satswana

Company registered number 09329065 www.satswana.com

**Consolidated Update Documents from 2019**

This document contains a consolidation of all the updates published in 2019 and must be seen as being information in a historical context. Many aspects will remain entirely relevant and useful, especially some of the draft document supports. Others, such as our attendance at the Schools and Academies Show and the historical view of Brexit will not be of continuing interest. It is our hope that the following contents list will identify any articles that you might wish to study. We are astonished to note that it is 75 pages!

**Contents**

## A New Year GDPR Update from Satswana

1 **After Brexit?**
2 **PECR**
3 **No Fear!**
4 **Training video**
5 **All websites should be HTTPS**
6 **Data Care Act (US)**
7 **New risk identified for MAC's**
8 **Prize for the worst PR following a breach**
9 **Extortionists lie!**
10 **Just how dangerous is data**
11 **Prosecutions do take place**
12 **ICO determination regarding Public Health England (NHS data)**

Happy New Year, let's start with a pat on the back for our customers, since in a recent survey, when asked how far along they were in achieving GDPR compliance, only 29% said they had implemented all necessary changes. Thus you are all "thought leaders" in this field.

### 1 After Brexit?

Hard or soft, little will change if you process data only in the UK, but you will still have to apply GDPR to anybody whether they are a customer, pupil, or parishioner who is European within your database.

The Government stated: "The EU (Withdrawal) Act 2018 (EUWA) retains the GDPR in UK law. The fundamental principles, obligations and rights that organisations and data subjects have become familiar with will stay the same. To ensure the UK data protection framework continues to operate effectively when the UK is no longer an EU Member State the Government will make appropriate changes to the GDPR and the Data Protection Act 2018 using regulation-making powers under the EUWA."

The Government plans to issue more detailed guidance in the next few weeks, but have said that the new regulations and detailed guidance will:

- Preserve the GDPR in local law;
- Confirm that the UK will transitionally recognise all EEA countries (including EU Member States) and Gibraltar as 'adequate' to allow data flows from the UK to Europe to continue;
- Preserve the effect of existing EU adequacy decisions, including the EU-US Privacy Shield, on a transitional basis;
- Preserve EU standard contractual clauses and binding corporate rules authorised before Exit Day;
- Maintain the extraterritorial scope of the UK data protection framework; and
- Require non-UK controllers that are subject to the UK data protection framework to appoint a representative in the UK if they are processing UK data on a large scale.

"On Exit, the ICO will not be a supervisory authority for the purposes of the EU GDPR and so will not be an EDPB member."

## 2 PECR

An amendment by the Government to the Privacy and Electronic Communications Regulations that increased the maximum penalty for violations to half a million Pounds took effect on the 17th December 2018.

Whilst not GDPR, PECR is closely aligned and controls marketing communications - and now there is particular danger for Directors as the ICO (Information Commissioner's Office) has the power to find them personally accountable for violations. This applies even if their organisation goes into liquidation or they are no longer in a senior position at the company. This rule is intended to make it harder for those who breach the law to set up a new organisation and carry out similar non-compliant activities.

## 3 No Fear!

However, let us repeat the mantra that a properly structured organisation has nothing to fear, indeed the Information Commissioner Elizabeth Denham insists that the ICO's response measures are not geared to punishments. "The law is designed to push companies and public bodies to step up their ability to detect and deter breaches," she said. "What is foremost in regulators' minds is not to punish the organisations, but to make them better equipped to deal with security vulnerabilities."
"We understand that there will be attempts to breach organisations' systems, and that data breach reporting will not miraculously halt criminal activity. But the law will raise the level of security and privacy protections across the board."

## 4 Training Video

Whilst mentioning the ICO, they have an excellent training video for schools to be found here https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&query=data+protection+manager&profile=_default

## 5 All websites should be HTTPS

Apparently 20.9% of the top 100,000 websites still do not use web encryption at all. Please make sure you are not amongst them!

## 6 Data Care Act?

Do not hold your breath, but there is a movement within the US to pass an act of this name that will get closer to the principles of GDPR. However, we do not expect this particular Leopard to change its spots on data privacy any time soon.

## 7 New risk identified for Mac's - MAC.OSX.AMCleaner

Apparently this 'scareware' is primarily delivered by email to trick victims into installing fake cleaning software, and the report notes that "anyone who thinks Macs are invulnerable to malware are sadly deluded".

In one variation, the malware opens an HTML page that is stored in its contents. In another, it is a full application that shows false scan results. In both instances, the malware prompts victims to purchase a fake malware cleaning service.

Anyone who follows the link to buy the cleaner is taken to a malicious domain and prompted to download and install the bogus cleaning software. When the malicious installer is run, it is actually signed with a valid Apple-issued certificate. This valid certificate allows the malware to bypass macOS protections such as Gatekeeper, and helps trick the victim into thinking it is safe to run the software.

## 8 Prize for the worst PR following a breach?

This prize has to go to Ticketmaster who blamed a supplier (Inbenta), who then responded "Upon further investigation by both parties, it has been confirmed that the source of the data breach was a single piece of JavaScript code... Ticketmaster directly applied the script to its payments page, without notifying our team. Had we known that the customised script was being used this way, we would have advised against it."

A caution for us all there however, as it is routine for programs to seek to access data from other sources. We must check in future that there is no possibility of exfiltration, since if we just accept the code as Ticketmaster did, then it is you who will take the reputational hit.

## 9 Extortionists Lie!

Now there is a surprise. GlobeImposter ransomware victims have found themselves abandoned by their extortionists, so if you did not have a backup, you are well and truly in trouble. Those who were encrypted and tried to pay found that the recovery procedure did not work. Because backups can also be infected, Satswana advises that you take a monthly "Archive" copy of your data. If all is lost, you may have to recreate several days information, but at least you have most of your history.

## 10 Just how dangerous is data?

To prepare these reports Satswana spends considerable time reading up on every possible source, and we copied this without noting the writer, so with apologies to them for not acknowledging their copyright, it is nevertheless very thought provoking.

*"Until now, cybercrime was all about making money and stealing information (because information is money). Today however, we have the ability- from 30 feet away- to shut off someone's pacemaker. A malicious individual could walk down a street today, and shut-off bodily devices that are controlled by computer chips, murdering them. In a few years' time, they will be able to do this from thousands of miles away. A law enforcement agent today can stop a vehicle on the freeway providing they are within 35 feet of it, because the average vehicle has over 240 microprocessor-controlled components; you can shut it off, lock the doors, enable airbags…. In a few years' time, a malevolent individual may be able to do that from thousands of miles away, on mass. Today, we think of cybercrime as financial crime, but I fear it will become much darker, more of a terrorist tool, and much more harmful to our wellbeing."*

## 11 Prosecutions do take place

Notwithstanding our "no fear" message in item 3 above, the ICO have prosecuted and fined a former deputy head teacher for unlawfully obtaining personal data from two schools he had previously worked at. Darren Harrison was suspended from Isleworth Town Primary School only six months into his new role, having uploaded large volumes of sensitive personal data from Spelthorne Primary and The Russell School in Richmond to Isleworth Town Primary's server via a USB stick.

He was unable to provide a valid explanation for how the information had appeared on the server, and claimed it had been deleted. He later told the ICO that the data had been taken for professional reasons. Because he had no lawful reason to process the personal data, he was in breach of data protection legislation and was fined £700 under the Data Protection Act 1998 and ordered to pay £364.08 costs and a victim surcharge of £35.

Mike Shaw, the ICO's criminal investigation group manager, said: "The ICO will continue to take action against those who we find have abused their position of trust."

## 12 ICO determination regarding Public Health England

Satswana sought clarification on the position of Schools in the provision of data to the NHS. The decision is reproduced in full below.

3 January 2019

**Case Reference Number RFA0789669**

I write in relation to the concern you have raised about Public Health England (PHE).

**Our role**

We want to know how organisations are doing when they are handling your personal information.

If we think the organisation has not complied with their obligations under the data protection law we oversee we can give them advice and ask them to solve the problem. Our main aim is to improve the information rights practices of organisations, where there is an opportunity for us to do so.

Before reporting a concern to us, we expect you to give the organisation the opportunity to consider it first. In order for us to look at their information rights practices we need you to provide us with their reply.

**Your concerns**

I understand you are concerned about the lawful bases for processing of school children's personal data. You have explained that you are concerned about height and weight measurements, vaccinations and dental surveys and how information collected is shared with local authority providers such as the school nursing services.

**Our view**

You have raised your concerns with PHE and it appears they have provided you with a number of in depth responses.

Based on the responses you have received I am satisfied that the information you have been provided with does not suggest any concerns about PHE and their understanding of their obligations under the General Data Protection Regulation (GDPR).

PHE have advised that their lawful bases for processing information are:

- Article 6(1)(e)
- Article 9(2)(h)
- Article 9(2)(i)

Firstly, I feel I should emphasise that no single basis is "better" or more important than the others – the most appropriate basis to use will depend on your purpose for processing. As such consent is not always the most appropriate

basis for organisations. For further information on the lawful basis for processing please visit: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

I feel it is important that I reiterate advice provided to you by PHE that there is a difference between consent as a basis for processing under GDPR and parental consent for carrying out a medical procedure. As PHE have explained to you, they do ask parents to provide consent for a vaccination to be administered, however this is consent for a medical procedure and not for processing the data. They are relying on the articles listed above as their bases for lawful processing.

For further information you may wish to visit our website, specifically the information under the heading *"Do we need consent to process personal data for our patient care functions?"*: https://ico.org.uk/for-organisations/health/health-gdpr-faqs/

Furthermore PHE have explained that with regards to height and weight measurements, although consent is not the basis for processing this information, parents are given the opportunity to withdraw their children from the measurements. This is because although this is a nationally adopted scheme, parents have the option for their children's data to not be included in this collection. As such the basis for processing which they have provided appears to be sufficient.

Finally, PHE have advised that they have obligations under a variety of legislation in addition to the GDPR. They have requirements to fulfil under this additional legislation such as the NHS Act, which we do not regulate. I note that they provided you with appropriate links to this legislation as further guidance.

Therefore, as explained previously we do not have any concerns regarding the bases for processing information by PHE under the GDPR. I hope that this correspondence provides you with sufficient information and guidance. If you

have any further queries please do not hesitate to contact me.

## B Satswana February Update

1 **Risk to data access**

2 **Fake freedom of information request**

3 **Critical Data**

4 **Coping with challenging behaviour**

5 **Processor Agreements**

6 **Implementation**

7 **Digital Security Certificates**

### 1 Risk to data access

We hate project fear, preferring hope, or if that is too naïve, at least project "get on with it", but there is a possible scenario which we must alert you to, and that is in the event that we "crash out" on the 29th March, then data flows may be affected.

