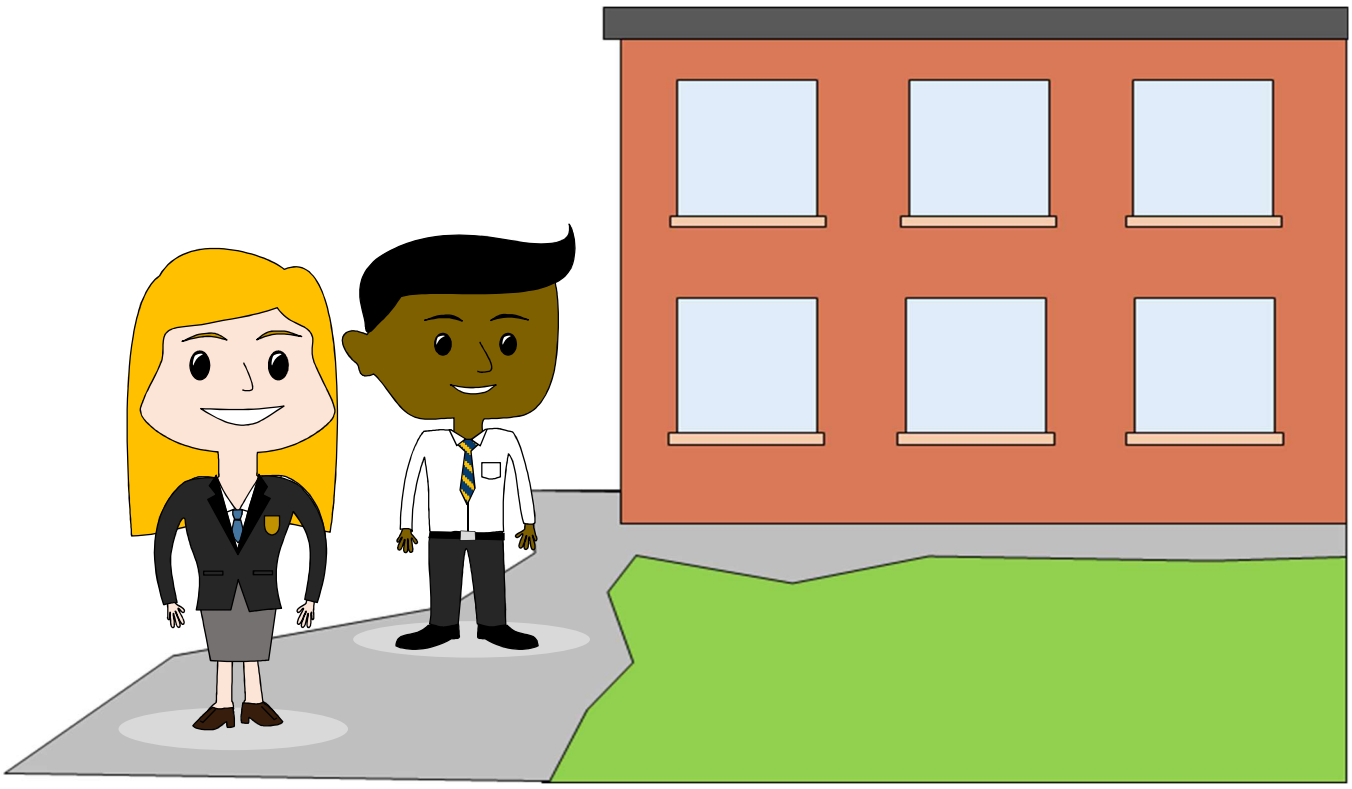
Firebird
Data Protection Consultancy Ltd

Data Protection Obligations:

Short Guide for Schools & Academies



The Data Protection legislation

In May 2018, we saw a big shake up in the Data Protection legislation, resulting in the birth of the EU General Data Protection Regulation 2016 (the GDPR) and the UK Data Protection Act 2018 (the DPA 2018), which came into force the same day as the GDPR. Schools and academies are currently required to comply with **both** pieces of legislation.

The GDPR is legislation which protects and empowers European citizens with regard to the handling of their personal data. It enhances people's rights and places greater obligations and sanctions on organisations that process personal data.

The DPA 2018 supplements the GDPR so that it works in a UK context and provides additional duties and exemptions to some organisations (these relate to public authorities, law enforcement and intelligence services). Both the GDPR and the DPA 2018 must be read alongside each other, to ensure full compliance and understanding of the laws.

