



The Exciting World Of GDPR

Term 2

Welcome

Well Christmas is nearly here and we at the RIT love to give you presents and boy have you got a great present in our latest GDPR newsletter. We hope like a good Christmas, you can enjoy and then maybe over indulge a little in reading your termly GDPR newsletter. Grab yourself a Christmas tippie, find a spot under the mistletoe and enjoy keeping up to date with the latest in the world of GDPR.



Two Top Tips

Here we provide you two top tips when using your school data at home:

- 1. When using your own technology (phones, laptops, PCs etc.) ensure it is password protected and adequately encrypted.**

Encrypting your devices helps to protect user data from theft and other malicious actions. Full-disk encryption allows the owner to protect everything with one easily-remembered passphrase, which is entered when the device boots up. A hacker will be unable to access the data without this passphrase, even if they remove the hard drive. Encryption also offers IT professionals the opportunity to enter a legal "backdoor" into the system, so they can gain control when a staff member leaves, for example. [Windows 10 contains BitLocker](#), which enhances file and system protections. BitLocker also helps render data inaccessible when BitLocker-protected computers are decommissioned or recycled.

- 2. Ensure laptops and PCs have adequate encryption, antivirus, malware and other protections**

Teachers often work at home in the evening, at weekends and during school holidays, but this can raise issues when it comes to data movement and storage. Information relating to pupils and staff can be lost or stolen if stored on unprotected USB sticks and personal laptops - according to [research from EE](#), almost 10 million mobile devices such as smartphones, tablets and laptops containing sensitive business data were lost by employees across Britain in 2013/2014. Moving data to easily accessible WiFi networks will also raise concerns. Always keep personal and work-related information separate, and encrypt all files and devices that relate to your job.

Regular Reminder

We have mentioned it before but just a timely reminder to be careful what you write and mention within any e-mails that you send. If the Trust is asked for a Subject Access Review then all of your e-mails sent or received will be included within this.

The following guidelines comes from a solicitor:

"So, a subject access request can relate to any personal data held on computer (for example mails to or from the data subject or between other individuals) including backups, any data held in hard copy where it is intended to transfer that data to computer and any data held in hard copy in such a way that it is very easy to locate data relevant to a particular individual (for example, a personnel file)."



e-
in-

Child Caution

GDPR regulation states that you need to be very careful in dealing with data related to children. Below are just a few areas which you really need to be considerate of.

- Children are identified as "vulnerable individuals" and deserving of "specific protection"
- Processing of data relating to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct.
- The GDPR does not prescribe the age at which a person is considered to be a child.
- Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the child. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit -which may be no lower than 13)



Quick Quiz

Do you think you have a great deal of GDPR knowledge? Try our new Term 2 GDPR quiz to see if you are a GDPR guru or need to go back to the GDPR drawing board.

[Quiz 1](#) - Click on the 'quiz 1' to start

RIT Rights

Do you know what your rights are under GDPR? Here we give you a guide to your rights :

Under GDPR, the personal data you hold or process about a living person gives them the following rights:

- The right to be informed -you must tell them what data is used, why and for what purpose
- The right of access - parents, staff and students are allowed to see what data of theirs is processed
- The right of rectification - if their data is wrong, you must correct it
- The right to erasure - they can demand that you delete all their data
- The right to data portability - they can decide to move their data to another processor, which you then must supply the data to securely
- The right to object - they can object to your use of their data and you must stop using it
- Rights in relation to automated decision-making or profiling - they can demand that automated decisions about them are reviewed by a human



Digestible Documents

Wonder how the data of our pupils is being checked. An interesting article discusses the idea of whether our children are being 'datafied from birth'

The children's commissioner for England is calling on internet giants and toy-makers to be more transparent about the data they are collecting on children.

Today's children are the first to be "datafied" from birth and little thought has been given to the consequences, a report for her says.

[Who Knows What about Me?](#) calls for a statutory duty of care between social media giants and their younger users.

And it urges the government to consider strengthening data protection laws.

'Canary in mine'

The report also highlights how very young children are now using toys that are connected to the internet.

These gather personal messages and information that may be insecure and open to attack from hackers, it says.

The report quotes research led by Sonia Livingstone, who describes children as the "canary in the coal mine for wider society" - the first to encounter new technology and its risks before many adults are even aware of them.

It says:

- children should be taught in schools about how their data is collected and for what purposes
- where a toy collects any video or audio generated by a child, this should be made explicit in a prominent part of the packaging or its accompanying information
- using language children understand, companies should explain clearly in their terms and conditions what data is collected and how it will be used

The report estimates:

- between the ages of 11 and 16, children post on social media 26 times a day, on average
- by the time they reach adulthood, they are likely to have posted 70,000 times

- by the age of 13, a child's parents will have posted on average 1,300 photos and videos of them to social media

There is also:

- the data gathered when children use the internet
- tracking devices and apps used by parents to keep tabs on their offspring
- the biometric data held by public bodies such as schools and the NHS

The report warns that there could be risks to young people where profiling of internet usage is utilised in areas of life where it can have deeper ramifications, such as the judicial system or the education system.

One worrying scenario it gives is if a health insurance company used information posted by a child on social media about their mental health as part of its decision on whether to issue a policy or how much to charge.

Technology develops

Anne Longfield, the Children's Commissioner for England, said: "We need to stop and think about what this means for children's lives now and how it may impact on their future lives as adults.

"We simply do not know what the consequences of all this information about our children will be.

"Companies that make apps, toys and other products used by children need to stop filling them with trackers and put their terms and conditions in language that children understand.

"And crucially the government needs to monitor the situation and refine data protection legislation if needed, so that children are genuinely protected - especially as technology develops."



If you have anything that you would like featured in any future editions of the 'Wonderful World of GDPR' then please contact me at

dadsp001@rivermeadinclusive.org