satswana

Company registered number 09329065 www.satswana.com

Satswana Reference Manual Version 1.1 May 2021

Please see introduction for more information but this is an early release copy designed to get the information into the hands of our customers as early as possible. It is intended that you can go straight to a heading that interests you for a summary, and where additional material is available please request a copy. In that manner we are able to keep track of what interests our customers, and seek to intervene and support where possible. We always welcome any criticism and contributions to the content, but do not include the explanatory papers in order to keep the Manual a manageable size. The fundamental intent is to ensure that all customers, especially new customers, receive a rapid understanding regarding what is available to support you from Satswana

Contents

1 Introduction

This Reference Manual will be constantly updated, with the latest version being available on the Satswana website (https://www.satswana.com/Resources) under the Resources tab.

Under each heading there may be a reference to other available resources which can be supplied on request. They are not contained within the manual itself since it would become too unwieldy, and in any event they may be subject to change.

Our purpose is to provide you with access to the information you need, or the confidence that it can be found. However it is Satswana's role and task to be expert in these subjects and we would wish to stress that we always want to hear from you whenever you have any sort of issue. Under the "Contract" heading you will note both the duties of your DPO, and also your responsibility to involve us appropriately in your decision making. As such we are peripatetic members of your staff.

It is perfectly reasonable for you to have concerns as to whether you are doing the right thing, is your training up to date, should we conduct an audit, are we exposed to breaches and attack, how do we handle access requests? It is our job to provide those answers and to remove any concerns you might have. Thus this reference manual is for your comfort and guidance, not a replacement for our doing the job for you.

We will always stress that we love questions, it is never a bother – we learn what concerns you as a result of the contact. Furthermore, when we cannot answer, and we are unashamed to be constantly learning, we will ensure that we research a solution, thus adding to our experience and competence, and subsequently enhancing this manual. We thank you in advance.

2 Processing

Satswana will manage a master spreadsheet containing the Processor organisations that you deal with in order to provide you with an asset register of compliant organisations.

If a Processor you are dealing with is not listed, please forward the contact details to us and we will check them out and add them to the list, thus benefitting everybody with enhanced content.

We would point out that ultimately it is your management decision as to whether or not you use a Processor. We might describe it as being non-compliant, but if your risk analysis satisfies you that the operational benefit to your school outweighs that risk, then (to use our oft quoted mantra) "you are the Boss" – but you must please record that executive decision in case of any challenge.

Currently we are seeking updates from Processors following the decision of the CJEU in July 2020 to declare "Privacy Shield" non- compliant (in the same manner and for the same reasons as they previously disqualified "Safe Harbor.") Where appropriate we are also confirming compliance with the Children's Code, effective September 2021.

Additional material, Processor List

3 Data Audit

Much is made within the Regulations regarding a Data Audit, but in practical terms every school deploys substantively the same data, though some functions might be available from different software providers. Satswana will be pleased to discuss this aspect with you, but in the meantime we can provide a template answer which we believe will suit most organisations

Additional material

Information Asset Guide (template)
GDPR Audit check.doc

4 Impact Assessment

When GDPR first came out it was a requirement of the Regulation that a School should conduct an assessment of the impact of the new regulations on their administrative and managerial functions. Most will have done this and by subsequent osmosis, or indeed because your data practices were originally compliant with DPA 1998, you will be assured that your practices are satisfactory.

However, Satswana will always be pleased to discuss any arising concerns, and we would point out that you must make a further assessment whenever you adopt new software. Please see the Contract heading for notes regarding the requirement to involve us

Additional material

Examples of documented Impact Assessments will be found within our Guidance Manual under Resources on the website

Information Asset Audit Guide (Draft of standard DPIA for schools)

5 Retention

Our thesis is that no school can currently effectively manage a digital data retention policy because the software tools they have are not fit for purpose, so any automated or algorithm driven compliance is out of the question. Similarly, any manual deletion might reduce the quantity, but it is not a sustainable policy for the future.

