



The Exciting World Of GDPR

Term 4 and 5

Welcome

I can't possibly imagine how you have managed to get through the last two terms without your GDPR updates via our newsletter. Well panic over because you can now take a nice drink, find a quiet spot and switch off and enjoy everyone's guilty pleasure—The latest edition of **'The Exciting World of GDPR'**



Frightening Fine

Did you know that if you fail to get a child's consent for using their data (under 16 parental consent), under section 83 of the GDPR act you could be fined 10 million Euros or 2% of the annual turnover of the Whole Trust.

A scary thought so make sure you get that consent for any pupil data that you might need



Finger Facts

Some of our Trust schools may consider collecting fingerprints for registration, library book borrowing and catering. However, some people are concerned about their fingerprints being used in this way.

What does the Act say?

The Data Protection Act says that personal data (in this case fingerprints) must be fairly obtained. In other words, the school should ensure that pupils are fully aware of the implications of having their fingerprints taken before doing so. Depending on the level of understanding of the pupils, this may need to involve their parents.

What should I expect the school to do?

Schools should explain the reasons for needing to collect fingerprints, and how the fingerprints and any other personal details will be used and kept safe. Schools should respect the wishes of pupils and parents who object to school fingerprinting, especially where a card can be used instead of a fingerprint.



Quick Quiz

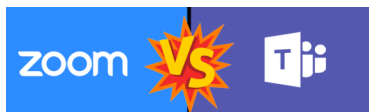
How well do you think you know GDPR and GDPR laws. Whether you are a GDPR guru or a nervous novice; why not try out quick two minute GDPR quiz to see if you know as much as you think you do?

To access the quiz click on the link below:

<https://www.lsoft.com/news/gdpr-issue3-2017.asp>



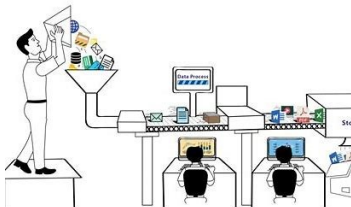
Top Teams



With an increase with working at home and the use of Microsoft Teams we wanted to reassure that under GDPR this is the most secure package to be using. Teams data is encrypted in transit and at rest. Microsoft uses industry standard technologies such as TLS and SRTP to encrypt all data in transit between users' devices and Microsoft datacentres. This includes messages, files, meetings, and other content. However if you can limit the amount of documents that you save in Teams this will also improve the security of the system.

For those currently using Zoom we suggest that you **NEVER** share any documents that contain sensitive information as currently Zoom does not offer end to end encryption.

Processing Personal Data



Any data that you process within schools must fit into one of six conditions for the processing of personal data.

These six are:

- a) **Consent: the individual has given clear consent for you to process their personal data for a specific purpose.**
- b) **Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.**
- c) **Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).**
- a) **Vital interests: the processing is necessary to protect someone's life.**
- b) **Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.**
- c) **Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks. Public authorities will need to rely on official functions.**

Digestible Documents

In this editions article we look at the two articles on the risk of having a data breach at your school.

Exclusive: More than 700 school data breaches in a year
Schools risk 'extensive reputational damage' if personal data of parents or pupils is compromised, accountants warn

The number of data breaches reported by schools increased by almost a quarter in just two years, new research shows.
Schools in the UK reported 703 data breaches to the Information Commissioner's Office (ICO) in 2016-17, compared with 571 in 2014-15.

A freedom of information request by accountancy network UHY Hacker Young showed that 674 were reported in 2015-16.

The news comes after a school business managers' leader last year warned that funding pressures on schools were making them more vulnerable to cyber-attacks.

And earlier this year, the Charity Commission warned private schools that fraudsters were trying to intercept fee payments from parents using emails.

Allan Hickie, partner at UHY Hacker Young, warned that cyber-attacks can cause schools "extensive reputational damage, especially if the personal data of children and parents is compromised".

He added: "As almost all data is now stored electronically, safe-

guards must be put in place to ensure that schools' sensitive data is kept secure.

Guarding against cyber attacks

"Parents must be reassured that the information held on their children, and their own financial data, is kept safe.

