The Exciting World Of GDPR

Term 5—2020/21

Welcome

Don't not fear as the panic is over. After waiting patiently for what must have seemed longer than the lockdown we are thrilled (and I know you will be too) that we are welcoming you back to…….

'The Exciting World of GDPR'

Get yourself a lovely cup of tea, find a quiet spot and enjoy the guilty pleasure of catching up with everything data protection.

'More exciting and slightly less annoying than finding a piece of chewing gum on your shoe'

Cookie Conundrum

We all love a cookie but sadly we are not giving a packet of cookies away with this edition of the 'Wonderful World of GDPR'. However, even better than food we have managed to find for you (Thanks to Chris Riley @Rivermead) a game which tests our knowledge of computer cookies.

Since GDPR came into our lives, we've all had to struggle with obtaining our basic privacy rights. With each cookie banner we have all been honing our skills, learning to navigate ambiguous options and distrust obvious buttons.

Now is your chance to show what you have learnt. However before this, here are some basic cookie facts:

What are cookies in a computer?

Cookies are text files with small pieces of data — like a username and password — that are used to identify your **computer** as you use a **computer** network. ... Data stored in a cookie is created by the server upon your connection. This data is labelled with an ID unique to you and your **computer**.

Should I delete cookies?

When you **delete cookies** from your computer, you erase information saved in your browser, including your account passwords, website preferences, and settings. **Deleting** your **cookies** can be helpful if you share your computer or device with other people and don't want them to see your browsing history.

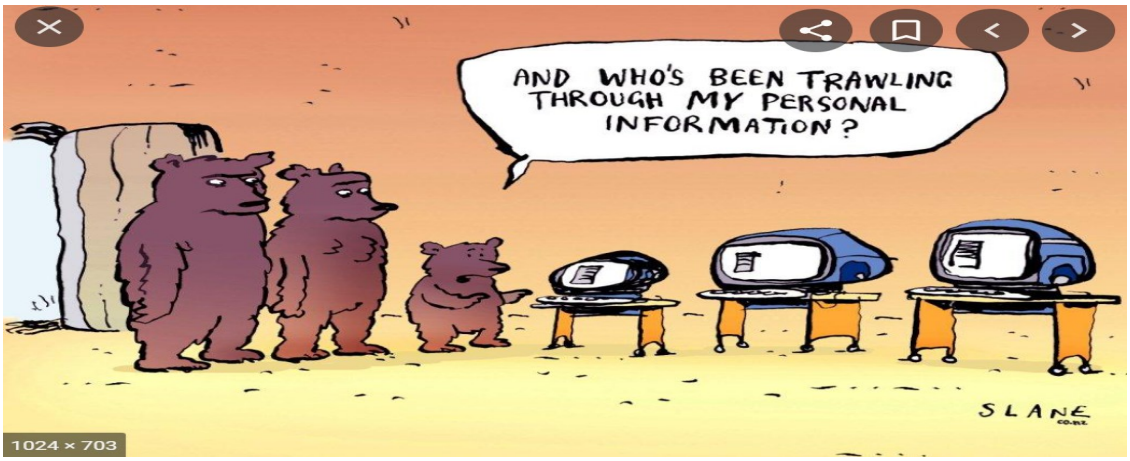
Are cookies a security risk?

Yet, depending on how **cookies** are used and exposed, they can represent a serious **security risk**. For instance, **cookies** can be hijacked. As most websites utilize **cookies** as the only identifiers for user sessions, if a **cookie** is hijacked, an attacker could be able to impersonate a user and gain unauthorized access

To access the game then press CTRL and CLICK HERE

Just Joking 3

GDPR continues to be a very dry subject and not a matter to giggle over. We thought however we would bring back our feature from our last two editions with a few more GDPR cartoons



Digestible Documents

.WhatsApp data protection implications for Trusts/Schools

WhatsApp is a great app. It's free, easy to use and rarely has technical issues. It allows everyone to share words, audio and pictures at the click of a button, and during the Covid-19 pandemic, it has been a lifeline to many people. With everyone spread far and wide, working remotely, it has seen an exponential increase in its use.

Be under no illusion if it's "too good to be true" then it usually is!

WhatsApp carries high risks to any organisation that chooses to use it for anything besides inter-staff chit-chat or conversations which do not include personal data. Anything else will make the organisation non-compliant with data protection law.

You might argue that during the pandemic the Information Commissioner's Office endorsed WhatsApp's use in the health and social care system.

So why not schools?

Clinicians have been told they can use messaging services like WhatsApp "where the benefits outweigh the risk" to share information about coronavirus. The Information Commissioner said:

"The ICO is a reasonable and pragmatic regulator, one that does not operate in isolation from matters of serious public concern. Regarding compliance with data protection, we will take into account the compelling public interest in the current health emergency."

"We know you might need to share information quickly or adapt the way you work. Data protection will not stop you doing that. It's about being proportionate".

Very little communication within Trusts/Schools would fit this criterion; anything else may not meet your privacy obligations.

The ICO has published the Accountability Framework to which every organisation must comply. Trusts/Schools, as public bodies, must demonstrate that their data protection protocols are fully aligned to these principles.

The conclusion is very clear

WhatsApp is a wonderful communication tool for individuals. During the pandemic it can be used by health professions if there is no alternative and helps to save lives. However, the risk of using WhatsApp must be understood and every opportunity must be taken to mitigate those risks.

