GDPR FOR SCHOOLS

Preparing for the New Data Protection Regulation

groupcall™

built on **trust**

CONTENTS

PART 1

THE DATA PROTECTION LANDSCAPE

INTRODUCTION

We are all aware of the need to protect personal data, whether our own or that of others. In the UK, the most commonly known rules on this subject are contained in The Data Protection Act (DPA) of 1998.

Over recent years there have been numerous cases of data being accessed unlawfully or inadvertently being disclosed to people who should not have been able to view it.

One of the most high-profile instances of this of late was the WannaCry Ransomware attack which affected computers across the globe, notably causing restricted NHS services, as well as problems for international shipping company FedEx and others, by releasing malware into computers which then locked the files preventing access. The malware then demanded a 'ransom' in Bitcoin in order to regain access to the files[1].

Another, in October 2016, saw almost 157,000 TalkTalk customers have their personal data stolen including, in some cases, bank account numbers, dates of birth and addresses. This led to TalkTalk receiving a record fine of £400,000 from the Information Commissioner's Office (ICO) for failing to prevent the attack[2]. At the time is was reported that under the forthcoming GDPR, the bill could have been £73 million[3].

It is invariably only the high-profile cases that we hear about – but these are merely the 'tip of the iceberg'. The vast majority of data breaches are far smaller, affecting fewer people and rarely do these even get reported to the ICO at all. This does not, however, minimise the distress caused to those affected.

Just think how you would feel if your own personal details were made public, or your bank account was accessed unlawfully. It might be 'small' in the grand scheme of things, but it certainly wouldn't feel insignificant to you!

CURRENT DATA PROTECTION LEGISLATION

As mentioned, the main rules in the UK around data protection come from the DPA, which itself actually originated in the 1995 European Data Protection Directive.

As a European Directive, the rules contained within the regulation had to be encompassed into the laws of all countries that were part of the European Economic Area (EEA), including the UK. However, the fact that this was a 'Directive' meant that each country was allowed to pass its own laws which had to meet the standards set by the European Union (EU).

Each country proceeded to implement its own interpretation of the rules, which resulted in twenty-seven countries each having a slightly different variation of them. Some countries interpreted them almost literally, with no changes being made, whilst others interpreted them more liberally resulting in a less effective set of laws in that country around protecting people's personal data.

WHY DO WE NEED A NEW DATA PROTECTION LAW?

So the DPA was passed in 1998 and was a direct result of European legislation passed in 1995. That means we have had the same data protection regime for the past 20 years!

In the meantime, the world of personal data has changed beyond all recognition. In the very year the DPA became law, 1998, Google launched. Now the company processes an average of over 40,000 search queries every second[5].

6 years later, in 2004, Facebook was founded, followed by Twitter (2006), WhatsApp (2009), Instagram (2010) and Tinder (2013). All of these, and so many more applications, have millions, sometimes billions, of users who are posting, tweeting, swiping and chatting millions of times a day, sending personal data all round the world in fractions of a second. The legislators in 1995 could never have foreseen the incredible way that data is used and processed today.

In school terms, things have changed massively too over the past couple of decades. From a mere 800,000 computers in UK schools in 1998 to several million now; schools communicating with parents, staff and pupils using text messaging, emails, Twitter etc.; the huge adoption of tablets and smartphones for learning.

Given this colossal transformation to the data landscape since the DPA was introduced, the rules required an overhaul to reflect it.

In addition, there is a need to coordinate the data protection regimes across all the countries in Europe so that everyone sings to the same song. This will ensure stronger protection for our personal data anywhere across Europe that it is used or processed whilst making it far easier for UK companies to do business across Europe without having a different set of rules to follow in each country.

INTRODUCING THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

There has been much said about the new GDPR, some of it true, some exaggerated and some used simply as a scare-mongering tool. Almost everywhere that GDPR is mentioned, the first things talked about are the massive fines that are going to be imposed on us all for the slightest infringement of the new rules. This recently prompted the Information Commissioner, Elizabeth Denham, to publish a series of blogs aiming to debunk the 'fake news' surrounding GDPR[4].

Yes, the new GDPR does provide potential for massively increased penalties, including fines up to twenty million Euros, or 4% of an organisation's global turnover (whichever is greater) – but these penalties are for major breaches which affect large numbers of data subjects and which cause, or could cause, huge issues for the people affected. These fines will not be imposed for minor infringements any more than the current maximum fine of £500,000 under the DPA is ever used.