There is absolutely no excuse for it, since DPA 2018 is an exact 'equivalence' to GDPR 2018 (save for the ludicrous reduction in the consent age to 13 that surely must be considered again). But there is a sector of the bloated Brussels bureaucracy that will continue to seek every means to extract revenge for our temerity in disrupting their gravy train.

As ever, commerce, schools and councils will be collateral damage, it is the UK Government which will be the target. Much of the Governments online services are hosted by Amazon Web Service (AWS), located in the Republic of Ireland, where

Amazon legally (sic) contribute as little as they possibly can to society (though there is an option in Slough). It is claimed (source, The Times 4/2/19) "dozens of Government Departments are still holding personal data on EU computer networks. In the event of a no deal Brexit it will be illegal under European law from March 30th for that data to be transferred to the UK, potentially crippling government services."

Is that mean and nasty? Yes, and hopefully commercial interests will ensure that it is ignored, especially as the beneficiary would be servers in the United States which is holding out against the sort of data privacy regulation that GDPR can rightly be applauded for ushering in, so Europe would shoot itself in the foot, as they say.

But we cannot absolutely discount supreme stupidity, so what can be done? If your servers are on premise, then your only consideration is with the cloud services you may use, mainly processor agreements, but also services such as Microsoft 365 or Google Docs. Microsoft has a huge data centre in Wales, so if you are located there, no problems, but Google may well be in Ireland.

If all your services are "in the cloud", then you do need to establish exactly where the data is located.

Our expectation is that nothing adverse will happen on March 30th, but it does no harm to raise the intellectual question with your IT support as to how you would access data in the case of any event that disrupted it, with a "ransomware" attack probably having a higher probability than negative European activity.

To conclude, we really do regard GDPR as being good law, to the point that it is being adopted as an international standard, and we discourage any use of servers in the US that rely on "Privacy Shield" as very weak protection. Anything that impacts its adoption would be entirely counterproductive to the purpose behind the law, but unfortunately that requires a common sense approach, and we cannot take that for granted.

## 2 "Fake" Freedom of Information request

Many of our customers have been bombarded with an alleged FOI request that sought information on their energy usage. Initially we advised:-

"This is a circumstance where a Non-absolute exemption applies under S (2) 43, where a public interest test applies.

We can see no circumstance where disclosure of these matters of Commercial Interest would be of Public Interest when sought by an individual using a Gmail Address."

Having now seen many more, we are stronger in our rejection, advising that this is a sales approach and suggesting you delete it as otherwise you are confirming that the address exists by responding, then blacklist the sender. Every one we have seen has come from a different Gmail address, without providing a postal address, which is a requirement.

## 3 Critical Data

Have you got a securely archived note of all the critical user names and passwords that trusted staff use to access sites and information that are essential to your operation? It may be HMRC, VAT returns, bank access details, or even something like a Twitter account. The "knowledge" may be within the head of one person, as it was in the case of a Bitcoin exchange in New York. When the Founder died at the age of 30 millions of Dollars' worth of customer's assets became irretrievable because nobody else knew the access codes.

Of course, how you resolve having the information recoverable and yet keeping it secure is going to be an individual challenge but if it is essential to the organisation, you must find a way.

## 4 Coping with challenging behaviour

We are seeing all too often how schools are increasingly required to cope with behaviour that would normally require specialist support, but for which there is no budget. One possible contribution to a solution in certain cases may come from distraction in the form of the direct involvement of the child with a computer. In which case may we draw your attention to https://www.khanacademy.org/ where there is free educational content without the advertising that you find on YouTube.

It is a remarkable site that can be enjoyed by anybody with an enquiring mind who wishes to learn about a subject. A lesson in Quantum Mechanics anybody?

## 5 Processor Agreements

At the request of customers, and indeed with the support of many, Satswana are making a consolidated list of processors who have been checked out either directly by us or from information provided by a customer. We will be making this available in early April, but in the meantime would welcome any lists that you want to have confirmed as being compliant, and indeed information on any Processor that you can confirm you are happy with.

## 6 Implementation

Similarly we are learning alongside our customers about the challenges of actually implementing the changes in both procedures and practices that have flowed from an understanding of data risks triggered by GDPR. We expect to be able to share the output once available. One tip was that reviews should be fast and frequent, preferably held standing up, rather than having long formal meetings! Make of that what you will, but a serious subject will be the requirement to train staff to deploy new skills. Somebody who has spent all their life with a paper based administration system will need support to go digital.

## 7 Digital Security Certificates

A research organisation has advised that there has been a wave of large scale DNS (Domain Name Server, the device that turns an IP address into a name you can read like something.com) hijacking attacks affecting dozens of domains belonging to government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America, since 2017.

Since the origin was alleged to be Iran, it was even more embarrassing for the US that certificates could not be renewed during the recent shut down of their administration! Without the HTTPS security miscreants can intercept and redirect web traffic, and you do not want that happening to your tax return!

Make sure your web certificate is up to date.

## C Satswana March Update

1. **Ransomware**
2. **Drugs**
3. **FOI Responses**
4. **GDPR report to Governors**
5. **Accountability**

### 1 Ransomware (urgent action required)

As far as we are aware the many phishing attacks that we have dealt with over the last month only had an annoying and disruptive effect, with a requirement to change passwords. However we cannot be complacent as attackers appear to have used this method to penetrate the network of The Sir John Colfox Academy in Bridport, Dorset, encrypting all the GCSE coursework of Year 11 Students. (Source, The Times)

We are guessing that this will have been stored on an open drive that all students had some space on, but even so it should have been protected by the school firewall policy. The data is neither personal, nor sensitive, so it is not a GDPR issue, but clearly it is devastating for those about to take their exams – and of course they have

been asked for money to release the encryption. The immediate message must be that if the dark side have identified this as a target, then they will be looking to repeat their success. Thus immediate action should be taken as follows.

a) Review your network security for any shared drive that has multiple accesses to it. We recognise that it will be hard to defend with many points of compromise. Also, strongly reinforce the training message that you should question all emails containing content that you are asked to click on before doing so.
b) If you are attacked, contact us immediately. There are remedial sites that can unencrypt some of the ransomware that is used (not all sadly.)
c) Do NOT even consider paying. Of course we cannot enforce that, it is always your executive decision, but the raw fact is that payment does not ensure that your files are released; you cannot assume that the attacker even has the systems needed to manage a 'customer relationship', let alone that they are likely to be ethical! So you could lose your money, and remain encrypted.
d) Seek to rebuild the data from any other source. You may have to accept that it is totally lost.

Which brings us back to reminding you of our suggestion that you ARCHIVE data on a regular basis, preferably in a manner that keeps the drive off the network, you should also recommend that anybody that has exam data keeps a personal copy without relying on a shared drive.

We recognise that an archive is imperfect, it only has data up until the date it is taken, and anything subsequently added may be potentially lost. But at least it is not ALL lost.

## 2 Drugs

Can you tell Parents if you have uncertain evidence that they are involved in drugs, and what if they are over 18? A challenging question that had us looking beyond GDPR for the answer, which was found within the "Keeping Children Safe in

Education Act 2018", namely Clause 75. The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children. We have left on the highlight that our colleague with 30 years Police experience in safeguarding added for emphasis.

DfE guidance confirms that Schools still have a safeguarding responsibility for 19 year olds. You are recommended to advise Police on an intelligence basis, even if you intend to take no action as a School.

## 3 FOI responses

Our advice on anonymous Freedom of Information Act responses has been challenged by both lawyers advising Schools, and also County Authorities. With respect we think they have only responded to a solitary request, they have not seen the multiple use of obvious pseudonyms in one instance, and a totally unconfirmed identity on what proved to be a campaigning website in another. Thus they are advising on the letter of the law, not the spirit. Quite apart from the legitimate exemptions that you can consider (we advised one School to deploy the defence that it would cost too much to provide the information) may we please remind you that the University of Worcester decision provided a case law precedent that effectively reinterprets the law. If you can kindly discuss any requests with us we can consider whether it is appropriate to respond. We totally support transparency in information, but believe it is being misused and weaponised by certain parties.

## 4 GDPR Report to Governors

We note that Schools are being encouraged to provide an annual report to governors. We can help you with this by providing a template and also evidence of your performance.

### 5 Accountability

We are hearing this word more and more often in the context of GDPR. We are contacting all customers with a view to providing them with an Implementation plan, support check sheets and template conclusions to both promote and measure the adoption of "privacy by design and default to ensure you are "accountable".

## D April Technical Chat



### 1 Email Authentication

"Phishing" e-mails, those that persuade you to open an attachment that then infects your computer with a virus are one of the most prevalent sources of scams, and because "Simple Mail Transport Protocol" was designed in the 1970's – when security had scarcely been thought about – there is little protection. However, there are three add-ons that you can ask your provider for. Please do not worry what it stands for, but their initials are SPF, DKIM and DMARC, they are all involved with authenticating the address, the sender and the content – we have deployed them at Satswana. The result was that the other day the writer was unable to forward a mail that still contained a phishing infection. Initially annoyed – I realised how powerful the protection actually was. We recommend their adoption.

## 2 Dedicated connectivity

If you have a situation where you absolutely must deploy a secure network – and examples of a need for this can only grow, linking schools together in a Trust, linking business offices together, or secure links within a local authority – then you should be aware that this is not as costly as you might have originally thought. There is a longer brief attached at Appendix A provided by Concept Solutions People, based at The Pinnacle, 67 Albion Street, Leeds, LS1 5AA**T**: 08456 805 906 **M**: 07803 737321 **E**: richard.auld@conceptsolutionspeople.com Satswana has no financial interest in any transaction, but can recommend the management.

## 3 Apple cards

The news that Apple has launched a credit card is fascinating on a number of levels, but mostly as an example of change, fresh thinking, fabulous design and new approaches to security. Its relevance to the world of GDPR is that it demonstrates how business processes are being completely reworked in a manner that we will all benefit from.

We highlight just one aspect of this Apple development, in that "They do not need to invent new things, they only need to reinvent the experience"

Here you have a card, that is actually a phone, or alternatively you talk to Siri (or Alexa) etc. and you will instantly see the transaction, even if it is less than one cent.

You will get instant cash back to spend credited to your account immediately after any transaction

Of course you can have a card as well, but it will not have any numbers on it, it will be Titanium coloured, with just your name and a chip

Representing absolute elegance in design plus absolute privacy and wholly new features, the card is an utterly fascinating insight into the future.

## 4 What3words

Did you read that the Police found a car driver who had crashed out of sight of the road using https://what3words.com/ ? It is so much more precise than a post code when giving directions and the concept is that three words are much easier to remember than a string of numbers representing a location, as in a traditional grid reference for example. Is this worth adding to your Contact information?

