Firebird
Data Protection Consultancy Ltd

General Data Protection Regulation (GDPR) Short Guide *for schools*

What is it?

The GDPR (EU General Data Protection Regulation 2016) came into effect on the 25 May 2018. It is designed to protect and empower European citizens with regard to the handling of their personal data. It enhances people's rights and places greater obligations and sanctions on organisations.

The UK's Data Protection Act 2018 provides additional duties and is supplementary to the GDPR. UK organisations will still be required to comply with the GDPR when the UK leaves the European Union.

Main changes affecting schools

1. Data Protection Officers *(Articles 37-39, GDPR)*

All public authorities (maintained schools and academies) must appoint a Data Protection Officer (DPO). Independent schools that process 'special categories' (i.e. sensitive) personal data on a large scale, may also be required to appoint a DPO.

DPOs can be an existing employee or schools can appoint an external person to fulfil this role. The individual is required under the new law to have *"expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR"**

The DPO must have the freedom to carry out the role independently and cannot have a conflict of interest. The DfE suggests this post should **not** be carried out by the Headteacher, IT Manager or person involved in school policy.

*Article 29 Data Protection Working Party Guidelines

2. Data controller obligations
(Articles 24-32, GDPR)

There are several new obligations for schools to fulfil under the GDPR. These include:

- ***Data protection policies and training*** - You need effective data protection policies, procedures and regular employee training.
- ***Written contracts with suppliers*** - Schools are required to assess the suitability of all suppliers and contractors who process personal data on their behalf and have written contracts in place.
- ***Record of processing activities*** - Schools need to identify and record what categories of personal data they are processing; why; how long it is kept for; who it is shared with and a brief description of the security measures they have in place to keep it safe. This document must be provided to the Information Commissioner's Office or the public upon request.
- ***Technical and organisational measures*** - Proportionate and adequate technical security measures, policies and procedures need to be implemented to ensure data protection compliance is built into everyday practices.
- ***Data protection impact assessments*** - Data protection impact assessments (DPIAs) must be carried out prior to any processing of personal data which could result in high risks to the rights and freedoms of data subjects.

Firebird
Data Protection Consultancy Ltd

Data Protection Impact Assessments

Carry out an assessment (DPIA) if you plan on doing the following:

- Install CCTV cameras
- Store personal data in the Cloud
- Use new technology which involves personal data
- Process sensitive or highly personal data (e.g. health data, religious beliefs, a person's sexual orientation)
- Process information about vulnerable people
- Obtain or use biometric data (e.g. fingerprints)
- Process personal data on a large scale
- Process personal data that could endanger a person's physical health or safety in the event of a security breach
- Use profiling or special category data* to decide on access to services.

This list is not exhaustive

Your DPIA should:

- describe the nature, scope and reasons for the processing
- assess the necessity, proportionality and compliance measurers in place
- identify and assess the potential risks to individuals
- identify the measures that will be taken to reduce the risks
- be kept under review and revisited

DPIAs are usually carried out by the project lead; the Data Protection Officer should be consulted during the assessment process along with any other experts e.g. your IT lead.

*Special category data are listed in Article 9, GDPR

3. Data breaches (Articles 33-34, GDPR)

Schools must investigate and document all breaches of security involving personal data.

There are 3 types of personal data breaches to look out for:

1. Confidentiality breach:
*Unauthorised or accidental **disclosure** or **access** to personal data.*

2. Integrity breach:
*Unauthorised or accidental **alteration** of personal data.*

3. Availability breach:
*Unauthorised or accidental **loss of access** or **destruction** of personal data.*

If the breach is likely to result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, the school must notify the Information Commissioner's Office (ICO) within **72hrs** of becoming aware of the breach.

Data subjects must also be informed if they could suffer 'high risks' as a result.