Satswana can discuss with you possible work arounds, especially a policy on reducing the use of emails.

Additional material

Records schedule and Records Management Policy
Satswana data retention document

6 Policies for DPA

Satswana have reviewed the original policies that were created in the main by either the DfE or a Local Authority legal team and have sought to bring them into a more current form by amending the original references to GDPR and replacing them with DPA 2018, bearing in mind we now operate under English Law, not European Law

Statutory policies include Data Protection and Protection of Biometric Data

Additional material, we can provide updated templates for all policies

7 Reporting

If you think you have a breach, or suspect an incident might be one, please immediately report it to us – since if it has to be then reported to the ICO we only have 72 hours from the time of the incident to do so.

Many breaches may not have to be reported, especially if we assess that there is no subsequent risk to persons from the incident, however to protect yourselves you should have an email trail showing you consulted Satswana

Please note that by informing us via email we keep a record of all breach reports

8 ICO Liaison

If an incident does have to be reported, then we will manage that for you. Similarly if you receive a complaint from the ICO, Satswana will prepare a report in response and manage the interaction.

9 Training

Satswana are always delighted to take any opportunity to support your staff training, either with the materials noted below, or in person. If you wish us to attend an SLT meeting, or discuss matters with a Governor, we will be delighted to do so. Similarly if you wish us to address your whole staff on an inset day, then we will endeavour to make the subject interesting and engaging for them, whilst ensuring that they are relaxed and confident in the subject

Additional material, we have a range of training resources available to suit different audiences

10 Software

As mentioned under our retention heading Satswana has distinct views on the poor calibre of software provided for management in education and we will be constantly campaigning for an improvement. We always welcome engaging with interested customers on this subject.

Additional material, papers on strategy and implementation available

11 Access requests

If you get any form of access request, be that a request for a copy of an education record, a Subject Access Request, or one under the Freedom of Information Act, please immediately advise us so that we can assist your response.

Additional material, Satswana Exemption Guide

12 Disposal

How you dispose of anything from your estate has to be carefully considered in the light of data protection. One organisation never recovered from casting out a filing cabinet that still had extensive and sensitive records stored in it.

Paper of any sort is one area of risk, clearly cross shredding is the preferred means of reducing the risk, but still people have been known to reassemble documents.

Any form of digital disposal almost certainly requires a specialist contractor, but even then you have to be sure you can trust them to do what they say they will do, and not export the disks to a West African country where they are routinely examined for valuable data.

We provide a guide on how to delete the data yourselves and if you can possibly make the time, that is the only really certain manner in which it can be done.

Incidentally we are aware of what we consider to be fairly underhand behaviour by some copier companies to extort funds for the removal of sensitive data. Please contact us if you experience this, since we believe the supplier has the liability to make the data safe, and should not be charging the customer

Additional material, guide to data deletion

13 Data Security

That Data Security should be number 13 on our list is probably Karma, because it is clearly a huge subject with a host of variations and no single school is likely to be the same.

You may have on premise equipment, use a Cloud service, have a hybrid of the two, or indeed place considerable reliance on the support of a third party such as one of the Grids for Learning

Satswana will be happy to discuss any arising matters with your IT provider or in house specialist

Additional material, Satswana Systems Analysis spreadsheet for recording IT spends

14 Physical security

Satswana discovered from an ICO inspection that the physical security of your premises, buildings and offices are considered just as seriously as any digital security so you should have conducted a risk assessment of this aspect as well as your documentation.

Additional material, summary of an ICO visit

15 Encryption

This is possibly the biggest and most important word in data security since data that is encrypted becomes impossible to read – meaning that any hack or other exploit does not have to be reported to the ICO.

Satswana will be encouraging all its customers to adopt encryption wherever possible, particularly on USB sticks if they have to be used at all.