## 5 Some current scams

The following information was taken from The Times dated 30/3/19, referencing original sources from UK Finance and Which, and added to by Satswana. "Being aware" is part of the defence.

a) Man in the middle attack

A fake email redirects a payment you are expecting to make (having monitored your email) into the wrong account

b) Investment Scams

Criminals persuade victims to move money into a fictitious investment fund with the lure of high returns.

c) Romance Ruse

A stranger on a dating site attracts a suitor, often male. The stranger pretends to need money for an emergency.

d) Advance Fee

Criminals promising good news persuade victims to pay to release a larger sum

e) Malicious redirection

Using fake emails conmen pose as tradesmen owed money to get payments to fake accounts

f) CEO Fraud

An apparent contact from an organisation CEO demands that an urgent payment be made

g) Impersonators

Tricksters pose as officials to convince victims to transfer money to halt fraud on their account

h) Brexit deception

A website posing as HMRC tells businesses to apply for a "UK Trader Number" in time for Brexit, (Aiming to harvest your data.)

## 6 Why does software underperform so often?

The essence of GDPR is change, and Satswana forecasts that we will all be adopting the sort of document collaboration techniques represented by either Microsoft 365 or

Google Cloud – all running on servers that are themselves embedded in an Internet that provides security, resilience and backup in a manner that we could never structure on an individual basis.

But what about all those "packages" we buy to support our activity, Payroll, accounts, HR, management information systems for example? Why are they not all connected?

They will be, one day, but only when we learn how to create major software packages.

What stops us? Bad management is the pure and simple answer, a total failure in every case of the managers of a project to understand and control it. Many have never coded anything themselves, and probably know very little about the subject they are seeking to automate. Some will be accountants, whose only interest will be to spend as little as possible, with no concept of testing, documentation, release planning etc., it must just all be contained within a certain cost, it guarantees failure.

For success, there are three simple rules. The first is that in order to automate something it must first work perfectly when managed, performed and executed by people, that is – it is a manually operable system. It is that which captures the flow, and it is essential to learn the tricks and traps from the operator.

The second is that one person must be able to understand the project from A to Z, sufficient to ensure that the automated system does exactly what the manual version did.

The third is that if you now wish to add other features to what is now a faster, slicker, less cumbersome process, then you have to do that by going back to the first two rules.

Think of it as a jigsaw puzzle. Of course you need the picture on the top of the box, and then it must all fit onto a table, and all the pieces must be cut accurately.

What has happened so often, with NHS software or anything else that you can think of, is that the jigsaw is the size of a warehouse, there is no picture of what it should look like, some parts of it are assembled in India and there is no standard shape for the pieces.

If you add to that a demand that it has to fit together with another jigsaw created 30 years ago, where everybody who made it retired long ago, and there is no picture of that either, then there can be no surprise that you will fail!

But it is changing, we are learning, and the Apple Card example in 3 above is an indication.

## 7 Windows 7

Yes, we know you love the look and feel, but it can be replicated in Windows 10 and Microsoft are now dedicated to updating that on a constant basis rather than producing a new release. So the fact that support for Windows 7 will cease on the 14th January 2020 means that if you are still running this, then you have to change, you really do!

**Appendix A**

# Dedicated Fibre Connectivity

With so much internet connectivity, MPLS Wide-Area Networks, and SDN, sometimes it's better to consider simple solutions for point-to-point and hub-and-spoke networks for shorter links (up to 45Km).

These services are simple, straightforward and secure.

DEDICATED FIBRE IS A CONTINUOUS STRAND OF FIBRE DIRECTLY LINKING YOUR TWO SITES, END-TO-END. NO ROUTERS, SWITCHES OR CONTENTION (SHARING OF BANDWIDTH).

## Benefits

**Secure** – only your equipment is attached at each end. Government CAS(T) approved.

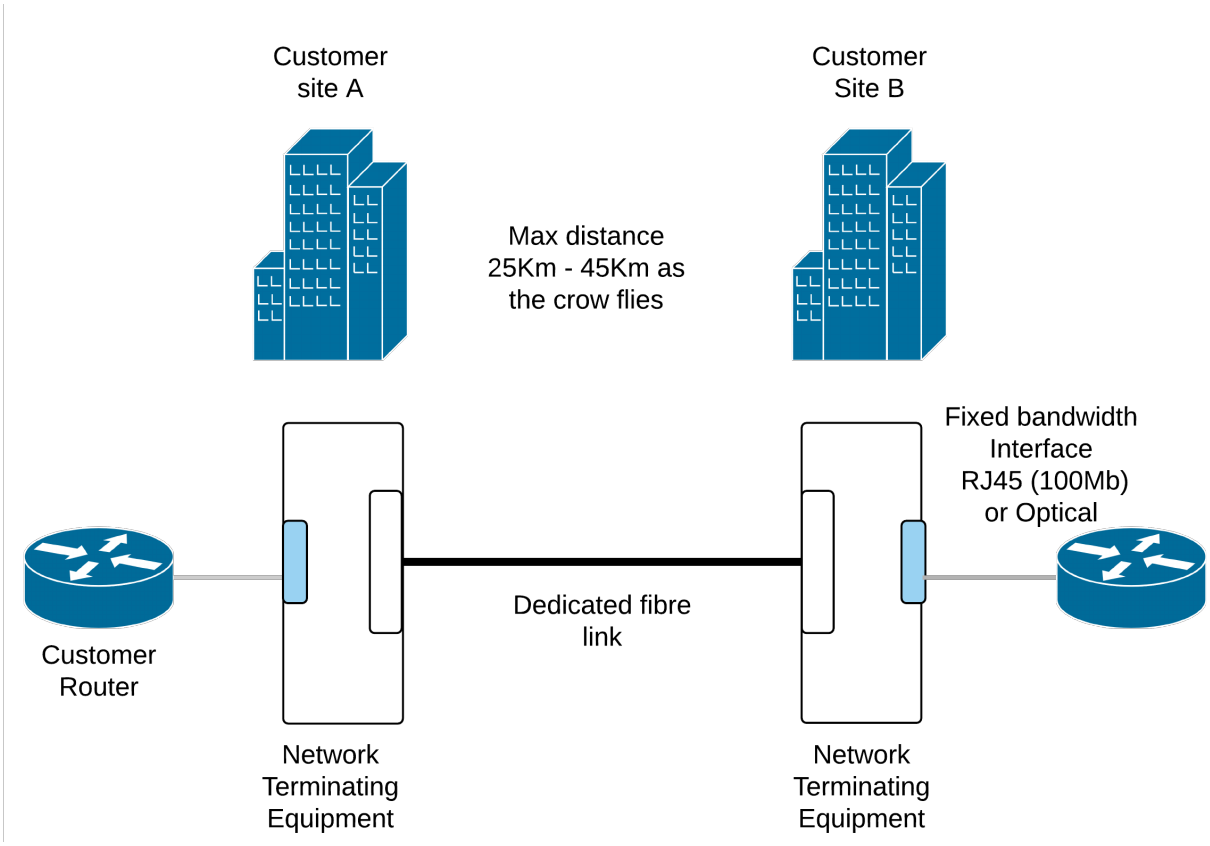
**Very Low latency** – At 230,000Km/sec light moves quickly in fibre and it's going straight to your other site.

**High Throughput** – If you select a bandwidth of 100Mbps, 1Gbps or 10Gbps that is what you will get. The only routers or switches are yours and there's no contention.

**Jumbo Frames** – 1Gbps and above services accommodate large frame sizes or "Jumbo Frames".

Options: 100Mbps, 1Gbps, 10Gbps Ethernet.




# How much will this cost?

Dedicated Fibre Connectivity prices are based on the distance between sites and on Openreach Exchange areas. Here are some examples, please ask for a firm quote.

**Two sites in the same Openreach Exchange area**

| Dedicated Fibre | | Monthly Rental | |
|---|---|---|---|
| **Bandwidth** | **Connection charge** | **12-month term** | **36-month term** |
| 100Mbps | £2,850 | £180 | £160 |
| 1Gbps | £2,850 | £210 | £190 |

| | | | |
|---|---|---|---|
| 10Gbps | £6,965 | £525 | £465 |

**Two sites in the same town, but in different Openreach Exchange areas.**

| Dedicated Fibre | | Monthly Rental | |
|---|---|---|---|
| **Bandwidth** | **Connection charge** | **12-month term** | **36-month term** |
| 100Mbps | £2,850 | £295 | £260 |
| 1Gbps | £2,850 | £325 | £290 |
| 10Gbps | £6,965 | £635 | £565 |

**FAQ**

| | |
|---|---|
| What's the lead-time to install? | 2-3 months |
| Can I have two separate circuits? | Yes, there is a resilient option with separate routes which requires a survey and design. Prices will be a bit higher than 2x the figures above. |
| What can I use these for? | Anything that runs over your LAN such as voice, video, data and any applications that can communicate over Ethernet. |



**Motto of the moment** "If you want tomorrow to be different, you must not do today what you did yesterday".

Just about sums up our change journey towards "privacy by design and default"!

## 1 CCTV

Parents are apparently demanding access to CCTV footage, notably in Nursery Schools.

Many opinions on it, but "Mumsnet" sensibly stated "it can have the effect of escalating dramas into crises" adding "given that identity would be blurred out…it doesn't add any useful information – unless you suspect nursery staff of safeguarding failures," the last point of course being very different from Johnnie bashing Jane.

But the ICO stick to the party line, "People have the right to see information held about them, including CCTV images", the key word here that you should take note of is "held".

Satswana submits that the mere operation of a camera does not amount to "holding" data unless there has been a reason to review an incident and a record kept on a separate medium. You may well have a legitimate reason for doing that, but unless you do so there is no "record". Of course that view may be subject to an alternative interpretation, but then they must make their case and only the determination of a precedent will establish who is "right".

CCTV can be a modern business blessing, but overly sensitive parents could make it a curse. We do recommend you make it clear in your policy that you only make a record of an incident if there has been a reason to review it. Otherwise all images are overwritten. Your decision on a retention period then becomes critical!

## 2 Duff Insurance

Zurich Insurance rejecting a claim for compensation after a cyber security attack as having been "an act of war by a foreign power" is a very troubling new evasive approach, by an industry notorious for their 'small print' when you have to claim.

Will they get away with it? Does State sponsored hacking amount to undeclared war by a foreign power? Probably Zurich can afford the enrichment of lawyers that will result from the defence, but no school could fight that. Your insurance costs are an exorbitant burden without finding that the cover is worthless.

Cyber-attacks are clearly criminal enterprises, and too much of it is supported by rogue countries, some of it aimed at destabilising an established view of society, but war? No, not any more so than the reality that there has always been propaganda – and peaceful efforts at disrupting competitors, whether that is business or a regime. Crime is as constant as evil is a reality.

So before you pay any premium for insurance cover in this area we suggest you challenge them on this point, and get any assurance in writing.