GDPR and Brexit

When the UK exits the EU, the GDPR will no longer be law in the UK. However, the work schools and academies have been doing to comply with the GDPR, **will continue to be relevant** after Brexit, as the UK's government will amend the DPA 2018, to ensure it implements the main provisions of the GDPR into our laws.

Schools should therefore **not be concerned** about Brexit and should continue to comply with their existing data protection obligations as these will still apply going forward.

Obligations for schools/ academies

Schools and academies have many obligations under the Data Protection legislation, these are set out in Chapter 4 of the GDPR. The following sections offer a brief overview of these obligations, so you can make an assessment as to whether your school is complying with these:

1. Data Protection Officers

All 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 legislation to have *"expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR"*
(Article 29 Data Protection Working Party Guidelines)

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 a person involved in school policy, therefore Governors are also unlikely to be suitable.

2. Data protection policy and training

Schools/academies must have an effective data protection policy in place, which is communicated to employees and is accessible. Appropriate data protection training must also be provided to employees. The Information Commissioner's Office says this should be provided annually or every 2 years at the latest.

3. Written contracts with suppliers

Schools/academies must assess the suitability of all suppliers who process personal data on their behalf (these are known as 'data processors'), before purchasing their services, and have written contracts in place which contain data protection compliance assurances (*Article 28 GDPR*).

4. Record of processing activities

Schools/academies need to identify and record the 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.

5. Technical / organisational measures

Schools must have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction or damage. This can be achieved by implementing appropriate technical and organisational security measures *(see 'Knowledge Check' section).*

6. 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 data subjects *(see Firebird's 'DPIA: Short Guide for Schools').*

7. Document your data breaches

Schools must investigate and document all breaches of security involving personal data. There are 3 types of 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*

High risk breaches (e.g. likely to result in damage, discrimination, detriment or distress) must be reported to the Information Commissioner's Office **within 72hrs** and data subjects **without delay**!

Knowledge Check!

Technical and organisational security measures

*Examples of **'technical security'** measures:*

- ✓ Having a Firewall, anti-virus and anti-malware software in place.
- ✓ Applying security patches promptly.
- ✓ Restricting access to systems on a 'need to know' basis.
- ✓ Enforcing strong password policies; passwords should be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others.
- ✓ Encrypting laptops, USB/memory sticks and other removable media or portable devices, which store personal data.
- ✓ Regularly backing up data.
- ✓ Regularly testing the school's disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident.

*Examples of **'organisational security'** measures:*

- ✓ Employees sign confidentiality clauses as part of their employment contract.
- ✓ Data protection awareness training is provided to employees during induction and annually.
- ✓ Data protection compliance is a regular agenda item in governing body and Senior Leadership Team meetings.
- ✓ Cross cutting shredders and/or confidential waste containers are used to dispose of confidential papers.
- ✓ The school's buildings, offices and where appropriate classrooms, are locked when not in use.
- ✓ Paperwork is locked in cabinets/cupboards and access restricted on a need to know basis.
- ✓ Security procedures are in place for visitors, such as signing in and out; wearing a visitor's badge and being escorted if no DBS certificate shown.

8. Comply with people's rights

People are afforded many rights under the data protection legislation. Schools and academies must therefore have the appropriate procedures, resources and training in place to be able to comply with these rights when they are exercised.

Transparency & information (Privacy Notices)

Schools must have privacy notices in place which include a description of the personal data it holds about people; the purpose and lawful basis for processing that data; how long it will be kept for; who it might be shared with; what rights people have and the contact details of the school's Data Protection Officer. Schools are recommended to publish these notices on their website, include in their pupil/student admission packs and provide during employee induction. The DfE have template notices on their website at www.gov.uk

Access to personal data (Subject Access Requests)