Additional material, please request support on how encryption might be enabled

16 Briefing

When an organisation first joins Satswana we are pleased to provide an SLT briefing and pending being able to do that – or indeed in circumstances where staff change - we can provide a pre-briefing document that we are happy to provide on request

Additional material, Pre-briefing document

17 Contract

You may already be contracted to us, but if not we are happy to provide you with our standard form. We would also like to bring to your attention how the Regulation requires you to interact with your DPO (essentially you must consult us on any aspect that could affect your data security, including taking on a new product).

Additional material

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

18 Governors

Since January 2021 Governors have a responsibility for cyber security so Satswana requests that our update documents be shared with the Governor responsible for data protection so that they in turn can brief other members on any subject of importance.

We believe that the most effective way of informing Governors is to share discussion documents with them on a regular basis, rather than a more structured and formal reporting process – because it provides detail that can be genuinely addressed, rather than a generalised overview that might not carry the same impact. Satswana also thinks that Governors will find that approach more interesting and rewarding.

However, if a formal report is ever required, we will be happy to provide it

19 Data sharing

Satswana does not support the majority of data sharing agreements, seeing them too often used as a means of illegally seeking to circumvent the regulations. Our paper on the subject goes into greater depth, but if you are asked to agree to one, please let us know immediately and we can cover the specific detail together

Additional material, issues arising from data sharing

20 ICO registration

All schools must be registered with the ICO and their choice of DPO notified, however please consult us on this issue since many overpay. For instance an entire Trust is covered by a single £40 registration; they never have to pay more regardless of staff numbers. Working the other way a small Primary also paid £40 and had to pay additionally for a tiny nursery that was contained within a Limited Company. It is a small point, but we have learned the hard way. A Public Authority that is not a charity or a Trust will pay according to the number of Staff, and very often that will be a £60 Tier 2 fee, but it can go up to £2900!

21 Backup

We cannot stress strongly enough the importance of backing up your software, and also recommend taking an additional "snapshot" backup at a given point in time so that if your backups are compromised by ransomware you have your history in a secure form. The snapshot should be removed entirely from your network and perhaps stored in a secure location off the premises entirely. If you do get hit with an exploit they may wait until all your backups are infected, and then only the snap shot will give you a chance of recovery. You will possibly lose all your data since you took the record, but that can normally be partially recreated – what you cannot possibly recover is your entire back history.

Please note that there is no question of paying a ransom, not least because you are dealing with criminals who have already stolen your data and who will cheerfully steal your money as well.

Additional material, further advice and reports on backups

22 Images

Satswana can provide a consolidated policy to cover all your use of images, including CCTV

Additional material, Images policy

23 Data Protection Manager

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

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

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

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

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

The most material point is the manner in which the original GDPR returned rights over the ownership and management of data to the individual, which in turn placed a responsibility with the controller to look after something that does not belong to

them. Whilst that introduces a new liability to an organisation, many will applaud its intent from a personal perspective.

Additional material, Data Protection Manager Duties in Schools

24 Passwords

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

Additional material, Satswana Password Guidance

25 Future direction

Satswana seeks to continuously advance the adoption of technology in order to achieve the objective of "privacy by design and default". As such we will be researching and implementing new ideas such as that represented by the "360° economy" whereby an individual retains absolute control over their personal data, only granting consent to its access and use for a specific purpose.

Additional material, a briefing on the movement towards a 360° economy

26 Visitor system

Satswana must declare an interest in www.idmesafe.com as a visitor system, since members of Satswana are also investors into what is effectively a first example of the availability of a product that meets the objectives of a 360° economy. Currently undergoing final trials it is due to be available in September 2021.

27 Audits

Satswana will always be delighted to support you in any audit that you feel your system requires, especially perhaps where your Responsible Officer requires assurance regarding your Cyber Security and GDPR compliance. Equally we have a range of resources that you can use for a self-audit, please let us know your requirements.

28 Satswana Contact Details

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.