The penalties meted out under GDPR will certainly be larger than under the DPA and there will undoubtedly be more fines imposed, after all the ICO has announced plans to recruit a further 200 investigative and enforcement staff[6], but GDPR lays down rules for these penalties and states that they must be "effective, proportionate and dissuasive" and also that the ICO (in the case of the UK) must take into account when deciding the fines the "nature, gravity and duration of the infringement" as well as the "intentional or negligent character" of the breach. What this means is that the biggest fines will be levied on the worst offenders only, not on everyone for every minor breach!

SURELY BREXIT MEANS GDPR WON'T APPLY TO THE UK?

The United Kingdom's withdrawal from the European Union does not affect GDPR at all.

The UK Government accepted GDPR in full and recognised that we are going to be part of Europe for at least the next 2 or 3 years and would therefore be subject to GDPR. Added to that was the realisation that, if we are going to continue doing business with Europe after Brexit, we will still need to be GDPR compliant. To that end, the government has announced that they will be enacting the Data Protection Bill which will encompass all the GDPR legislation into UK law, meaning that even after Brexit we will still have exactly the same legislation as GDPR[7].

"GDPR IS COMING IN MAY 2018"

This is not strictly true. GDPR was actually enacted back in 2016 but, across Europe, we were all given a 2 year 'grace' period in which to get ourselves fully compliant with the new rules before they start to be enforced.

So, far from coming into effect from May 25th 2018 as is frequently stated, GDPR already exists and is going to be enforced from that date. This means that everyone that processes personal data has to be fully compliant with GDPR by the 25th May 2018 or face the potential consequences.

PART 2

GDPR AND ITS PRINCIPLES

WHAT DOES GDPR ACTUALLY DO?

GDPR does a few things:

- It defines what is meant by 'personal data'
- It confers rights on 'data subjects'
- It places obligations on 'data controllers' and 'data processors'
- It creates principles relating to the processing of personal data
- It provides for penalties for failure to comply with the above.

WHAT IS 'PERSONAL DATA'?

The definition of personal data under GDPR, is given as being:

> *"Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*[8]

In effect, this has increased the definition that was there under DPA so that it also includes such things as IP addresses, biometric data, as well as genetic data etc. to reflect how these can also be used to identify someone and therefore are 'personal data'.

It should be noted that this relates to any personal data processed using computers etc. but also covers personal data contained within any kind of filing system too, even paper based files.

GDPR has also extended the definition of 'sensitive personal data' which requires even more protection than 'personal data'. Sensitive personal data includes data relating to the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life
- Sexual orientation.

Schools should be careful when handling sensitive personal data, especially if it's necessary to share it with other organisations, to ensure it is adequately protected at all times.

WHAT RIGHTS DO DATA SUBJECTS HAVE?

Data subjects – the living individual that the personal data being processed relates to – have the following rights under GDPR:

- The right to be informed – this means that they must be told what data you are using, why and for what purpose
- The right of access – they have to be allowed to see what data of theirs you are processing if they request it
- The right of rectification – if their data is wrong, you have to correct it

- The right to erasure – they can demand that you erase all data of theirs that you have
- The right to restrict processing – they can demand that you stop using their data unless you have a legitimate legal basis for continuing to do so
- The right to data portability – they can decide to move their data to another processor and you have to provide them with all their data so they can do this
- The right to object – they can object to your use of their data and you must stop using it unless you have an overriding legitimate reason to continue
- Rights in relation to automated decision-making or profiling – they can demand that automated decisions about them are reviewed by a human.

WHO ARE DATA CONTROLLERS AND DATA PROCESSORS?

The Data Controller is the person or organisation which determines the purposes and means of the processing of personal data. In the UK education landscape this would be the school themselves, other than in Scotland where the Data Controller of school level data is actually the local authority.

GDPR stipulates that the Data Controller shall:

"Be responsible for, and be able to demonstrate, compliance with the principles."

In effect, what this means is that a Data Controller not only has to comply with 'the six principles' of GDPR (detailed below) but must also be able to evidence how they do so.

The Data Processor is the person or organisation which processes the personal data on behalf of the controller. In the world of education, examples of this would be the MIS provider, cashless catering supplier, library system supplier, or any other third-party supplier that uses pupil, parent or staff personal data to provide the school with services or products. The school determines which supplier they will use and what data these suppliers can use to provide their services.

WHAT OBLIGATIONS DO CONTROLLERS AND PROCESSORS HAVE?

To comply with GDPR, Data Controllers are obligated to determine:

- The legal basis for collecting data
- Which items of personal data to collect
- The purpose(s) the data is to be used for
- Which individuals to collect data about
- Whether to disclose the data and, if so, to whom
- Whether subject access and other individual's rights apply
- How long to retain the data.

