



Full Governors

06.12.23

Signed *EN Smith*

Data Protection

Portway Infant School is committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Portway Infant School will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

What are the UK GENERAL DATA PROTECTION REGULATIONS (UKGDPR)

This is a European Directive that will be brought into UK law with an updated Data Protection Act for May 2018 and remains unchanged by Brexit.

The current Data Protection Act 1998 has been replaced with the Data Protection Act 2018.

What is the purpose of UKGDPR

UKGDPR and new the DATA PROTECTION AUTHORITY exists to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

UKGDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As public bodies, schools have more obligations than some small businesses. It is mandatory to comply with UKGDPR and proposed provisions in the new Act. We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, sexual orientation, genetic data and biometric data, where processed, to uniquely identify a person.

Schools often collect sensitive data for DfE (Department for Education) and LA (Local Authority) requirements and of course pupil data may contain information about safeguarding, SEND or health needs. Information about other family members may also be on the school file.

Every school must also publish a Privacy Notice on the website.

What are the key principles of UKGDPR?

These are lawfulness, transparency and fairness. School must have a legitimate reason to hold the data and we explain this in the Data Privacy Notices on the website. We often ask for consent to use data about a pupil for a particular purpose e.g., permission to take photographs. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects Rights' later in this document.

- **Schools may only collect data for a specific purpose and use it for that purpose;** to clarify, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.
- **Limited collection;** data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.
- **Accuracy;** data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and then check again on an annual basis. If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller at all then a dispute resolution process and complaint process can be accessed, using the suitable forms.
- **Retention;** school has a Data Retention Policy that explains how long we store records for. This is available on request and on the website.
- **Security;** we have processes in place to keep data safe and secure be it in paper files, electronic records or other information.
- **Who is a 'data subject'?** Someone whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.
- **Data subjects' rights** Individuals have a right:
 - To be informed
 - Of access to data stored about them or their children
 - To rectification if there is an error on the data stored
 - To erasure if there is no longer a need for school to keep the data
 - To restrict processing, i.e., to limit what is done with their data
 - To object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools. Data subjects' rights are also subject to child protection and safeguarding concerns as well as sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

Subject Access Requests

You can ask for copies of information that we hold about you, or a pupil at school that you are a parent of or for whom you have parental responsibility. This Subject Access Request process is set out separately. You need to fill out the form and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays, if the request is complicated, or the data cannot be accessed. The maximum extension is up to two months.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g., school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information within this policy.

Who is a 'data controller'?

Our school governing body is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. UKGDPR places additional obligations on organisations to make sure that data controllers require contractual agreements to ensure that this is the case.

Processing data

School must have a reason to process the data about an individual. Our Privacy Notice sets out how we use data. UKGDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are;

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of;

- explicit consent from the data subject their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by UKGDPR. Guidance from the Department for Education, health, the police, local authorities, and other specialist organisations may be used to determine whether data is shared. The basis for sharing or not sharing data is recorded in school.

Breaches & Non-Compliance

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

If there is non-compliance with the policy or processes, or there is a DATA PROTECTION AUTHORITY breach as described within the UKGDPR 2018 and DATA PROTECTION AUTHORITY 2018 then the guidance set out in the Breach & Non-Compliance Procedure and Process needs to be followed.

Protecting data and maintaining the data subjects' rights is the purpose of this policy and associated procedures.

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory, and regulatory occasions when consent is not required. However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the UKGDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website we have a 'Privacy Notice' that explain how data is collected and used. It is important to read this notice as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school, you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes (a form is available from the school office). This is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints at any time. Where more than one person can provide or withdraw consent the school will consider each situation on the merits and within the principles of UKGDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Policy

We use CCTV and store images for a period in line with the policy. CCTV may be used for:

- Detection and prevention of crime
- School staff disciplinary procedures

- Pupil behaviour and exclusion management processes
 - maintaining a safe environment for the whole school community
- Please also see the CCTV Policy for further information.

Data Protection Officer (DPO)

We have a Data Protection Officer whose role is to: -

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations under UKGDPR
- To monitor compliance with the UKGDPR and DATA PROTECTION AUTHORITY
- To provide advice when requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- To cooperate with the supervisory authority and manage the breach procedure
- To advise about training and CPD for the UKGDPR

Our DPO is Mr John A Walker, Solicitor

Address: 6 Delamore Park, Cornwood, Ivybridge, PL21 9QP

Email: info@jawalker.co.uk

Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e., locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Headteacher, along with the Office Manager, is responsible for authorising access to secure areas.

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party, are subject to contractual conditions to ensure UKGDPR and DATA PROTECTION AUTHORITY compliance.

- Hardware is disposed / recycled by our IT Support
- Hard copy files are destroyed by school office staff in school.
- Servers and Hard drives are cleansed by our IT Support
- Portable and removable storage are destroyed/cleaned/recycled by our IT Support

Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data protection issues and there is a right to complain if you feel that data has been shared without consent or lawful authority. You can complain if you have asked to us to erase, rectify or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure.

Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk

Helpline: 0303 123 1113

Website: www.ico.org.uk

Review

A review of the effectiveness of UKGDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Reviewed autumn 2023

To be reviewed autumn 2024