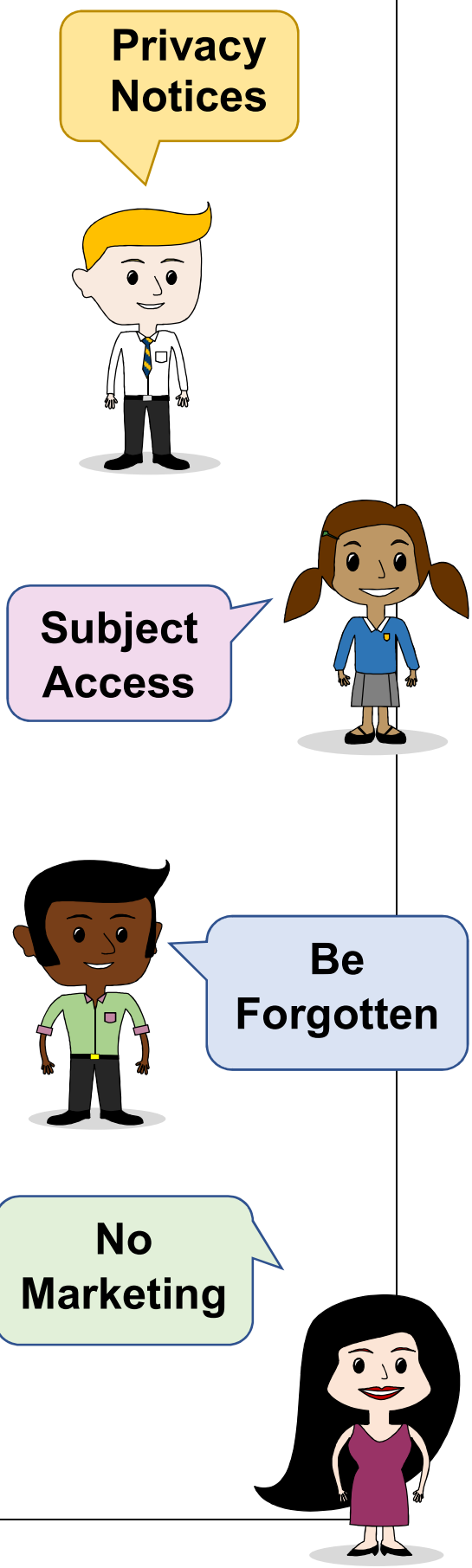
This right entitles students, parents/guardians, governors and anyone else the school/academy holds information about, to receive a copy of their personal data upon request, without charge and within **one month**. Maintained schools have additional duties under The Education (Pupil Information) (England)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

Rectification and erasure

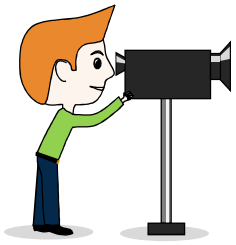
Individuals are entitled to have inaccurate personal data about them rectified or incomplete information completed. They are also entitled to have their personal data deleted in cases where the data is no longer needed or if the individual withdraws consent (where relevant). This right does not require a school/academy to delete data upon request, if they are complying with a legal obligation in holding it.

No electronic direct marketing without consent

People have the right not to receive electronic direct marketing or fundraising communications (e.g. by email, call or text), unless they have explicitly 'opted-in' to receive these. This will be relevant where schools target individuals for fundraising, advertise their school prospectus or send out advertising literature for other organisations.



9. Consent



There are tighter rules around obtaining consent from adults and children. Most of what schools/academies 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, share data with other organisations and so on.

Under the Data Protection legislation, schools/academies need to demonstrate that consent has been obtained freely, the individual is fully informed and they have *opted-in* to the specific activity. Schools/academies cannot use pre-ticked consent boxes or assume consent has been given, just because the parent or student has 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, 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.

The Data Protection Principles

Whenever you process personal data (e.g. collect it, use it, store it or share it), you must comply with the following principles, or your processing may be unlawful:

Personal data shall be:

- processed **lawfully**, **fairly** and in a **transparent** manner
- collected for **specified**, **explicit** and **legitimate** purposes and not further processed in a way that is incompatible with those purposes
- **adequate**, **relevant** and **limited** to what is necessary for the purposes in which they are processed
- **accurate** and where necessary **kept up to date**
- kept for **no longer than is necessary** for the purpose it is processed (personal data can be held for longer periods if this is necessary for **archiving purposes**)
- processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate **technical or organisational measures**

The legislation requires that schools / academies are responsible for and be able to **demonstrate compliance** with these principles. There must be documented evidence of how these principles are being met; this should be referred to within your **Data Protection Policy** and any associated procedures.

*DfE Data Protection: Toolkit for Schools

How is your compliance?

The requirements under the GDPR and the Data Protection Act 2018, are often daunting and time consuming for schools and academies 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 over a year, schools and academies are by now expected to have invested the time and resources into achieving a good level 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 legislation requires an active role to lead and manage the school/academy'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 / academy.

Quick self-assessment

- ✓ Do you have a **dedicated Data Protection Officer** who has an in-depth knowledge of the data protection legislation, 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 data?
- ✓ Have you communicated separate **privacy notices** to parents, students, employees and governors, informing them of their rights under the legislation?
- ✓ Have you **carried out an audit** to assess your compliance against the legislation, 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 security breaches** and communicated these to staff?
- ✓ Do you have **Data Protection 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

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, academies and other education organisations, achieve their data protection 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

"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**