## 3 Update consolidation

To make room under our Resources tab the 2018 updates have been consolidated, indexed and edited to ensure they remain relevant. We appreciate that there is "much to read", but that only represents the rate, speed and sheer volume of

change that has been triggered by the necessity for society to totally review every approach to privacy that we had ever thought of. Some are arguing that proposed legislation is a restriction on free speech, but read 4 below and you will recognise that something had to be done.

## 4 Total privacy failure in the US

You will be aware that we do not trust any aspect of data from the United States (Satswana objection to EUUS Privacy Shield), but it took a speech by Mark Rotenberg who campaigns there as EPIC (Electronic Privacy and Information Centre) at the ICO 2019 conference to lay bare just how bad the landscape is in America.

As briefly as we can, the Federal Trade Commission (the alleged Regulator) obtained a consent order from Facebook in 2011 that looked very much like the requirements of GDPR, in that privacy would require specific consent, could be removed etc. You will be well aware how far Facebook have moved from that in 2019, and the FTC have received over 26,000 formal complaints, from organisations such as EPIC, but Mark pointed out that they are only just one.

So what action has the FTC taken against Facebook's clear breaches of all the undertakings in the consent order? Absolutely nothing, zero, nil, nada.

## 5 Surveillance Capitalism

If you should want to be totally terrified by the consequences of the burgeoning abuse of privacy, then "The Age of Surveillance Capitalism" by Shoshana Zuboff is a turgid and complex read. For those who do not, just reflection on the title probably describes the danger adequately.

## 6 Restatement of objectives

In her speech to the ICO 2019 conference, the Commissioner (Elizabeth Denham CBE) stressed the "accountability" aspect of GDPR/DPA (that may become even more focused if personal liability for offences becomes a feature of future legislation). She identified the growing distrust of social media, saying that we must increasingly question the control we have. (Including, in the education sector, questioning how any "free" service makes its money!)

We would all identify with her stating that by holding data we are creating risks for others that have to be mitigated by embedding processes that have a real and lasting impact. She concluded that "there is plenty that needs to be done, so let's get on and do it."

## 7 Further documentation

In "doing it" you should by now have received a copy of our "Implementation Plan" and supporting Strategy paper. (If you have not, please contact us immediately for a copy.) You will also have been copied with our April release of our qualified Processor list. We apologise for all the reading involved, but scheduled for release in early May is our Technology Review, aimed at a non-technical readership, not just for IT!

Please note that, whilst we are happy to share our update notices on a public forum (recognising that we are all learning from each other, so there is value in being open and transparent) these documents will not appear on our Resources tab, being exclusive to the customers who retain us as their DPO. Please kindly therefore if you are the recipient of the contact email, can you ensure that they are correctly distributed to all interested parties within your Trust or School? If your name should be added to the mailing list, then please request its addition by mailing admin@satswana.com

## 8 Meetings and questions

May we conclude by restating that we are always delighted to receive an invitation to visit you, for a quick update, introducing GDPR to new staff, or dealing with a problem that you might have, for whatever reason. Equally we continue to relish your questions. Great if we know the answer, but if we do not it gives us the impetus and opportunity to find one – and that helps us learn, thank you!

**F June Update**

**1 Funding opportunities from the D of E**

**2 Continuing Professional Development**

**3 Data Protection Toolkit for Schools (link)**

**4 National Cyber Security Centre (link)**

**5 Registry Scam**

**6 Data Protection Qualifications?**

**7 Chicken Pox (Consent request)**

## 1 Funding opportunities from the D of E

Three important announcements that all Schools should be looking into, with the first being that the Department of Digital, Culture, Media and Sport is working with the D of E to identify schools where they will accelerate funding of full fibre connectivity over the next two years. Everybody should be applying for this, since if you have a proper fibre connection (as opposed to the 'last mile' being over copper) you have essentially unlimited speed broadband, and that is going to be desirable as we move ever further into cloud based provision. A guidance area to be found here https://www.gov.uk/government/publications/choosing-the-right-broadband-for-your-school/broadband-for-schools-introductory-guide-for-senior-leaders

Secondly the D of E are proposing a national retraining scheme to help "adults whose employment is at risk of automation, to upskill or retrain staff". Is that an additional teaching opportunity, or can it be also embraced to retrain

teaching staff who are moving from paper based systems to digital automation?

Finally they are talking about an “Edtech” leadership group seeking testbed organisations to assess various challenges, including “exploring the needs of teachers in accessing quality curriculum materials”. Satswana believes that this drive is exactly in line with the Implementation plan we have published, and associated Strategy papers and Technology review. Could you become a testbed?

## 2 **Continuing Professional Development (CPD)**

As you will know Satswana perceives it to be a benefit of GDPR/DPA that it provides an opportunity for change as we drive for “privacy by design and default”. We also suggest that there is a “return on investment” from that exercise. Thus it is helpful to find the D of E publishing the following “challenges” defining how this may be obtained.

Please embrace this as additional support within your adoption of the Implementation plan and strategy.

a) Administration

Challenge 1 **–** improve parental engagement and communication, whilst cutting related teacher workload by up to five hours per term

Challenge 2 **–** show how technology can facilitate part-time and flexible working patterns in schools, including through the use of time-tabling tools

b) Assessment

Challenge 3 – cut teacher time spent preparing, marking and analysing in-class assessments and homework by two hours per week or more

Challenge 4 – show that technology can reduce teacher time spent on essay marking for mock GCSE exams by at least 20 percent

Challenge 5 – identify how anti-cheating software can be developed and improved to tackle the problem of essay mills (the process of academic fraud, i.e. procuring a third party to write a piece of work on a pupil's behalf)

c) Teaching practices

Challenge 6 – challenge the research community to identify the best technology proven to help level the playing field for learners with SEND

d) CPD

Challenge 7 – demonstrate how technology can support schools and teachers to identify their development needs and support more flexible CPD

e) Learning throughout life

Challenge 8 – prove that the use of home learning early year's apps contributes to improved literacy and communications skills for disadvantaged children

Challenge 9 – widen accessibility and improve delivery of online basic skills training for adults

Challenge 10 – demonstrate how artificial intelligence can support the effective delivery of online learning and training for adults

## 3 Data Protection Toolkit for Schools

Naturally we both support and align ourselves with the advice received from the D of E, so to remind customers that you can find a comprehensive toolkit supporting GDPR here https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

## 4 National Cyber Security Centre

Similarly we take great note of advice from the National Cyber Security Centre and for those wishing to review this further please start here https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

## 5 Registry scam

We advise you to ignore any emails received alleging that a Domain Registry, normally but not exclusively Chinese, is telling you that someone else is trying to register your name with a foreign extension; they are simply seeking to sell you a subscription to that name. Unless you are planning to open a school in China (or wherever) it will be useless to you, as it would be to anybody else!

## 6 Data protection qualifications?

We note an increasing desperation from GDPR providers who tend to operate principally "online" in the sale of support material and training. We are sympathetic, since once the legal requirement to appoint a DPO was satisfied last year – and you all adopted change following your Impact Assessments – the intensity has gone out of the issue, only raising its profile if you have a problem. Satswana is striving to maintain its relevance through implementation support and discussing improved capability with MIS providers, totally in synch with the "Edtech" objectives in 2 above, thus we respect that others will do the same. Are we therefore being unfair in doubting the value of expensive courses that provide illusory "certification"? We suggest that the links provided in this update, together with documentation we have supplied, will give you all you need so, as ever, Caveat Emptor!

## 7 Chicken Pox

Finally we are constantly impressed by the pure excellence in administration that is developed by our customers, and a recent example was the beautifully constructed and sympathetically expressed document that a school sent to parents requesting information on vaccinations and infections. It was designed to protect young teachers who might be pregnant and met the GDPR requirements of consent in any event, but equally was a perfect example of the "Duty of Care" in action. We would be happy to both share the content and acknowledge the author if it is of interest to other schools.

## G Urgent Technology Review Update

It has come to our attention that certain IT support organisations have been suggesting that customers need to change their server because of a "Spring Update" from Microsoft.

In very rare cases that may be true, but there are many other options to consider before you spend money on new hardware.

It is a fact that Microsoft are discontinuing support for Windows Server 2008 in January 2020, and for those who wish to "read all about it" it is very responsibly documented here https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Further, they supply a guide here https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-migration-guide-for-windows-server/Azure_Migration_Guide_for_Windows_Server.pdf which is a pitch for Cloud based Azure, which is one of your options, and indeed we do anticipate that many processes will be moving to the "Cloud" as bandwidth speeds improve, to take account of the greater security, resilience and back up options that apply there.

For those who wish to continue to maintain their server "on premise" you can choose to upgrade to Windows Server 2012, or 2016 – and we would expect most existing hardware to continue to run those operating systems.

For those Schools running SIMS MIS you therefore have the option to continue with an on premise server – but upgraded operating system, or use their Cloud service for the current Release 7, or wait for the release of the "pure cloud" software of SIMS 8. It is our current understanding that the D of E has mandated that Schools should re-tender rather than simply "upgrade" to SIMS 8 so (as per our technology review) you will also have the option of considering the Cloud provisioned products of alternative MIS suppliers. We are seeking to organise either a road show or a conference for you to be able to examine the competing benefits in September.

Please note that we are also forecasting a change within the distribution system of software providers. In the past some schools have sourced systems from what was originally a centrally negotiated Local Authority contract, or a grid for learning provider, or indeed a Distributor such as Groupcall. You may wish to continue that arrangement, but we think it more likely that the best pricing will come from a direct association with the supplier, and you will then also get a direct line of support.

And indeed your local support function will change markedly. The on premise local management will largely disappear (though you may still have a local network [printers etc.] and of course WiFi) but be replaced with an IT requirement to manage the permissioning of document collaboration files (One Drive or Sharepoint) and the crucial control of managed file deletion according to emerging policies. Similarly as Office 365 becomes the network of choice, so the complexity of local device management will decline.

So we exist in a time of change, dictated by the requirement to demonstrate "privacy by design and default" as a guiding principle of GDPR. Thus we submit that the last thing you need to be pressured into doing, is investing in last year's technology – that is anyway not before you have considered all the options!

## H Update Notice Summer 2019



### 1 IRMS Schools Toolkit

We are pleased to advise that this essential update is now available here https://irms.org.uk/page/SchoolsToolkit

## 2 The Kids Code

Not actual law yet, but in consultation headed by the Information Commissioner Elizabeth Denham, the "Age Appropriate Design Code" (Kids Code for short) will give children special rights in the law. Summarised as being "the best interest of a child should be a primary consideration" and tech firms will have to make their services "suitable by default".

