to third parties.	Yes.		
The organisation has a policy for how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from the Data Protection Officer at Satswana Ltd.	Yes		
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes. (Daily checks)		

CCTV Signage It is a requirement of the General Data Protection Regulation to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

All CCTV operations should be compliant with the ICO Code of Practice

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for any enquiries

Example sign.