Data Processors also have obligations which must be set out in a legal contract which ensures that the processor:

- Processes the personal data only on documented instructions from the controller
- Ensures their staff involved in processing the data observe confidentiality
- Takes appropriate security measures to protect the data
- Helps the Data Controller by using appropriate technical and organisational measures
- Helps the controller to ensure compliance
- Returns or deletes all the data at the end of the contract
- Provides the controller with all information necessary to demonstrate compliance.

Schools can no longer merely sign a supplier's order form – they need a legally binding contract in place that stipulates all the above or they are not legally allowed to use the processor at all.

School suppliers that use personal data from the school – whether on pupils, parents, staff, governors, volunteers etc. – will need to review their contracts to ensure they meet these requirements and re-issue them as necessary.

THE SIX 'PRINCIPLES' OF GDPR

GDPR stipulates six data protection principles that we all have to adhere to when processing personal data to ensure that it is:

1. PROCESSED FAIRLY, LAWFULLY AND IN A TRANSPARENT MANNER

As Data Controllers, you have to ensure that the personal data you are collecting, storing, using, sharing or processing in any way is being done so fairly and lawfully. You must have a legal basis for using the data and have made sure the data subjects are aware of the fact that you are using their data. You must understand:

- What personal data you are using
- What specific purpose you are using it for
- If it is to be shared, details of who it is to be shared with (name of the company/supplier etc.)
- How long it will be stored for and/or processed
- The identity of the Data Controller (usually the school, but in Scotland the local authority)
- Name and contact details of the Data Protection Officer
- Their subject rights and how to exercise these.

This last one is important as Article 11-2 of GDPR states:

> *"The controller shall facilitate the exercise of data subject rights."*

This means that, as well as telling data subjects what their rights are, you must explain how they can exercise these – by complaining to the ICO, making a Subject Access Request, having incorrect data erased or rectified etc.

2. USED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

This means that once you have explained to the data subject what data you are using and why, you cannot then decide to use that data for another purpose without first making them aware of this. It also means that you cannot use any form of 'blanket' basis for processing. In other words, you can't simply say that you are going to use their data for whatever the school needs.

A school scenario here could be that you tell the data subject (pupil or parent depending on pupil's age) that you are going to be using their personal data within the behaviour software that the school uses, which is supplied by XYZ Ltd. This is a specific, explicit and legitimate use of their personal data within the school.

You then decide to buy an online homework system from ABC Co. and use the pupil's personal data for that too. In this case, if you do not explain this to them before using it in the new software, you would be in breach of GDPR because the data is not being used for the specific purpose that you had previously given.

3. USED IN A WAY THAT IS ADEQUATE, RELEVANT AND LIMITED

What is meant here is that you should ensure you use as much personal data as is required for the specific purpose and no more, especially if you are sharing pupil's personal data with a school supplier.

A school scenario here could be where your behaviour software takes pupil data such as name, age, class, teachers etc. This is fine because the data is relevant to the use, adequate for the purpose and limited to only what is necessary. However, if the same supplier then started taking additional data items, such as parental contact details or telephone numbers. This would be a potential breach of GDPR since there is no obvious reason for that data to be used for behaviour systems and therefore the data is not relevant to the purpose, nor is it being limited to what is needed.

4. ACCURATE AND KEPT UP-TO-DATE

We all know how difficult it can be to keep contact data, medical data etc. up-to-date when so many parents forget to inform schools when things change.

The personal data must be accurate when it is obtained – so schools need to consider how they can verify this - and also needs to be kept up-to-date too.

Consider this scenario. You use a parental communication system which syncs with your MIS to get the required parental contacts, phone numbers and email addresses but, unfortunately, when the parent's mobile number was entered it was mistyped. An easy mistake to make which occurs in schools all the time.

The school sends a message out to this parent about their child's behaviour resulting in a message going to the wrongly entered mobile number, owned by someone not connected to the school at all and therefore someone that should not be receiving the information.

Fortunately, this person contacts the school to let them know they have the incorrect mobile number. The school tries to contact the parent to update their mobile number but cannot get in touch with them for several days. During this period, more messages go out and are received by the wrong person again.

This represents a data breach under GDPR! The school should have erased the incorrect number as soon as they were informed of the error rather than waiting until they were able to contact the parent concerned. This led to the data being inaccurate and also not up to date, the school knew yet failed to take appropriate, timely action.

5. KEPT NO LONGER THAN IS NECESSARY

Personal data must only be retained as long as it is required for the processing specified. Once it is no longer needed it should be securely erased unless there is a legitimate reason to keep it – such as legal requirements, the need to retain financial records etc.