The 16 items in the code are as follows:-

I. The Childs best interests should be the primary consideration in any services likely to be accessed by a child
II. Age Appropriate standards must apply to all users. Robust age verification mechanisms must distinguish children from adults
III. Privacy information and other terms must be in clear language suitable to the age of the child
IV. Do not use Children's personal data in ways that have been shown to be detrimental to their wellbeing
V. Uphold your own published terms, policies and community standards
VI. Settings must be "high privacy" by default, unless you can demonstrate a compelling reason for a different setting
VII. Collect only the minimum amount of personal data you need to provide the service in which a child is actively and knowingly engaged
VIII. Do not disclose children's data unless you can demonstrate a compelling reason to do so
IX. Switch geolocation options off by default and provide an obvious sign for children when location tracking is active
X. If you provide parental controls, give the child age appropriate information about this, and provide an obvious sign when they are being monitored
XI. Switch options that allow profiling off by default. Only allow them if you have measures in place to protect the child from any harmful effects, in particular content that is detrimental to their health or wellbeing
XII. Do not use nudge techniques to encourage children to provide unnecessary personal data, weaken their privacy protections, or extend use
XIII. Ensure any connected toy or device complies with this code

XIV. Provide tools for children to exercise their data protection rights and report concerns
XV. Undertake data protection impact assessments
XVI. Ensure that your policies proceedings and terms comply with this code

Many readers may be appalled to realise the tricks that have been deployed that this Code moves against, and note the power of Item 11 (XI!) Brilliant drafting to reduce it to 16 points, it will change the Internet for good, in both senses.

## 3 DPA 2018

We thought that it might be helpful to provide you with an index to the DPA 2018 and will publish it as a separate "Resource" subject, but in the meantime please be advised that the full content can be found here
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

## 4 Technology Review Update

Published separately, but important enough to repeat again

It has come to our attention that certain IT support organisations have been suggesting that customers need to change their server because of a "Spring Update" from Microsoft.

In very rare cases that may be true, but there are many other options to consider before you spend money on new hardware.

It is a fact that Microsoft are discontinuing support for Windows Server 2008 in January 2020, and for those who wish to "read all about it" it is very responsibly documented here https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Further, they supply a guide here https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-migration-guide-for-windows-server/Azure_Migration_Guide_for_Windows_Server.pdf which is a pitch for Cloud based Azure, which is one of your options, and indeed we do anticipate that many processes will be moving to the "Cloud" as bandwidth speeds improve, to take account of the greater security, resilience and back up options that apply there.

For those who wish to continue to maintain their server "on premise" you can choose to upgrade to Windows Server 2012, or 2016 – and we would expect most existing hardware to continue to run those operating systems.

For those Schools running SIMS MIS you therefore have the option to continue with an on premise server – but upgraded operating system, or use their Cloud service for the current Release 7, or wait for the release of the "pure cloud" software of SIMS 8. It is our current understanding that the D of E has mandated that Schools should re-tender rather than simply "upgrade" to SIMS 8 so (as per our technology review) you will also have the option of considering the Cloud provisioned products of alternative MIS suppliers. We are seeking to organise either a road show or a conference for you to be able to examine the competing benefits in September.

Please note that we are also forecasting a change within the distribution system of software providers. In the past some schools have sourced systems from what was originally a centrally negotiated Local Authority contract, or a grid for learning provider, or indeed a Distributor such as Groupcall. You may wish to continue that arrangement, but we think it more likely that the best pricing will come from a direct association with the supplier, and you will then also get a direct line of support.

And indeed your local support function will change markedly. The on premise local management will largely disappear (though you may still have a local network [printers etc.] and of course WiFi) but be replaced with an IT requirement to manage the permissioning of document collaboration files (One Drive or Sharepoint) and the crucial control of managed file deletion according to emerging policies. Similarly as

Office 365 becomes the network of choice, so the complexity of local device management will decline.

So we exist in a time of change, dictated by the requirement to demonstrate "privacy by design and default" as a guiding principle of GDPR. Thus we submit that the last thing you need to be pressured into doing, is investing in last year's technology – that is anyway not before you have considered all the options!

## 5 Advice on recording meetings

We have had several requests recently for advice on this subject, please find an answer below.

Considerable work has been done on this subject by the Transparency Project, with their website to be found here

http://www.transparencyproject.org.uk/guidance-on-parents-recording-meetings-with-social-workers/

and a guidance PDF here

http://www.transparencyproject.org.uk/press/wp-content/uploads/Whymightparentswanttorecordmeetingsv3mar18.pdf

It refers to social workers, but we feel the parallel with Teachers makes the guidance totally relevant.

Essentially, you might feel uncomfortable about being recorded but, as the above note makes clear, you cannot rely upon the Data Protection Act or RIPA as a reason to refuse permission to a parent to record meetings. There is no law that says the consent

of the Local Authority is required before a parent can record meetings they are participating in.

If a School wishes to make a recording, then they must seek consent to do so, since they will be doing that in their role as a Data Controller.

It is not illegal for a Parent to make a covert recording, but it may then be inadmissible in evidence, or not be accepted in quality terms.

Our recommendation would be to agree to a recording and ask for a copy – or take your own recording at the same time. You may wish to seek their agreement that it is not published online, but that is unenforceable in practise, since they could equally post a narrative account.

## 6 Childhood Illness Letter

As with 5 above we learn from you regarding your requirements. This letter was written by Louise Mellor of Cranmere Primary School on the instructions of the Head, Mrs Kathie Daniels and we felt that its purpose was excellent and that it sought information in a manner totally appropriate to GDPR. We mentioned it in an earlier note and received many requests for a copy. We are delighted to say that we have been given permission to reproduce it here.

June 2019

Dear Families

**Childhood illnesses update – and a request for information**

You may be aware that we have a number of staff in school who are pregnant at the moment and, during a recent review, we found that we need to update our records about childhood illnesses and vaccinations for pupils in order to be able to properly assess any risks.

At the moment we do not routinely hold information about whether any of our pupils have had the MMR (measles, mumps and rubella) vaccination and / or whether they have had chicken pox. Therefore in order to protect any pregnant women who work or volunteer in our school we need to be clear about the risks of them coming into contact with the pupils.

The NHS advises pregnant women about the risk of contracting chicken pox during pregnancy and also the risk of contracting measles or rubella. Luckily the risk of catching these diseases and the risk of either illness causing complications is extremely low in most cases. However, whilst most members of staff and volunteers will have either had these illnesses or been vaccinated against them, some have not, and if contracted during pregnancy there is a small risk of the consequences being quite serious for both the mother and, potentially, the unborn baby.

Therefore, we would like to ask all our families to complete the reply slip (overleaf) and return it to the school office by: (date). Rest assured that there will be no consequences to your child if they have not had either the vaccination or the illness, all this will mean is that should a member of staff or volunteer advise us that they are pregnant then we may need to re-consider the staffing arrangements of that class or group. The pupil will not be moved out of their class and they will not be identified to any adults who are not directly involved in their care.

If you decline to answer these questions and / or you do not return your reply slip then we will have to assume that your child has not had these vaccinations or illnesses. We will update our records if you tell us during the year that your child has either contracted one of these illnesses, or been vaccinated against it. We would be grateful if you could keep us informed if this is the case. Although you do have the right to decline to answer please do consider this very carefully. We are not collecting this information in response to any recent media coverage about the MMR vaccination; it is purely to enable us to protect our staff and other volunteers or visitors to school.

The information will be kept confidential and added to our pupil database. It will be held on our system for as long as our retention policy allows (for pupil records this is normally until your child leaves our school, then the records are transferred over to the new school).

Thank you very much for your assistance with this process, please be assured that we would not be asking for this additional information if we didn't consider it to be extremely important.

The reply slip is on the reverse of this letter.

Yours faithfully

_____ Please return this slip to the school office by (Date)

_____

Child's name : _____ Child's class :

_____

**Please indicate if the statement applies to your child by ticking the relevant box:**

| | **Yes:** | **No:** |
|---|---|---|
| My child has been vaccinated against MMR (measles, mumps and rubella): | ☐ | ☐ |
| My child has had chickenpox: | ☐ | ☐ |
| I decline to answer (in which case we will assume your child has not had the vaccination or the illness): | | ☐ |

Parent / Guardian's name : _____ Date :

_____

Thank you very much for your help.

**Privacy Notice:**

The information you provide will be used for the purposes of providing appropriate pastoral care. We are committed to protecting your information and will handle it in line with the Data Protection Act 2018. For further information about how we will handle personal information and your rights please visit our website at: (Address)

Essentially, you might feel uncomfortable about being recorded but, as the above note makes clear, you cannot rely upon the Data Protection Act or RIPA as a reason to refuse permission to a parent

7 Offsite activity generic consent form

Similarly Lucy Owen Of Esher High Schools sought a generic consent form to cover all their school trips. This version was also approved for use by the County Council

**OFF-SITE ACTIVITY MEDICAL AND CONSENT FORM**

Name: _____ Tutor Group: _____

Date of Birth: _____

Please sign and date the form below if you are happy for your son/daughter:

a) To take part in school trips and other activities that take place off school premises; and
b) To be given first aid (including a mild painkiller) or urgent medical treatment during any school trip or activity.

**Please note the following important information before signing this form:-**

- The trips and activities covered by this consent include:
  - ❖ All visits which take place during term time in and out of school hours
  - ❖ All visits (including residential trips) which take place during the holidays or a weekend
  - ❖ Adventure activities at any time
  - ❖ Off-site sporting fixtures during and outside the school day (including consent for your son/daughter to travel to fixtures either on the school minibus, staff car or parent car)

- The trip leader will send you information about each trip or activity before it takes place.
- You can, if you wish, tell the trip leader that you do not want your son/daughter to take part in any particular school trip or activity.

Written parental consent will not be requested from you for the majority of off-site activities offered by the school, for example, year group visits to local amenities, as such activities are part of the school's curriculum and usually take place during the normal school day.

**I understand that the teachers responsible during the off-site activities will be acting in loco parentis.**

_____

Please complete the medical information and dietary requirement sections below (if applicable) and sign and date this form if you agree to the above.

**MEDICAL INFORMATION**

Details of any medical condition and/or allergy that your son/daughter suffers from and **any medication** they should take during off-site visits:

……
……
……
……

**DIETARY REQUIREMENTS**

……
……

**Signed**_____ (Parent/Guardian) **Date** _____

8 In conclusion

We hope this update assists you in your work, thank you for the contributions that you make, which we can then share, we will provide a further update in September, have a great summer holiday.

**I September Update**

**1 Technology**
**2 Data Retention**
**3 Ransomware**
**4 Brexit**
**5 SAR consent**
**6 European Representative**
**7 Schools and Academies Show**
**8 Subject Access Requests**

**1 Technology**

It all seemed so straightforward, as per our strategic review the future was cloud based – with a more capable MIS supported by the collaboration tools facilitated by Microsoft 365.

Furthermore, the possible server costs to upgrade Windows Server 2008 once it ceases to be supported could be mitigated by moving data to the Cloud.

Then the German federal state of Hessen, supported by similar conclusions from the Swedish and Dutch Governments cried foul, stating that US cloud solutions are not GDPR compliant. That is regardless of whether or not the servers are European based, affecting Microsoft, Google and Apple. (Microsoft pulled out of a previous data trustee arrangement).

