Ashleworth CE Primary School

General Data Protection Regulation (GDPR) Policy

Approved by:	Resources Committee
Date of review:	18 March 2024
Next review due by:	March 2026

Responsibility

It is the responsibility of the Data Protection Officer, the Governors and Headteachers to ensure procedures are in place to ensure that the school complies with the General Data Protection Regulations 2018 (GDPR)

Introduction

In order to operate efficiently Ashleworth CE Primary School has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, third parties and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is committed to ensuring personal information is properly managed and that it ensures compliance with the General Data Protection Regulations May 2018 Act. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

This policy applies to all employees, governors, contractors, volunteers, agents and representatives and temporary staff working for or on behalf of the School.

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The GDPR does not apply to access to information about deceased individuals.

Responsibilities

The Data Protection Officer is responsible for ensuring compliance with the DPA and this policy within the day to day activities of the School. The DPO is responsible for ensuring that appropriate training is provided for all staff.

The Data Protection Officer (DPO) should not be the head teacher, DSL or Business Manager.

The Data Protection Officer and the Governor with for this school overall responsibility for compliance with the DPA is Roger Ingham. The DPO can be contacted via the school office or by email dpo@ashleworth.gloucs.sch.uk

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA and duplication is minimised

The Requirements

The GDPR stipulates that anyone processing personal data must comply with eight principles of good practice; these principles are legally enforceable. The principles require that personal information:
From 25 May 2018, schools and academies should be able to demonstrate that they comply with the following data protection principles, which require that personal data is:

- Processed in a lawful, fair and transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate, and where necessary, kept up to date
- kept in a form which enables individuals to be identified for no longer than necessary
- Processed in a manner that ensures appropriate security
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

Notification

- **Under the General Data Protection Regulations all Data Controllers must notify the Information Commissioner's Office (ICO) about how they process personal information.**
- Each individual school is a data controller and so must register with the ICO. Failure to do so is a criminal offence.

The Data Protection Act requires every data controller (the School) who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School is registered.

Consent

Whenever information is collected about individuals or families consent must be sought and they must be made aware of the following:

- The identity of the data controller, e.g. the School;
- The Data Protection Officer
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;

- Who the information is recorded and how it will or may be shared with; and
- How to contact the data controller.

This must be at the time that information first starts to be gathered on an individual.

Privacy Notice – see Appendix for Privacy notices

Information that will be collected may include.

- Children's registration forms
- Electronic records for admin
- SEND register and forms
- Health care plans/allergies/medical records
- Class lists
- Interventions
- Permission slips
- Photographs
- Electronic and paper tracking systems
- Test results
- Observations of learning
- Reports and parents evening notes
- Safeguarding records
- Records of meetings/behaviour incidents/family concerns
- Records from other settings
- Teachers notes

Conditions for Processing

- The requirement that data is processed in a 'lawful' and 'transparent' manner means schools' and academies' privacy policies and certain supplier contracts need to be reviewed and brought up to spec: the GDPR sets out a number of new, mandatory requirements for these legal documents

Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- *other members of staff, governors on a need to know basis;*
- *relevant Parents/Guardians;*
- *other authorities if it is necessary in the public interest, e.g. prevention of crime;*
- *other authorities, such as the LEA and schools to which a pupil may move, where there are legitimate requirements (DfE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).*

The School should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict advice should be obtained.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

The individual's right to access their personal information (Subject Access Requests)

The rights of individuals

- Schools and academies will already be familiar with the right of subject access. This right is changing slightly under the GDPR (MAY 2018): a charge can no longer be made for responding to a subject access request (unless particular circumstances apply) and the time for responding to a subject access request is being reduced from 40 days to one calendar month.

When providing the information, the School must also provide

- a description of why the information is processed
- details of anyone it may be disclosed to
- the source of the data.

Provision of data to children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records.

Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. These should be changed on a regular basis.

Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most, relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined.

Disposal of data – see Appendix at end of policy for Disposal schedule.

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.
A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.
(*PRONI – public records office Northern Ireland – archives for records.)

Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime, a caution should be marked on the person's file that there is

a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

Photographs

Whether or not a photograph comes under the GDPR is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

Breach of the policy

Non-compliance with the requirements of the GDPR by the members of staff could lead to serious action being taken by third parties against the school authorities. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data that must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, memory stick, portable or mobile device is **encrypted** and is transported securely for storage in a secure location;
- Users must protect all portable and mobile/memory devices, including media, used to store and transmit personal information using approved **encryption software**; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Data Breach

A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

If there is a breach we must

- notify the ICO (Information Commissioners Office)
- consider whether to notify our customers; and
- record details in our own breach log.

When and how do we notify the ICO?

We must notify the ICO (www.ico.org.uk.) within 24 hours of becoming aware of the essential facts of the breach. This notification must include at least:

- our name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

.

If possible, we should also include full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about our notification to customers. If these details are not yet available, we must provide them as soon as possible.

Failure to submit breach notifications can incur a large fine.

When and how do we notify our customers?

If the breach is likely to adversely affect the personal data or privacy of our subscribers or users, we need to notify them of the breach without unnecessary delay. We need to tell them:

- our name and contact details;
- the estimated date of the breach;
- a summary of the incident;
- the nature and content of the personal data;
- the likely effect on the individual;
- any measures we have taken to address the breach; and

- how they can mitigate any possible adverse impact.

We do not need to tell your subscribers about a breach if we can demonstrate that the data was encrypted (or made unintelligible by a similar security measure).
If we do not tell your customers, the ICO can require us to do so if they consider the breach is likely to adversely affect them.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.
The school has a policy for reporting, managing and recovering from information risk incidents, which establishes

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Appendix

Abbreviations

Abbreviation	Description
GDPR	General Data Protection Regulations May 2018
EIR	Environmental Information Regulations 2004
FoIA	Freedom of Information Act 2000

Glossary

Use of technologies and impact levels

The following provides a useful guide:

	The information	The technology	(Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupil's work, lunchtime menus, extended services, parent consultation events	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about school's closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED

	online means.		(Impact Level 0) category.

Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Member of staff with overall responsibility for data identified (SIRO)

- Risk assessments complete
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests.
- If school has CCTV appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*

Privacy Notice

Ashleworth CE Primary school is a data Controller for the purpose of the General Data Protection Regulations. We collect information from you and may receive information about you and your child. We use this data to –

- Keep your child safe and healthy
- Support teaching and Learning
- Monitor, report and share progress and achievements
- Assess how well we are doing.

This information includes your contact details, curriculum assessment, photographs, video, results, attendance as well as personal characteristics such as ethnic groups, special needs and relevant medical information. We also share summarised, aggregated data for statistical analysis purposes with the WGSP We are required by law to pass some information to the Local Authority (LA), the DFE and safeguarding authorities.

We will not give information about you to anyone outside the school without your consent unless the law or our procedures require us to.

If you want to see a copy of the information about you that we hold and/or share, please contact the head or the school office

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.gloucestershire.gov.uk/article/105060/Privacy-Notices and

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- CYP Systems Support Team
  ICT Service
  Gloucestershire County Council
  Quayside House
  Quay Street
  Gloucester. GL1 2TZ

  Website: www.gloucestershire.gov.uk
  Email: cypdsystemsupport@gloucestershire.gov.uk

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London

Ashleworth CE Primary School is the Data Controller for the purposes of the General Data Protection Regulations

Personal data is held by the school about those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information. We also share summarised, aggregated data for statistical analysis purposes with the West Gloucestershire Schools partnership - WGSP.

We will not give information about you to anyone without your consent unless the law and our policies require us to.

We are required by law to pass on some of this data to:

- the LA
- the Department for Education (DfE)

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- http://www.gloucestershire.gov.uk/council-and-democracy/data-protection/privacy-notices/
  and
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- ICT Service Application Support
  Gloucestershire County Council
  Block 4 First Floor
  Shire Hall
  Westgate Street
  Gloucester. GL1 2TP

  Website: www.gloucestershire.gov.uk
  Email: cypdsystemsupport@gloucestershire.gov.uk

- Ministerial and Public Communications Division
  Department for Education
  Piccadilly Gate
  Store Street
  Manchester
  M1 2WD
-
  Website: www.education.gov.uk
  email: http://www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288