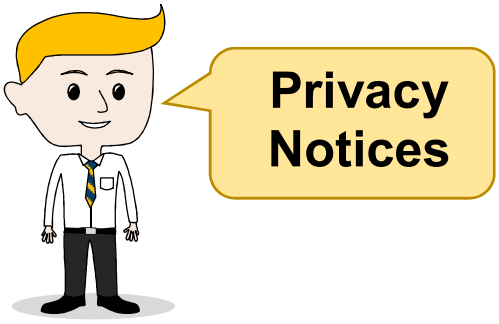
Examples of **high risks** include:

- Identity theft
- Physical harm
- Humiliation
- Reputational damage
- Psychological distress

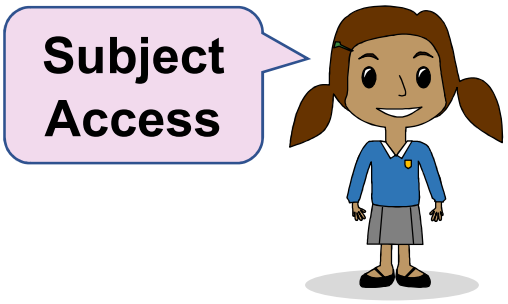
Data subjects must be informed *'without undue delay'* when the school becomes aware of a high-risk breach, so they can protect themselves where necessary.

4. People's rights

• *Transparency & information* (*Articles 12-14, GDPR*)
There are new requirements to publish more information in Privacy Notices – these include the contact details of your Data Protection Officer; the purpose and lawful basis for processing personal data; how long you keep data for; who you share it with and what rights people have. Privacy notices must be clear and accessible. Schools are recommended to publish these on their website, include in their pupil admission packs and provide during employee induction.



• *Access to personal data* (*Article 15, GDPR*)
This right entitles pupils, parents/guardians, governors and anyone else the school holds information about, to receive a copy of that information without charge, within one month. Maintained schools have additional duties under The Education (Pupil Information) (England) Regulations 2005 and must provide education files to parents/guardians within 15 pupil days.

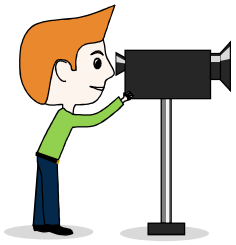


• *Rectification and erasure* (*Article 16-17, GDPR*)
Individuals are entitled to have inaccurate personal data rectified or incomplete information completed and have their personal data deleted in cases where the data is no longer needed or if the individual withdraws consent. This right does not require a school to delete data upon request, if the school is complying with a legal obligation in holding it, for example if the school is required under statute to collect and retain the data for a certain length of time.

• *Object to direct marketing* (*Article 21, GDPR*)
By default, people have the right not to receive direct marketing. Schools must obtain explicit 'opt-in' consent before sending out marketing material. This will be relevant where schools target individuals for fundraising, advertise their school prospectus or send out advertising literature for other organisations.

• *Compensation* (*Article 82, GDPR*)
Individuals are entitled to compensation for any damage or distress suffered as a direct result of an organisation breaching the GDPR. Schools should therefore review their practices for handling personal data to ensure they comply and reduce the risk of a claim.

5. *Consent* *(Articles 7-8, GDPR)*



There are tighter rules around obtaining consent from adults and children. Most of what schools do involving personal data, do not require consent, unless for example they photograph a school event and publish images of identifiable people, collect and use biometric information, send out direct marketing or fundraising information and so on.

Under the new rules, schools need to demonstrate that consent has been obtained freely, the individual is fully informed and they have *opted-in* to the specific activity. Schools cannot use pre-ticked consent boxes or assume consent has been given, just because the parent or student have not said otherwise. If a consent form is not returned or is left unticked, the school must assume consent has not been given.

Consent forms must be written clearly and in a way that is easy to understand. Different types of processing or use of personal data should be listed separately, so the data subject can indicate their preferences easily in each case.

Schools are required to keep clear records of all consent they obtain, inform individuals of their right to withdraw consent at the time consent is obtained and offer easy ways to do this.

Consent can be sought direct from children (under 18s), providing they have the capacity to understand the implications of their decision. The Department for Education (DfE) suggests* students aged 13+ are likely to have capacity in this regard.

When making any decisions involving children's data, the child's best interests must be the deciding factor.

*DfE Data Protection: Toolkit for Schools

Consent Checklist!