And it is not an easy issue to fix, having three elements – perhaps the most important of which is that the US authorities do not have the resources (or perhaps the will) to either define or regulate the abuse of privacy. (It is alleged that the Privacy and Civil Liberties Oversight Board only found out what was going on as a consequence of the Snowden revelations.) There is a great deal of evidence that other US authorities have a great deal of access to the data managed by US companies, regardless of where it is hosted, actually along exactly the same lines as objections are raised to Huawei. "Statements confirm that several intelligence operations affecting EU citizens have been ongoing". Finally there is a great deal of automated telemetry within (for instance) Microsoft 365 that is not adequately defined or understood. Some suggest this feature can be turned off, but it is on by default, so dangerous, perhaps?

We do not really know, which makes everything worse, but it gives us cause to pause for thought, as the French expression goes, 'Plus ca change, plus c'est la meme chose'.

Paradoxically that is going to delight huge numbers of our customers who are very happy with their on premise SIMS, together with having their data on their PC!

Satswana are continuing to research options on your behalf, but that is going to take time – there is a German product called Nextcloud that has been widely adopted in Europe, including all Swiss schools that may be the answer to document collaboration.

In the meantime we suggest that you do not change any of your current plans. If you are already upgrading, no current reason to stop. Windows Server 2008 does cease support in January, but we suggest you challenge any suggestion that you therefore need a new server. You do not have to switch to Windows Server 2019 (The 2012 version will be supported for a few more years for instance), and certainly you do not have to migrate to Azure (as promoted by Microsoft.) It is possible that some very old servers might benefit from replacement, but make sure you get a second opinion please. (Most schools will know of an IT competent parent or supporter who can check on a 'hard sell'.)

For the rest, if it is not broken, do not fix it, further advice will emerge.

## 2 Data Retention

Following the issue of IRMS 2019 Schools policy we provide a precis and a draft of a Records Management Policy taken from that document here
https://www.satswana.com/resource/RecordsRetentionSchedule.pdf

## 3 Ransomware

To note that US schools and colleges have come under attack over the last six months. May we stress again our suggestion that you take an "archive" copy from time to time that (however out of date) would give you some history to go back to if you are attacked?

## 4 Brexit

With apologies for using that word, but we covered a possible risk to data access in Item 1 of our February update here
https://www.satswana.com/resource/SatswanaFebruaryUpdate.pdf

That was pending March, with October pending now perhaps it is worth a read again?

## 5 SAR consent

In an interesting exercise a guy (with his fiancées consent) sent out a Subject Access Request asking for the information held on her. 40% responded without question. The good news really is that 60% did not, but we should all be aware that only the actual person concerned can give consent, and you must receive that directly. We

suggest that is very applicable to the manner in which the Police are currently automatically generating requests whenever anybody is involved in a case, regardless of its relevance (paranoia that there "might be something"). It often contains an "authorisation" from the person, but we say you cannot accept that from a third party, even the Police. Our experience is that a refusal to supply unless a very specific aspect of data can be defined is normally not followed up.

## 6 European Representative

We will avoid using the word in 4 above again, but there may be circumstances where elements of your data holding for European children will require you to have a continuing representative in Europe, in which case Satswana can provide that at no extra charge. (In the town of Aubusson for students of Tapestry!)

## 7 Schools and Academies Show

Satswana will be present at this show on the 13th and 14th November in Birmingham and we would love to meet up there with anybody who plans to go. We attended the London show as visitors and found it very helpful to be able to review the offerings of so many organisations under one roof, and will build on that in November.

## 8 Subject Access Requests

Noting the Ofsted commentary regarding rogue parents making life a misery with emails, Satswana (in conjunction with a number of other DPO providers) sent a submission to the ICO stating that SAR's were similarly unacceptable "weapons" in the hands of a certain category of bully or opportunist – seeking revisions to the law.

We interpreted their response as being very sympathetic, but they are law enforcers, not law changers. Having said that we have found increasing ways of using exemptions and other techniques to lessen the burden (and sometimes significant

stress) on staff, often through determinations provided by the ICO to the classic "I know my rights" merchants who submit a complaint.

Fact is that they actually do not know the state of current case law and precedent, and as a consequence their complaint has always failed. Thus if you get one, please call us in, that is what we are here for. In recent times we have been able to take the load off staff completely by acting as a peripatetic member (which is of course what we are) and take pleasure in doing so.

## J Satswana October Update

1. **Are the right people receiving our update information?**
2. **Serious data flaw in CTF**
3. **Deleting data when a Student leaves/ keeping School records**
4. **The School and Nursery Milk Alliance, FOI**
5. **DfE Brexit guidance and your free European Rep**
6. **Additional requirement for your School website?**
7. **Do's and Do not**

### 1 Are the right people receiving our update information?

May we please request that you let us know whether other staff within your School would benefit from receiving these emails? Please advise us at admin@satswana.com of any additional addresses we should be sending data to.

### 2 Serious data flaw in CTF

We are concerned to note that when data is transferred to a new school using CTF there is a circumstance where the software tries to de-duplicate an entry by amalgamating it. This is not safe as it stands, since there have been instances where data was shared regarding totally unconnected persons, and (worse) a record was connected where one party was excluded from parental contact. One "fix" would be to require authentication of the change before it is published, but pending

something of that sort becoming available, we recommend you double check any transfer that could be compromised if amalgamated.

### 3 Deleting data when a Student leaves?

It seemed to be such a simple question "this query relates to our students who have left and how long we should keep their digital information on file."

Then the full horror of the potential challenge emerged.

Once upon a time we did not concern ourselves overly with deletion, we were happy to keep data (especially paper records) and if we were able to find a past students exam paper from the loft dated 1954 we did!! In some senses that was a much softer, more generous culture that we regret passing. But criminal activity has forced a rethink, so we must now create barriers where they did not exist before.

There were two areas of concern, one was where pupils had a school email address, with all its related history, the second was all their notes, documents, exam elements etc., that were stored on the students drive.

One approach was the suggestion that the schools should ensure that leaving students are told that THEIR data is THEIR responsibility, and that they must ensure it is copied to their own archive media, and to be clear that the School will not be accepting any liability for data that is lost if they do not do so.

In practice you might decide to archive off an entire years data onto a removable drive and then store it off net, "just in case", but then entirely forget about it, since you do not want to find that you are being forced to declare data by a future FOI or SAR. The data should be clearly "inaccessible" – except in extremis, for a very special exception – and what that might be would be a matter for the School to decide.

The issue of school email addresses is similarly interesting intellectually, especially since if you do not have them, you lose a specific point of contact with that person. Of course you can just decide that the access to your email server ceases when they leave, that is the clean break that is simplest to manage.

We wonder however whether there is merit in forcing them to put a "forward" on their School address, to a new address? One benefit might be that you acquire their new address! You would then be in a position to control a "switch off" that might be

less traumatic for them. It represents a workload for IT that may not be welcome but we have to accept that there is an entirely new liability for managing data that did not exist before, and these questions are all a part of that.

As to what data has to be kept, that is a very interesting question that has had us searching for answers. One source we found was https://www.haringey.gov.uk/children-and-families/schools-and-education/projects-consultations-and-inspections/school-records-individual-pupil and you will find there the following:-

We are often asked by schools how long certain records should be retained by them before they can be disposed of.

It is important to remember that many school records are of invaluable help, not only for former pupils but also for local historical and genealogical research.

There should be a presumption against destroying any records unless it is considered that they are of no such value.

The following guidance is by no means exhaustive but covers the items most frequently asked about.

- **School log:** school logs should be retained permanently. They are retained in the school for 6 years from the date of the last entry; then transferred to the archives.
- **Admission registers:** admission registers should be retained permanently - note that this is not the same as the class register in which daily attendance is marked. These are retained in the school for six years from the date of the last entry, then transferred to the archives.
- **Pupil record cards or printouts:**
    - Primary - these are retained while the child is in the school; then transferred to the relevant secondary school.
    - Secondary - these are retained until the child is 25 years old and then shredded.
- **Class registers:** class registers are retained whilst the pupils are still at school and for three years after the last date in the register; then destroyed. For example, if a pupil enters school in September 2001 and leaves in July 2008,

the September 2001 register for that class can only be destroyed in August 2011.

So the question Satswana asked ourselves is "does this represent the information you have to keep"? We have worked with the IRMS 2019 advice and have produced a precis of what otherwise is long and convoluted.

Where have we got to? Hopefully a bit further forward and in any event recognising that this is a serious and complex issue that needs addressing. We have some suggested answers, all of which can be subject to your own decision making, and therefore ongoing policy.

We unashamedly benefit from this sort of discussion with our customers, and seek then to share the knowledge in any event!

## 4 The School and Nursery Milk Alliance FOI

You may have received an FOI request from the above organisation

We understand from other correspondence that their objective is one that you could probably support, namely to "Engage with schools outside of the project to ensure everyone in an education setting environment knows about the benefits of milk, their obligation to provide milk to their pupils, and how best to do so."

They do not say this in their request, which is a pity as it appears hostile, whereas their objective appears to be very different. Many Schools apparently responded by asking for advice, and that seems to be acceptable, so we recommend a positive attitude to this one!

## 5 DfE Brexit guidance and your free European Rep

Sorry to bring this up, but this is the guidance from the DfE…

If the UK leaves the EU without a deal, the UK will not have in place an Adequacy Agreement for processing personal data and will be classed as a third party under GDPR. There is therefore a chance that a narrow interpretation of the provisions in GDPR could lead to a regulator in an EU country restricting the transfers of UK personal data in the EEA.

It is important, therefore, that schools review their current data protection contracts and policies before 31 October, as they will need to ensure that they have the correct Standard Contractual Clauses (SCC) or other Alternative Transfer Mechanisms to continue to legally receive and process personal data from the EEA. If schools do not complete this action, they may be unable to access personal date stored in the EEA that they require to operate and may find that organisational partners restrict relationships due to regulatory concerns.

For more information please see the Department's guidance, at:

https://www.gov.uk/guidance/eu-exit-guide-data-protection-for-education-providers

The principal issue is that you must have a legal representative in a European Country, so we would advise Satswana customers that we have an office in Aubusson (famous for its tapestry) for that purpose.

## 6 Additional requirement for your School website

This was the somewhat concerning information sent to Birmingham Schools by their Local Authority, as if you did not have enough to deal with, here was something else.

The claim was that "you need to publish a 'Publication Information Scheme'. A model version, which just needs a few tweaks, can be found at the following link: https://ico.org.uk/media/for-organisations/documents/1153/model-publication-scheme.pdf

So is that so? After a degree of research, and most valuable input from discussion with other DPO's, we came up with the answer that might be summarised as being a "yes" or "no", and it must be your decision as to which way you go.