In secondary schools, guidelines suggest that the majority of pupil data should be retained until the pupil reaches 25 years of age, except in special circumstances. In primary schools, guidelines suggest that the data should be retained whilst the pupil is attending the school and then should move with the pupil to their next educational establishment.

In schools, there needs to be a clear data retention policy which is adhered to but unfortunately there are often large amounts of personal data that are retained within administrative software well beyond the guidelines. Think about your school management information system – how far back does the data go?

6. PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF THE DATA

Personal data has to be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.

Technical measures could include firewalls to prevent unauthorised access, encryption of the data in any software the school uses or strong passwords in place that are forced to be frequently changed.

Organisational measures are those that help us to ensure staff don't cause data breaches, such as policies and procedures around use of the personal data in school, access controls so that only those staff who actually need the personal data can access it, no more access than is required for the role, as well as clear screen / clear desk policies etc.

A simple school scenario could be where an authorised member of staff is accessing personal, sensitive data on a pupil and gets called away, but leaves their PC screen open to view. Another member of staff passes by, who is not authorised to view the data, but does so. Again, this is a clear data breach!

Either there was no 'clear screen policy' in place, or the policy was not followed by the authorised member of staff, perhaps because of a lack of data protection awareness training or simple carelessness. Both are failures by the school to implement the appropriate organisational measures to protect the personal data against unauthorised processing – in this case access by an unauthorised staff member.

THE PENALTIES FOR FAILING TO COMPLY WITH GDPR

These are now a maximum of 20 million Euros or 4% of the organisation's total global turnover, whichever is the higher.

There are two tiers of fines – the higher tier for the really serious offences such as using personal data without consent or other legal basis.

The lower tier, with maximum fines of half the upper tier, is for less serious failings such as failing to have adequate records of processing, not conducting impact assessments etc.

However, as we touched on earlier, these maximum fines will be for the really serious cases only and then only where the organisations involved are very large and more significant fines are considered appropriate to help persuade them to change their behaviour.

In practice, the ICO has other enforcement powers as well as the ability to issue fines and is likely to make greater use of these, including the ability to issue warnings of non-compliance, carry out audits on organisations to check their compliance, require you to take specific actions within a specified timeframe, order you to erase data etc.

Whatever enforcement the ICO imposes is not the only issue for the organisations that have infringed the GDPR rules. All these enforcements are published on the ICO website and are therefore publicly available. So in addition to any penalty, whatever that may be, you will also have your 'name in lights' on their website and risk having the issue covered by the press, which could cause a great deal of embarrassment and loss of credibility, not to mention inevitable questions and Subject Access Requests from concerned parents.

PART 3

KEY CHANGES AFFECTING SCHOOLS

There are quite a few key changes under GDPR that we need to be aware of in schools and ensure we comply with. These are discussed below:

THE NEED TO IDENTIFY AND RECORD THE LEGAL BASIS FOR PROCESSING DATA BEFORE IT IS PROCESSED.

Before any personal data is processed, the data controller has to identify what legal basis they are using to process the data and ensure this is recorded. There are six legal bases that a data controller can consider and record:

1. CONSENT HAS BEEN OBTAINED FROM THE DATA SUBJECT

In schools, there should be few occasions when it is necessary to obtain consent since the vast majority of the processing of personal data within schools will fall under the basis of 'public interest', discussed below.

2. NECESSARY FOR THE PERFORMANCE OF A CONTRACT WITH THE DATA SUBJECT

This legal basis is designed for situations where there is a legal contract between the data controller and data subject where processing of the data subject's personal data is required to fulfil the contract.

An example would be where you order a sofa from a supplier and pay for it by credit or debit card. The data controller is the store you are purchasing from but they will have to pass your personal data to the card company in order to complete the contract to purchase the sofa and to the delivery company in order that they can deliver it to you. They do not need to ask your consent for this as it is necessary for the performance of their contract with you.

3. NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION

Think of payroll for your employees – it is a legal obligation to pass their personal data to HMRC for tax purposes.

4. NECESSARY TO PROTECT THE VITAL INTERESTS OF A DATA SUBJECT OR ANOTHER PERSON

Here we are talking about critical situations where there is no time to obtain consent. An example would be where you have been badly injured and need an emergency operation. You are unconscious so cannot give consent but will die or suffer badly if the operation does not go ahead. Your doctor or a relative could release details of your blood type to enable the operation to go ahead to save your life.

5. NECESSARY TO CARRY OUT TASKS IN THE PUBLIC INTEREST

This is the legal basis that will apply to the majority of processing of personal data by schools.