Trusts/Schools may use WhatsApp to share personal data in limited circumstances but for 'business as usual' communication it's really not suitable.

Go to our next page of the newsletter to see why

WhatsApp

is not compliant

Digestible Documents—The Facts

ICO Accountability Category	WhatsRight	WhatsApp
Leadership and Oversight	Trusts/Schools should be the data controller for personal data. Data protection governance structure and protocols must then be implemented and controlled as defined in their Data Protection policy and working practices. *[GDPRiSPro provides many resources to enhance this work]*	WhatsApp is the data controller. There is no option to implement any form of governance. Trusts/Schools have no control of data; only individuals can exercise their rights.
Policies and procedures	Trusts/Schools should choose systems which process personal data that have been developed with 'Data protection by design and default'. They should support best practice in ensuring all data subjects' rights and freedoms are maintained. *[GDPRiSPro provides examples]*	As WhatsApp is the data controller Trusts/Schools have no say in the direction of policies and procedures. 'Data Protection by design and default' is not evidenced across the WhatsApp organisation.
Training and awareness	All staff must know how to use a system and are fully aware of their responsibilities regarding the data collected. Training should include security, retention, breach management and SAR reporting *[GDPRiSPro provides this training and more]*	No training is available. Whilst the app is very easy to use, the implication of how it is used may have serious impacts on data security and risk.
Individuals' rights	Individual rights must be clearly defined and understood and can be met by Trusts/Schools at all times. Systems must allow access to data for Subject Requests to be actioned with ease. *[GDPRiS Pro provides many resources to enhance this work]*	Individual rights are clearly defined. WhatsApp ensures these can be met at all times. However, if used as part of an organisation, these cannot be met. Trusts/Schools have no opportunity to respond to a Subject Request.
Transparency	Data processing protocols will be recorded in your RoPA and explained within your Privacy Policy. *[GDPRiS has data maps for all major suppliers. These important data protection documents reflect the evidence of processing]*	The WhatsApp privacy procedures are available online. They are easy to read and have full consideration of GDPR in the EEA. However, all data is stored in the US and you can only rely Consent from the users, yet the data subjects may be entirely different people.

ICO Accountability Category	WhatsRight	WhatsApp
Transparency	Data processing protocols will be recorded in your RoPA and explained within your Privacy Policy. *[GDPRiS has data maps for all major suppliers. These important data protection documents reflect the evidence of processing]*	The WhatsApp privacy procedures are available online. They are easy to read and have full consideration of GDPR in the EEA. However, all data is stored in the US and you can only rely Consent from the users, yet the data subjects may be entirely different people.
Records of processing and lawful basis	Several lawful bases for processing may be used but it is envisaged most Trusts/Schools will rely on Public Task. This will be included in the data maps for the products *[GDPRiSPro has videos to explain and the Training courses highlight this work]*	WhatsApp uses consent from individuals as a lawful basis of processing. Whilst WhatsApp does not produce a data map for a RoPA, this may be done easily.
Contracts and data sharing	Trusts/Schools must have a contract with their suppliers. In the contract should be a full explanation of how data is shared and the protocols in place to protect the data.	Trusts/Schools have no contract with WhatsApp and thus no data sharing agreement.
Risks and Data Protection Impact Assessments.	Full documentation for risk assessment, screening questions and a comprehensive DPIA is available for Trusts/Schools to adopt. *[GDPRiS Pro provides many resources to enhance this work]*	No risk assessment is possible as the Trust/School is not the data controller. A DPIA would be possible but inaccurate as the use of the system is controlled by the user not the organisation.
Records management and security	Trusts/Schools must demonstrate through their Privacy Policy how Data quality, Destruction, Asset Register, Access control and the Retention schedule are managed. *[GDPRiS Pro provides many resources to enhance this work]*	WhatsApp's security measures are extremely sound. However, since Trusts/Schools are not the Data Controller there is no sight of Data quality, Destruction, Asset Register or Access control. Neither can you manage the Retention schedule
Breach response and monitoring	Unfortunately, no one cannot prevent breaches happening! *[However, the GDPRiSPro resources guide you through how to address breaches and how they can be reduced. We will advise how an internal audit should be approached]*	Breaches will happen within WhatsApp as in all systems which process personal data. However, Trusts/Schools have no control except by contacting WhatsApp support process.

Malicious Malware:

As you are all aware there has been an increase in ransomware in education across the UK. Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This type of malware is a moneymaking scheme that can be installed through:

- an email messages
- instant message
- website.

The harms of ransomware are the following:

- Temporary or permanent destruction of sensitive information;
- Disruption of operations by crashing the network;
- Potentially pay the ransom in order to restore system and files.

Due to the potential loss of data, this could lead to a potential GDPR breach resulting in fines depending on the severity of the data loss.

Super Senso:

As you are all ware Senso is installed on devices across the trust. The ***Cloud***-Based Platform is used for: Remote Monitoring and Management.

It is an all in one software All-In-One Software for:

Network, that includes: Classroom, Safeguarding and Asset Management.
Manage and Monitor any Windows & Chrome devices from a Centralised Web portal.

To ensure that Senso complies with GDPR only designated staff are given access to the software.

Brilliant BitLocker

As you are all aware BitLocker has been installed onto staff laptops that are taken offsite. BitLocker Drive Encryption is a data **protection** feature that integrates with the operating system. This helps to address the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

By having BitLocker installed this helps us to comply with GDPR