The case for yes is that State maintained Schools are classified as a Public Authority, and one DPO made the case that you publish as much as you can and use the publication notice in an attempt to minimise FOI and queries.

But as a preface for a case for "no" they included the qualification that there should be balance and you should not over commit provision beyond what is available, so

just to direct people to the report and accounts, annual statements and generic exam results, not least on the basis that you will get FOI requests anyway.

Good points which lead Satswana to recommending that you do not publish, at least not while it is not a statutory requirement. We note the ICO say only that you "may" publish, not that you "must", and believe that the overhead for a School in managing this – as compared with answering the very few FOI's that you are likely to get anyway, is a reason to hold back.

The ICO document actually might be interpreted as implying that, this is how they conclude:-

*"Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act."*

## 7 Do's and do not!

Finally a customer asked us for a check list that can be used as an update prompt with Staff. Can you improve on these for us?!

1. Do Encrypt all PC's, mobiles and USB devices – avoid the latter if possible
2. Do ensure you have Consent where required
3. Do be careful of what you write in an e-mail - as the contents may be revealed if it becomes the subject of a SAR or FOI
4. Do understand the lawful basis for processing data and ensure others do too (The 6 Principles) and ensure that 'Opt In' is practised
5. Do delete all unnecessary data - without destroying your history – and know your retention schedules

Don'ts

1. Don't leave any PC or phone unlocked or paper data insecure
2. Don't share data unless it is necessary and beware of CC/BCC
3. Don't attempt to cover up or delete information if there is a breach
4. Don't use your personal lap top, USB or e-mail address – keep it business like
5. Don't respond to SAR and FOI without seeking advice

But remember – Safeguarding trumps GDPR

## K Final update for 2019

**Contents**



### 1 The role of the Head

Where Satswana come in to support customers with a Subject Access Request, or similar situation, we are often engaged following a (much appreciated, thank you) recommendation from another School – and find that they have been struggling alone for too long. Often that is with a Parent whose behaviour is – to our mind – unacceptable.

You will all know the type only too well. Often too clever by half, with time on their hands, and frequently with a SEN Child, they appear to have nothing better to do than to cause mayhem for the School. In their defence, in the current climate they may be inappropriately supported by their Local Authority, and genuinely might want help to make their case, if that is so I am sure you would be motivated to do so.

Thus engagement and communication is always the first recommendation, but what happens when that fails, usually not as a result of any fault of the School?

We have seen Parents go to war with the School, with a wish to prove something, anything, everybody and all actions to be "wrong", and the Subject Access Request becomes one of their weapons of choice.

We would like to make two points. First, in those circumstances we have never found a School to have behaved anything other than with the entire best interests of the Child at all times. Because somebody else throws wild criticism about does not make it true or fair, and where it is out of control there are sanctions available to support you. You should never doubt yourselves. You are "in loco parentis" and absolutely entitled to take decisions and the result is not subject to either an audit or a qualification by a Parent. That is what being "the Head" means, and society owes you a duty to respect your position and authority.

Secondly there are appropriate procedures to deal with the situation when they enter the realms of the campaigning bully. Of course these have to be used sensitively, and in accordance with full compliance with the Regulation, but there are words such as "manifestly unfounded and excessive" – together with case law and consequences for vexatious behaviour – that can be used to neuter unreason.

Our message is one of support for Heads, who have very considerable and often lonely responsibility whilst providing a critical social contribution, against unmerited and prejudiced attack from the very people you seek so hard to serve. Their behaviour is not correct.

## 2 Satswana prices for 2020

As we enter our third year of providing a fractional DPO service to Schools we have reviewed our pricing for 2020 which in many cases will involve no change, in others it will mean a reduction.

Excluding VAT the basis is that our standard charge will be £2 per pupil, unless there has been a locally agreed different rate, subject to a cap of £2000 per School. No fees will increase.

In the spirit of transparency, Satswana seeks to remain a small group providing strong personal service to their customers. To achieve that we are ten strong in total with four field based Principal DPO's supported by an effective back office, finance and IT section. We aim for a turnover in the region of £225,000 per annum, whereupon you will do the maths!

This price review will mean that we are looking for further customers in order to reach that target, and we are continuously grateful for the personal introductions that you have provided in the past. As the old line goes, if you like what we do, please tell other people, if there are any issues at all, please tell us!

## 3 Encrypting phones

May we please draw your attention to the paper published under our Resources tab on this subject, to be found here:-

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

## 4 Biometric information policy

Satswana are grateful for the provision of the following policy as a result of their cooperation agreement with David Powell of Sapphire Skies Restorative, he has 30 years Police experience of providing safeguarding consultancy to schools.

**Protection of Biometric information for children at (Name of School)**

**1.1 Legal Framework - Protection of Freedoms Act 2012 – Data Protection Act 2018 – GDPR - DfE guidance Protection of biometric information of children in schools and colleges**

1.2 At (Name of School) the written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18.

1.3 In no circumstances can a child's biometric data be processed without written consent.

1.4 (Name of School) will not process the biometric data of a pupil (under 18 years of age) where:

a) The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) No parent has consented in writing to the processing; or

c) A parent has objected in writing to such processing, even if another parent has given written consent.

1.5 (Name of School) will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

1.6(Name of School) refers to the latest guidance published by the DfE for the implementation of policy https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

## 5 Processing European Data

We will seek to avoid the "B" word, but predictably there is both contradiction and confusion in the advice being provided if we leave the European Union. The ICO talks of transitional arrangements, but those are subject to "a deal", which may not apply if we "crash out".

Before either can happen we now face an election, which might yet mean the revocation of Article 50 and mean the whole question can be forgotten!

However the common sense practical reality is that there will be no interruption to any data provision; we will all be concerned with much greater priorities and nobody will have either the time or capability to suddenly cut us off. (We are certain that we would be added to the list of those with adequacy agreements.)

But if you have the resources it would be a sensible precaution to assess what data you are sending to, or receiving from, a European based server so that you can react if you have to.

Bear in mind that any data you have on a Continental child remains subject to GDPR 2016 regardless of any change in the status of the United Kingdom.

## 6 The right to be forgotten

Satswana seeks to share the problem that exists between the European view of data and the US view; you will find some of our argument here https://www.satswana.com/resource/SatswanaobjectiontoEUUSPrivacyShield.pdf

It has been brought into sharp focus by Google's response to the "right to be forgotten". What they have failed to do is to remove the data. Instead they have introduced what they have called "Geo Blocking" – meaning that you will not see the data if you login from a European server, everybody else can see it.

Shades of the censorship methods used on Chinese networks.

Google's original motto was "don't be evil", now reinvented as "do the right thing". What do you think of this behaviour? They claim that the law does not apply to their users outside the EU, and that viewpoint has been supported by the European Court of Justice. We gather that the argument was that the EU did not wish to be seen to be dictating law to organisations outside their jurisdiction, something US law has no hesitation in doing! Whatever, it means that one ill-considered posting can potentially ruin a person's life forever, all for the commercial benefit of a vast corporate. "Do the right thing"? Huh!

Google are seeking all means to establish a presence in education with attractive products and absolute control of the Android operating system on phones. When considering your choice we do suggest you reflect on what will happen to any data they harvest.

## 7 Microsoft Teams

We are fans of central collaboration, where people come to the data rather than data being distributed to the edge, and specifically we are looking for a long term replacement to the ubiquitous use of email.

One new solution that is worth a serious look is Microsoft Teams, which is the 365 competition to the capability marketed by Slack – favoured by City traders who spend all their lives watching screens. Video, chat, file share, you name it.

To make this more interesting, please may we tell you the history of Slack? We would not guarantee the accuracy of all the data, but we understand that a proven management of gaming companies persuaded a Silicon Valley VC to invest $250 Million in a new game. They burned their way through around $80 Million before sitting round the table and agreeing that the product was rubbish, and would go nowhere. But hey, the collaborative tool we have developed to discuss these matters internally is pretty cool! So they used the rest of the money to launch Slack!

Microsoft Teams is both a logical copy and inevitable competition, with added benefits – notably with its current integration into Sharepoint, as an example. In the future Satswana believes that the file and data sharing will develop to the point that it will do what MIS suppliers are failing to do, and that is to provide the centralisation of program functions, so that an IT Manager will no longer have to manage multiple databases. They will have a common form in the centre, and then be passed out to the App in whatever form that requires.

Did the games programmers ever think of that?

## 8 Cookie Law?

We have seen emails from an organisation writing to schools stating that they are not compliant with "Cookie Law". Of course it is one of those "fear selling" organisations that we have total contempt for, especially since they are seeking to market to you without your consent. It is good practice to have a statement on your website regarding the use of Cookies, but this can be organised by your web designer – there is absolutely no need to go anywhere else!

## 9 ICO fines

The ICO have issued a few fines to schools that have failed to pay their registration fee. Please check that yours is up to date!

## 10 Artificial Intelligence

We note some commentators writing about the application of artificial intelligence in the class room and regret they largely do not understand what AI is!

The manner in which Google approached getting its computers to play the strategy game of "Go" probably explains it best.

All they did was to tell the machine what the rules were. The machine then had the capability to decide to play millions of games against itself, gaining experience and arriving at conclusions – until it was able to beat the very best human grand master.

Thus it learned entirely within its own intelligence, with no human support.

We think we will see a great deal of the application of intelligent computing in the future, but suspect that behind it all there will be a teacher, not a machine!

### 11 Schools and Academies Show

We have a small presence at the above show taking place at the NEC Birmingham on the 13th and 14th November on Stand L62. Please call in if you can!!

### 12 Republishing the ICO decision on the NHS

We have recently had customers asking about the legality of providing data to the NHS. Last year we asked the same questions, to the point that we raised the matter as a complaint with the ICO.

Below we republish their response.

The reality of the matter is that it is not up to us to either agree or disagree, it is the prerogative of the ICO to set case law in their determination. In the case of the University of Worcester decision (details to be found here) https://www.satswana.com/resource/DealingwithSubjectAccessRequests.pdf the precedent is supportive to our cause when dealing with SAR's. Thus, in this matter also, we are informed by their ruling.

3 January 2019

**Case Reference Number RFA0789669**

Dear Mr Howard,

I write in relation to the concern you have raised about Public Health England (PHE).

**Our role**

We want to know how organisations are doing when they are handling your personal information.

If we think the organisation has not complied with their obligations under the data protection law we oversee we can give them advice and ask them to solve the problem. Our main aim is to improve the information rights practices of organisations, where there is an opportunity for us to do so.

Before reporting a concern to us, we expect you to give the organisation the opportunity to consider it first. In order for us to look at their information rights practices we need you to provide us with their reply.

**Your concerns**

I understand you are concerned about the lawful bases for

processing of school children's personal data. You have explained that you are concerned about height and weight measurements, vaccinations and dental surveys and how information collected is shared with local authority providers such as the school nursing services.