A school is considered to be a public body and it is obviously in the public interest that we operate schools and educate our children. Accordingly, for all the common tasks carried out by schools we do not need to ask for the data subject's consent but rather we can use 'public interest' as our legal basis for processing the appropriate personal data.

This would cover our use of personal data for all the everyday tasks within schools – operating a curriculum, storing personal data about our pupils, their parental contacts, staff, timetable information, cashless catering, library systems, the annual census requirements.

However, there could well be some situations where we might need to obtain consent to process personal data or, at the very least, consider whether we need consent.

These could include situations where we share personal data with third party suppliers. If these are for everyday functions of a school that would be expected by any reasonable person, then 'public interest' is fine. If, on the other hand, the third party supplier is providing a service that might not be expected to be part of everyday school life, then consent would be necessary.

For example, let's look at school photographs.

It's common for schools to appoint a local photography company to come in and take the pupils' photographs with the intention of selling these to parents. The photographer takes the photos, produces them and delivers them to the school which then sends a photo package home with the pupils and the parent decides what they want to order before sending the monies back to the school. No personal data is being passed to the photographer other than the image of the pupil which any reasonable person would expect as the photos could not be taken otherwise.

An alternative process might be that, in order to avoid having to handle orders and cash, the school passes the parents email addresses to the photography company who in turn emails the parents with details of the photos and allows them to order directly. In this case, the school has shared personal data (email addresses and names, parental relationships etc.) with the photography company – is that something the parents would have expected?

The same consideration needs to be given where you share personal data with other schools, third party suppliers etc. Is the sharing of this personal data with this other party for that purpose something the data subject/parent would expect? If not, or if you are in any doubt, then you should obtain consent before you share the data.

6. NECESSARY FOR THE PURPOSES OF LEGITIMATE INTERESTS PURSUED BY THE DATA CONTROLLER OR A THIRD PARTY

This is similar to the 'public interest' basis above, but for private companies etc. This legal basis cannot be used by public bodies, such as schools, in the same way that 'public interest' cannot be used by private organisations.

CONSENT CONDITIONS HAVE BEEN STRENGTHENED CONSIDERABLY.

If the legal basis used is consent, this brings in a whole host of additional rules and requirements that could cause issues in school situations.

For instance, consent must be freely given – but GDPR specifically mentions the potential for 'imbalance' between the Data Controller and the data subject which could mean that any consent is not, in truth, freely given because the data subject feels compelled to give it. If you consider the fact that the school and school staff are seen as being in an authority position in a school situation, you can easily see how there could be an argument that consent was not in fact given 'freely'...

Consent must also be specific (i.e. the exact purpose for the processing must be clearly explained), informed (the data subject must be told about it and understand what the data is to be used for) and it must be an unambiguous indication of the data subject's wishes.

Consent under GDPR has to be in the form of a clear, affirmative action. This means that there can be no pre-ticked boxes and consent cannot be inferred from silence or inactivity (no phrases such as '...if we do not hear from you we will assume you consent).'

Also, consent has to be completely separate from any other terms and conditions – this it to prevent consent being 'lost' in amongst a 30-page set of terms and conditions.

Equally important is the fact that, if consent is used as the legal basis for processing, this consent would need to be from the pupil's parent whilst the pupil is under 13 (as laid out by the government in the recent Data Protection Bill announcement which brings GDPR into UK law8) but from the pupil themselves once they reach 13 years. Schools using consent will therefore need to have a process in place to identify when a pupil reaches 13 years of age and then obtain their own consent for the processing based upon the consent previously obtained from their parents. This poses an important question relating to what a school should do if a pupil refuses to give consent.

Additionally, if processing is based on consent, that consent can be withdrawn at any time and the processing must immediately be halted. It must be as simple for the consent to be withdrawn as it was to give it in the first place. If schools do use consent as their legal basis for any processing, they will need to have a process in place to handle withdrawn consent and halt the processing of that person's personal data.

Perhaps one of the biggest issues around using consent as the legal basis is the fact that this needs to be verifiable. In other words, if someone denies having given consent would you be able to produce some form of proof that they had indeed given it?

If you have already obtained consent, this will need to be reviewed to ensure that the consent you have already obtained meets the requirements for consent under GDPR. If not, then you will need to get it again...

Consent as the legal basis should be something that all schools strive to avoid wherever possible and only use where there is no other suitable legal basis available to them.

DATA BREACHES MUST BE NOTIFIED TO THE ICO WITHIN 72 HOURS.

Under the DPA, notification of data breaches to the ICO was voluntary rather than mandatory. This is not the case under GDPR.