"Many private and independent schools are attractive to fraudsters, as school fees that they are attempting to redirect are often of high value. It is vital that schools have strong data security in place."

His organisation warned that schools are now at a serious risk of large fines from the ICO if they fail to report data breaches, following the introduction of GDPR in May 2018.

The regulations make it compulsory for all organisations to report any data breach where there is a risk to people's data security, including incidents where no information is actually lost or stolen. However, UHY said that the ICO is unlikely to levy large fines on smaller schools and academies where data on pupils has not been put at risk.

The Department for Education said that all organisations, including schools and colleges, should have good basic cyber-security measures in place.

It pointed to the government's Cyber Essentials scheme, which aims to protect against common vulnerabilities which are widely reported online

Investigation: Schools heading for pupil data scandal

It is only a matter of time before schools become engulfed in scandals over breaches of their pupils' data, a leading expert has warned.

The claim comes amid a growing number of schools reporting data breaches to the Information Commissioner's Office.
Ross Anderson, professor of security engineering at the University of Cambridge, outlined fears that the education system was at risk of the sort of high-profile failings that have hit the NHS in recent years

"There are gazillions of companies using all sorts of computerised learning materials and schools are inhaling this without much pause for thought," he told *Tes*.

"There are a number of issues: the first is quality control and market regulation and now it is a huge free for all. Companies are also selling this data to all and sundry, even when it is personal health information. Surely there are concerns there?"

"The first thing [schools] must do is understand and have a list of all the personal data they keep and for what purpose, and figure out in advance what the lawful justification for that is, and is it something for which you need consent

"Eventually, there will be a scandal, perhaps fairly soon.

"Exactly the same risk applies to systems in schools [as in the NHS] which set out to collect what amounts to health data. What is it doing sitting on a server in Taiwan?"

"It will take a while for the penny to drop but eventually it will be on the front of the *Daily Mail* and there will be a huge outcry. They [schools] have no idea what is being done to the data or where it is.

"You have to look very closely under the hood to who gets the data and what are the secondary uses.

"Are they proposing to put Google ads in front of your kids? If so, you should probably run them out of town.

"There are a lot of people selling complete crap to a lot of complete suckers."

Professor Anderson has particular concerns about biometrics "being used aggressively for everything in schools, from libraries to lockers, but do we want the kids to be indoctrinated into the idea that biometrics are a good thing?"

He warned that many apps used by schools were "extracting personal health information, such as recognising whether children have special needs or are autistic". "Firstly, what is the robustness of these tests, and secondly what about the control of

this information?" he said.

Unless the school retains ownership of the data, it can be sold on, with the school having no idea who is using it and why. Although GDPR has made schools more aware of privacy issues, Professor Anderson said there was still a long way to go.

"I suspect that if a rigorous GDPR audit was given to the average school in England and Wales they would fail by a mile," he said.

"They often have no clue what is being hoovered up, by whom and to what use it is being put."

The academic said that schools needed to be savvier about what they were using.

"Lots of schools buy all sorts of crap because they don't understand it," he said. "They think it is going to help but it doesn't. If you are going to use it you have to understand it. If you haven't been on a chainsaw awareness course, don't buy a chainsaw." But Duncan Baldwin, deputy policy director at the Association of School and College Leaders, told *Tes* that schools were "very good at storing data and understanding what needs to be done with it"

He added: "GDPR means that their relationship with other providers has had to be more clearly understood. Schools have always had a responsibility for data and GDPR has made things more transparent.

"I don't think as far as schools are concerned it is substantially different from five or 10 years ago.

"There will be formal arrangements about data sharing in place with any providers they use, so the ownership of the data is clear."

Mr Baldwin said that "there are so many benefits that outweigh concerns about where the data is held and so on".

He cited the use of biometric data such as fingerprints to allow pupils to claim free school meals discretely and avoid stigma. He added: "Data on pupils is held securely on a school's servers, in conjunction with their management information providers, and it has always been thus. Information has always been held like that

"Schools are more vigilant about access to data, making sure that it is secure and encrypted."