**Our view**

You have raised your concerns with PHE and it appears they have provided you with a number of in depth responses.

Based on the responses you have received I am satisfied that the information you have been provided with does not suggest any concerns about PHE and their understanding of their obligations under the General Data Protection Regulation (GDPR).

PHE have advised that their lawful bases for processing information

are:

- Article 6(1)(e)
- Article 9(2)(h)
- Article 9(2)(i)

Firstly, I feel I should emphasise that no single basis is "better" or more important than the others – the most appropriate basis to use will depend on your purpose for processing. As such consent is not always the most appropriate basis for organisations. For further information on the lawful basis for processing please visit: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

I feel it is important that I reiterate advice provided to you by PHE that there is a difference between consent as a basis for processing under GDPR and parental consent for carrying out a medical procedure. As PHE have explained to you, they do ask parents to provide consent for a vaccination to be administered, however this is consent for a medical procedure and not for processing the data. They are relying on the articles listed above as their bases for lawful processing.

For further information you may wish to visit our website, specifically the information under the heading *"Do we need consent to process personal data for our patient care functions?"*: https://ico.org.uk/for-organisations/health/health-gdpr-faqs/

Furthermore PHE have explained that with regards to height and weight measurements, although consent is not the basis for processing this information, parents are given the opportunity to withdraw their children from the measurements. This is because although this is a nationally adopted scheme, parents have the option for their children's data to not be included in this collection.

As such the basis for processing which they have provided appears to be sufficient.

Finally, PHE have advised that they have obligations under a variety of legislation in addition to the GDPR. They have requirements to fulfil under this additional legislation such as the NHS Act, which we do not regulate. I note that they provided you with appropriate links to this legislation as further guidance.

Therefore, as explained previously we do not have any concerns regarding the bases for processing information by PHE under the GDPR. I hope that this correspondence provides you with sufficient information and guidance. If you have any further queries please do not hesitate to contact me.

Yours sincerely,

(Name redacted)
Case Officer
Information Commissioner's Office
0330 414 xxxx

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

**L Bonus update 2019**

"We are in an age of borderless data flows. And as data travels internationally, so do privacy issues. Microtargeting. Surveillance. Our digital footprint and the transparency expectations that go with that. Governance around data protection and meaningful privacy enforcement are more complex, multinational and political than ever."

Elizabeth Denham, Information Commissioner

## 1 Google report

One of the benefits of the great wealth of Google is that they have fabulous resources, so when they publish a report on emerging classroom trends it has to be worth a read. It is available from the link below, but as a precis there are eight assumptions as follows.

1 Online safety should be part of the Curriculum
2 A drive for general life skills is more important than academic qualifications?
3 STEM (Science, Technology, Engineering and Mathematics) together with coding skills is increasingly vital
4 There must be a more nuanced balance between teacher led and student led discussion
5 Classroom design affects a student's academic progress
6 Embracing parents as a partner in education?
7 Technology can be leveraged to free up teacher time
8 How to incorporate emerging technologies into learning

http://services.google.com/fh/files/misc/future_of_the_classroom_emerging_trends_in_k12_education.pdf?utm_source=email&utm_campaign=FY19-Q2-global-demandgen-website-other-futureoftheclassroom&mkt_tok=eyJpIjoiWlRsaE56SmpORFExTWpGaCIsInQiOiJ4WTBUWmF6alB5RXJoWTRqVFc2QjBPOXk0RlZCSlN0OGJ1MVVEc2ZEUFBRM3BkT0hZYWd4dGF6UGw2QUZ3eFl6dU90QmNcL3M5K2sxQldlendwVVhRcWZtWkFtdkZGTUxlRTZraFIxZUtYWlpRazNTNklWcTRYU3NqWGlrVE5iREMifQ%3D%3D

## 2 Special category data

The ICO has published updated GDPR guidance regarding special category data.

The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection. Special category data relates to personal data that:

- reveals **racial or ethnic origin**;
- reveals **political opinions**;
- reveals **religious or philosophical beliefs**;
- reveals **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning an individual's **health**;
- data concerning a person's **sex life**; or
- their **sexual orientation**.

## 3 Overcoming Phishing

The "Windows Defender" aspect of Windows 10 is a remarkable antivirus and firewall product, and Microsoft should be given further credit for the manner in which they automatically install patches to overcome vulnerabilities as they are recognised. (Though I wish it would not default to a US keyboard on my computer!)

They are now working on a new container structure that will counter the triggering of a macro which is the manner in which a phishing attack penetrates your computer, we quote:-

"You will be able to open an untrusted Word, Excel, or PowerPoint file in a virtualized container. View, print, edit and save changes to untrusted Office documents - all while benefiting from that same hardware-level security. If the untrusted file is malicious, the attack is contained and the host machine untouched. A new container is created every time you log in, providing a clean start as well as peace of mind."

Of course the criminals will find new ways, but full marks to Microsoft for their continued diligence on our behalf.

## 4 Marvellous me

We really are grateful for Schools that ask us to check out processing organisations, not least because once they are analysed we can add them to our Processor list.

A recent example was Marvellous me where we found multiple flaws, all of which we were able to resolve following a conversation with the Chief Executive.

It is not always that way, and some of our customers have declined to use a service once they saw the response to our enquiry.

Please keep them coming!

## 5 HTTPS

One of the issues with Marvellous me was that their main web page was secured with HTTPS, but the page carrying their privacy notice was not! Once pointed out to them it was corrected quickly, but please take a second look at your website and ensure that all pages are HTTPS!

## 6 Survey Monkey alternative?

The problem with the popular Survey Monkey is that their servers are US based. This organisation claims to be a GDPR compliant option.

https://www.smartsurvey.co.uk/survey-monkey-alternative

## 7 Cyber-attack?

Apparently a prominent political party suffered a serious cyber-attack that originated from Russia or Brazil, possibly both, no data was believed to have been taken.

My goodness, what absolute garbage. We cannot afford to ignore the real risks that are out there, but this was a “denial of service” attack, they can be purchased from the Dark Net for a few pounds. What you buy is an extensive network of infected processor capacity that bombards the target IP address with so much traffic that it is flooded – causing it to slow down or fall over.

Thus it really only has nuisance value, there can be no risk of data exfiltration, and it is totally impossible to define where it came from, there could be literally millions of IP sources involved.

It is disappointing that political drama was allowed to mislead a public that would not know the difference, and even more disappointing to read that the party concerned were not going to change their $20 defence mechanism. Not that it would help with a DDOS attack, but there will be far more professional forces at work, and they will be hoping not to be found, for people not to know they are there.

Two lessons, the first being that the lack of education and understanding of far too many who should know better makes it far too easy for cybercrime to prosper, especially when they fail to adopt counter measures. The other lesson? The truth is that we are yet to learn it. Complacency has been restored, and there will be something going on that we may discover in several months' time, and then we will all be appalled. Last time it was the Facebook fake accounts, with fake news. What will it be this time?

## 8 Do not sell?

The latest version of privacy protection thought emanating from the United States is the upcoming California Consumer Privacy Act (CCPA). One of the main requirements is the 'Do Not Sell' or 'Opt Out' Rule of CCPA which gives consumers the right to opt-out of the sale of their personal information. That of course is the polar opposite of the European approach that requires an "opt in", and bans "opt outs".

To comply an organisation must Add a "Do Not Sell My Personal Information" link or button to their website, Implement an efficient process to respond to consumer rights requests, and Implement an efficient process to respond to consumer rights requests.

We fear that the divergence on privacy rights and protections between the US and Europe remains as stark as ever.

## 9 Redacting documents using Adobe Pro

A good tip picked up whilst going through a complex subject access request is that any document that is scanned into Adobe Pro can be "redacted" digitally. It was also pointed out that if the entire document is captured in this digital form it can be shared to confirm that no redactions have been missed, and then delivered to the requesting party without having to print out reams of paper

## 10 Anonymising data in Teacher training

A most interesting question that will be relevant to all Schools with a training responsibility, and an example of an unintended consequence from well-meant legislation!

We were asked how personal information could be protected within Student Teacher files once they left the training school.

We decided that the answer was to use the GDPR provisions for research data, whereby if it is anonymised, then you can continue to use and keep data.

We assumed that the trainees need the names of the students whilst they are teaching them, so what we recommended was that they are “anonymised” before they leave – perhaps as a specific exercise which would have the merit of reinforcing the GDPR message to the trainees. An easy solution is to use Tippex to paint over the names, which has the merit that it does not show through if the document is photocopied (as some black markers do.)

We anticipated a theoretical argument that it would be possible to scrape the paint off, to which we would reply that would be a clearly criminal act that defeated the intention to protect personal data, thus demonstrating that all these things can be taken too far, and that in the real world we need to use data responsibly.

The MAT that enquired felt that was a suitable solution.

## 11 Criticism of DfE by ICO

The ICO has criticised the DfE for secretly sharing children’s personal data with the Home Office, prompting fears that the data could be used for immigration enforcement as part of the government’s hostile environment policy.

Acting on a complaint made by the campaigning organisation Against Borders for Children (ABC), the ICO ruled that the DfE failed to fully comply with its data protection obligations.

When representing the complainant, human rights organisation Liberty said teachers and parents were unaware that the information they gave to schools could be shared with immigration enforcement and result in families being deported.

The ICO is now considering whether to take further action against the DfE for “wide ranging and serious concerns” highlighted in this case and raised by “a number of other sources”.

## 12 Contractual necessity as a basis for processing

This is an extract from a longer document on this subject, it is provided in case the basis is appropriate to be considered. If it is we can go into greater depth.

Contractual necessity is the most appropriate basis when the processing is necessary in order for a product or service to be provided. Essentially, by choosing this basis you are saying ‘we can’t comply with our side of the contract without this processing’.

This is not a basis to use lightly – it means that the fundamental aspects of your product or service rely on the processing.

For example, you might be unable to complete an order without processing a delivery or home address. However, just because something is included or permitted by a contract doesn’t necessarily mean that it is contractually necessary. If you could deliver the product or service without the processing, then the contractual basis is not going to be the most appropriate.

In some cases, the distinction is clear – you need an address in order to deliver the socks a customer bought. However, any further uses of that address, such as using it for sending them marketing materials, will need a different lawful basis.

Similarly, whilst you need the address so you can post the socks, you don’t need to know why the customer bought them in order to do that – so you would need a different lawful basis to collect that information.

## 13 Images under FOI

An interesting amendment to the Freedom of Information Act following DPA 2018

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under the Data Protection Act 2018 and GDPR.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the Data Protection Act 2018 and GDPR.

## 14 No rights to email once resigned

And finally a person who resigned from a School demanded subsequent access to their School supplied email account, which had been blocked; it was denied. It is not sufficiently recognised that many aspects of School life remains the intellectual property of the School and not the employee (or Governor in this case.) Worth remembering!