Now, all data breaches which have the potential to have a significant detrimental effect on the individual(s) through discrimination, damage to reputation, financial loss, loss of confidentiality or any other economic or social disadvantage must be reported by the data controller to the ICO within 72 hours of discovery.

This means that if a data breach was discovered at 3.45pm on Friday afternoon, you have until 3.45pm on Monday to report this to the ICO. The report has to have full details of the data breach, who could be affected, what data is at risk and what you have done to minimise the impact.

If the breach is potentially a 'high risk' to the individual(s) affected then the school must also notify the data subject(s).

Data breaches occur for a wide variety of reasons including loss or theft of equipment, unauthorised access to data, unforeseen circumstances such as fires or flooding and the majority are caused by mistakes or carelessness rather than hacking or viruses.

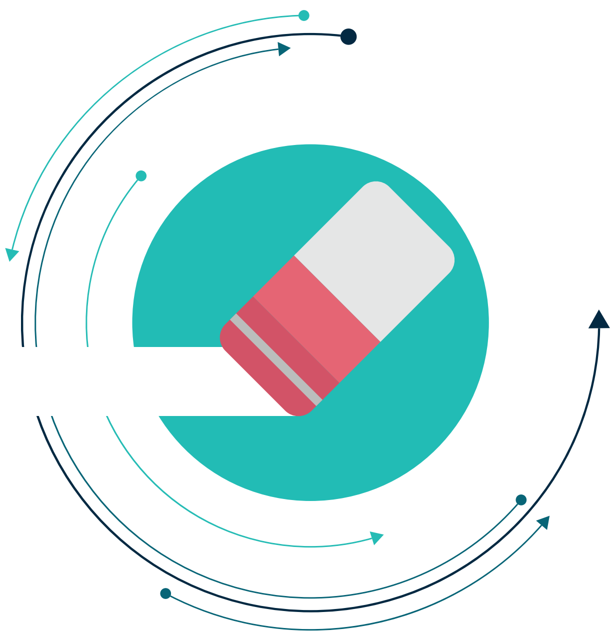
Schools need to have a robust process in place to ensure that they can identify data breaches, investigate the cause, respond quickly and implement measures to prevent recurrence.

INDIVIDUALS HAVE AN INCREASED RIGHT OF ACCESS TO THEIR DATA AND ITS USE.

All individuals will have a right to obtain confirmation that the Data Controller is processing their personal data. They will be able to demand access to all their personal data that you are processing including what data you are processing, why you are processing it, who it is being shared with, how long it is being retained etc.

If you receive a Subject Access Request (SAR) you must supply all the data to the individual within one month – and you are no longer able to charge for doing so.

With this now being free of cost, coupled with the fact that GDPR is gaining widespread press coverage etc. schools should expect to see a far larger number of these requests than previously and will need to put a process in place to ensure they can handle increased numbers within the one-month window allowed.



UNDER GDPR, INDIVIDUALS WILL ALSO HAVE THE 'RIGHT TO BE FORGOTTEN', ALSO KNOWN AS 'DATA ERASURE'.

Where the personal data is no longer required for its original purpose, their consent has been withdrawn or they object to the processing, an individual can demand that the processing is stopped and all their personal data is erased by the Data Controller, including from any processors the controller has shared this data with.

Individuals have this right under DPA but only if the processing of their personal data causes them unwarranted or substantial damage or distress. Under GDPR they do not have to have any reason at all, they can simply demand that all their data is erased and unless you can prove that there is a valid reason to continue processing it, you will need to ensure that it is deleted without delay.

Again, schools will need to have a process in place to ensure that, if they do receive such a request, this can be achieved. Remember, this would include any personal data shared with processors (library systems, MIS, cashless caterers or any other suppliers) that you use.

As with Subject Access Requests, you will need any suppliers that you share data with to be able to assist you in meeting these requirements, so you will need to ask them to confirm that they can do so.

GDPR REQUIRES DATA CONTROLLERS TO BE ACCOUNTABLE FOR THE PERSONAL DATA THEY PROCESS.

The GDPR states:

> *"The Controller shall be responsible for, and be able to demonstrate, compliance with the principles."*

This means that not only do we all have to comply with GDPR we also have to be able to evidence this too.

Schools will need to ensure they have a good governance process in place to record the measures taken to protect the personal data under their control and to comply with the GDPR requirements.

This will require regular staff training around the subject, keeping accurate records of processing, regular and documented monitoring and audits etc.

'PRIVACY BY DESIGN' WILL BECOME A LEGAL REQUIREMENT UNDER GDPR.

Privacy by design means ensuring that the protection of any personal data is considered at the very outset of any new processes or technologies that we intend to implement rather than being something that is thought about at a later stage.