The person must be informed

- ✓ They must fully understand your intentions
- ✓ Be made aware of the likely consequences of giving consent (unless this is obvious)

No ambiguous wording

- ✓ Use clear, plain language when asking for consent
- ✓ Adapt the wording where required for pupils, students and others

Consent must be specific

- ✓ Do not use 'catch all' general consent; itemise/separate out the different activities you would like them to consent to
- ✓ They must indicate their wishes. Consent cannot be inferred from lack of response.
- ✓ They must opt-in to the proposed activity (no opt-outs allowed)
- ✓ You cannot used pre-ticked boxes to gain consent

It must be freely given

- ✓ The individual cannot be coerced
- ✓ You cannot place unfair terms and conditions on them eg *'If you provide consent for your child to attend this trip, you consent to their photograph being published on the activity provider's website*'

They can withdraw consent

- ✓ You must inform them of their right to withdraw consent on the form
- ✓ Tell them how they can withdraw
- ✓ Make it easy for them to do this (provide an email address and phone number)
- ✓ Manage their expectations (e.g. provide a deadline date for you to be able to act on their wishes e.g. before the photograph is published in printed material)

How is your school's GDPR compliance?

The requirements under the GDPR and the Data Protection Act 2018, are often daunting and time consuming for schools to tackle. There's no doubt it takes time, patience, commitment and a good understanding of these laws to achieve full compliance.

As the legislation has been in place for nearly a year, schools are expected to have invested the time and resources into achieving at least a base layer of compliance and have evidence that they are continually reviewing and improving their practices to maintain this.

Data protection compliance is not a one-off project or a 'tick box' exercise, that only needs to be looked at every couple of years when the policy comes up for review. It's something that must be embedded into every day practices, across all roles in the school, from the governing body to senior management, through to teaching and non-teaching staff and even the school's cleaners, as they will have access to printed material containing personal data, which may be left out in offices and classrooms.

The GDPR requires an active role to lead and manage the school's compliance, which is where your Data Protection Officer comes in. The law requires that this person fully understands the data protection laws and has the time, support and resources to review and make the necessary changes in your school.

Quick self-assessment

- ✓ Do you have a dedicated Data Protection Officer who has an in-depth knowledge of the GDPR, the ability to perform the role, the appropriate authority to influence change as well as the time and support from senior management and the governing body?
- ✓ Have you reviewed how you seek, manage and record consent, ensuring that it is freely given, the person is informed, they have positively opted-in to the proposed activity and have been told they have the right to withdraw consent?
- ✓ Do you have policies and procedures in place to manage and respond when individuals exercise their rights and have your staff received training in how to deal with these requests, in particular the exemptions which prohibit the disclosure of some data?
- ✓ Have you communicated separate privacy notices to parents, students, employees and governors, informing them of their rights under the GDPR?
- ✓ Have you carried out an audit to assess your compliance against the GDPR, particularly around your policies and procedures; contracts; risk assessments and technical and organisational security measures?
- ✓ Do you have a record of your processing activities which identifies the personal data you process; the reasons why; the retention period; who you share it with and a brief description of the security measures you have in place?
- ✓ Have you created and implemented procedures for identifying, reporting, managing and investigating personal data breaches and communicated these to all staff?
- ✓ Do you have GDPR training built into your staff induction procedures and is the training provided to existing employees on an annual basis?

Useful Resources

Information Commissioner's Office *(UK Data Protection Regulator)*

- Guide to the General Data Protection Regulation (GDPR)
- Data Protection Self-Assessment
- Data Protection Impact Assessments
- Exemptions under the GDPR and DPA 2018
- Action we've taken - (*Headteacher prosecuted for unlawfully obtaining school children's personal information*)

Website - www.ico.org.uk

2. Department for Education

- Data Protection: Toolkit for Schools
- Data Protection: Annual Review Checklist
- Data Protection: Privacy Notices Model Documents
- Information sharing: Advice for safeguarding practitioners

Website – www.gov.uk

Further Support

Firebird specialises in supporting schools and other education organisations achieve their GDPR compliance. There are several packages to choose from to suit every budget! Further information is available on our website, including testimonials from some of our schools who have purchased our **most popular** outsourced **Data Protection Officer package.**

Website: www.firebirdltd.co.uk **Email:** info@firebirdltd.co.uk

"Absolutely worth every penny! We will definitely be purchasing this service again next year"
Headteacher, Primary School, East Devon

"Amber Badley is so much more than just a Data Protection Officer. She has provided us with a complete GDPR service" **Business Manager, Federation of 5 schools, South Devon**

Working in Partnership with babcock™

Firebird Data Protection Consultancy Ltd