Whilst privacy by design has been best practice for some time, it now becomes a legal requirement under GDPR.

It will mean staff training to evidence that they have been taught about this; conducting Privacy Impact Assessments (often known as Data Protection Impact Assessments - DPIA) to assess any risks involved in the processing and putting in place measures to reduce these risks; providing appropriate resources to implement the measures etc.

Schools will need to see the DPIAs (or summaries of them) conducted by their suppliers if they are sharing data with them, to ensure that they can evidence that this was considered and prove their compliance.

DATA PROTECTION OFFICERS NEED TO BE APPOINTED.

Schools (other than maintained schools in Scotland) will need to appoint a Data Protection Officer (DPO).

The DPO has three main responsibilities:

1. To advise and inform the school and its staff about their obligations to comply with GDPR and any other data protection legislation
2. To monitor the school's compliance with GDPR, train staff, conduct audits etc.
3. To be the first point of contact with the ICO and data subjects.

GDPR states that the DPO must report to the highest level of management, be independent and not penalised for doing their job and be provided with adequate resources to perform their tasks.

On top of that, the DPO must have professional experience and knowledge of GDPR and data protection law and must have no conflict of interest.

These last two requirements make it difficult to see how a school employee could fulfil the DPO role. The obvious choice would usually be the Network Manager – but that definitely brings in a conflict of interest. How can the person responsible for implementing technology in the school also monitor themselves?

Fortunately, the DPO does not have to be an employee of the organisation nor does there need to be a separate DPO for each school/organisation.

The DPO could be a current employee if the above criteria can be met but could also be a newly recruited role, an external party contracted in or someone provided by the local authority.

One DPO could be responsible for a number of schools provided they are available when needed and have sufficient time and resources to cover the schools adequately.

Whatever decision is taken around who your DPO will be, action should be taken as soon as possible so that he or she can be appointed in time to help you become compliant before May 25th 2018.

PART 4

12 STEPS TOWARDS GDPR COMPLIANCE

There is a great deal to be done in order to become compliant, so schools are advised to start as soon as possible. The following twelve steps are a good place to start:

1. AWARENESS

Make certain that your SMT, Governors etc. appreciate the impact GDPR is going to have on the school and the resources they might need to provide to become compliant.

2. INFORMATION YOU HOLD

Start to document what personal data you hold and process, where it comes from and who you share it with. Produce your data flows so that you can see clearly what personal data is moving through the school systems and where it ends up.

3. PRIVACY NOTICES

Review and update what you have already in place and plan for any necessary changes. Often schools put this information into the parent/pupil/school contracts and then ask the parent/pupil to sign to give their consent. This should be changed so that you are not relying on consent but rather are processing the personal data under the legal basis of public interest, wherever possible, to prevent issues around consent being withdrawn.

4. INDIVIDUAL'S RIGHTS

Consider all the personal data you hold or process and ask yourselves if you comply with the data subject's rights. Can you deal successfully with data erasure requests or withdrawn consent?

5. SUBJECT ACCESS REQUESTS

Update or develop procedures for SARs so you are ready to handle them within the time constraints outlined. Make sure you have someone responsible for dealing with these and a second person to cover in the event of absence so that there are no delays.

6. LAWFUL BASIS FOR PROCESSING

Identify the legal basis for your processing of personal data. Document the legal basis and update privacy notices to explain it. In the majority of cases, the legal basis will be public interest so be sure to state this in your privacy notices.

7. CONSENT

If you need consent for any processing, work out how you are going to get it, record it and refresh existing consents etc.

8. CHILDREN

Parental consent up to 13 years of age, thereafter the pupil's own consent. How are you going to manage this?

9. DATA BREACHES

Do you have procedures in place to deal with these if they occur? Whose responsibility will it be to handle them?

10. PRIVACY IMPACT ASSESSMENTS

As well as being a requirement for any new technologies or high-risk processing, it is good practice to have these for all processing and then update if your processes or technology change or new processing / suppliers are being considered.

11. DATA PROTECTION OFFICER

Appoint ASAP so they can help you fully prepare for in time for the GDPR deadline.

12. INTERNATIONAL

Do you know where the personal data is going? There are strict rules around moving personal data outside the EEA so make sure you find out where the personal data is held by your suppliers. If you use Cloud software, where is this hosted?

Taken from the ICO's "12 steps to take now" adapted for schools, courtesy of GDPRiS.

PART 5

CONCLUSION AND OTHER CONSIDERATIONS

CONCLUSION

In preparing for the GDPR we should not lose sight of what this new law is about. In our new digital world, it's about delivering greater transparency, enhanced rights for employees and pupils and increased accountability.

Remember, whilst GDPR is bringing in a number of changes and will be the most robust data protection legislation we have ever seen, it is also an opportunity to review your current data protection practices and update them so that you can demonstrate that your school understands the need to protect sensitive information and you are doing all you can to ensure any personal data you hold is looked after adequately.

Don't believe the scaremongering. Yes, there is a great deal to be done, but if your staff have undertaken GDPR training, you keep good records of policies, procedures and contracts with suppliers, conduct data protection impact assessments and take thorough risk minimisation measures, you'll be well on your way to compliance.

GDPR TRAINING

Groupcall is running CPD-certified GDPR training courses across the UK to support schools in their journey to compliance.

These sessions are designed for school senior leaders, data protection leads, compliance and governance officers, data managers, data officers, data architects, data specialists, chief executives and directors from schools, LAs and MATs.

On completion of this instructor-led course, delegates will have:

- A thorough understanding of the new GDPR and its impact on your organisation
- Awareness of the requirements GDPR will impose on you
- Gone through the steps you need to take to ensure your organisation is compliant
- Learned how to ensure your suppliers are GDPR compliant
- Practiced practical skills you can apply in your own organisation.

TO REGISTER FOR A TRAINING COURSE NEAR YOU, VISIT GROUPCALL.COM/GDPR-TRAINING

ENSURING COMPLIANCE WITH GDPR IN SCHOOLS (GDPRIS)

GDPRiS is a complete GDPR management solution specifically developed for schools. It's designed to reflect existing processes and the way schools work, whilst pro-actively prompting you to meet and exceed the new Regulations.

GDPRiS documents data flows, helps map and audit all personal data and prompts the use of Self-Assessment Questionnaires (SAQs). It helps guide all school staff to a new level of data protection understanding.

GDPRiS is easy to use, making it an invaluable tool for schools looking to achieve full GDPR compliance:

- Centrally manage GDPR across single or multiple schools
- Manage 3rd party suppliers that process data
- Streamline SARs & data breach reporting
- Store policy documents, training records & materials
- Provide an SAQ to all staff to ensure full accountability
- Access practical guidance on GDPR compliance
- Demonstrate commitment to manage data sensitively & ethically.

FOR MORE INFORMATION ON GDPRIS, TO ARRANGE AN ONLINE DEMONSTRATION OR REQUEST A QUOTE, PLEASE VISIT GROUPCALL.COM/GDPR

PART 6

BIBLIOGRAPHY AND FURTHER READING

BIBLIOGRAPHY

1. **WANNACRY RANSOMWARE ATTACK.**

   https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

2. **TALKTALK HIT WITH RECORD £400K FINE OVER CYBER-ATTACK.**

   https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack

3. **TALKTALK HIT WITH RECORD FINE OVER CYBER ATTACK.**

   https://www.ft.com/content/15ea6930-8b07-11e6-8aa5-f79f5696c731

4. **GDPR – SORTING THE FACT FROM THE FICTION.**

   https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/

5. **GOOGLE SEARCH STATISTICS.**

   http://www.internetlivestats.com/google-search-statistics/

6. **GDPR TO PLACE EXTRA BURDEN ON ICO, SAYS COMMISSIONER.**

   http://www.computerweekly.com/news/450414588/GDPR-to-place-extra-burden-on-ICO-says-commissioner

7. **GOVERNMENT TO STRENGTHEN UK DATA PROTECTION LAW.**

   https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

8. **ART. 4 GDPR DEFINITIONS.**

   https://gdpr-info.eu/art-4-gdpr/

FURTHER READING

9. **GETTING READY FOR THE GDPR**

   https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

10. **UK DATA PROTECTION BILL STATEMENT OF INTENT**

    https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

11. **OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION (GDPR)**

    https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

12. **RESOURCES FOR SCHOOLS**

    https://ico.org.uk/for-organisations/education/resources-for-schools/

13. **ICO INFORMATION RIGHTS VIDEO FOR SCHOOLS**

    https://www.youtube.com/watch?v=xtLR0Ey5-vo&feature=share&list=UUFVNJT2oNNsVr2hY2KYWszQ

For more information on how Groupcall can assist your school prepare for GDPR, please visit:
www.groupcall.com/gdpr
e-mail **gdpr@groupcall.com**
or call **020 8506 6100**

groupcall™

built on **trust**

GROUPCALL LIMITED
COMMERCE HOUSE,
1 RAVEN ROAD,
SOUTH WOODFORD,
LONDON E18 1HB

T: 020 8506 6100
E: GDPR@GROUPCALL.COM
W: WWW.GROUPCALL.COM/GDPR