Data Protection / GDPR Policy

Date policy created: September 2026

Date of last review:

Date of next review: September 2027

Created by: Mrs B Readey

1. Introduction

Ashton Primary School is committed to protecting the privacy and personal information of pupils, parents and carers, staff, governors, volunteers, visitors and other individuals with whom the school works.

The school collects and processes significant amounts of personal information in order to fulfil its educational, safeguarding, employment, administrative and legal responsibilities.

Ashton Primary School will ensure that personal information is handled lawfully, fairly, transparently and securely.

This policy has been developed with regard to:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025;
- relevant education legislation;
- guidance issued by the Information Commissioner's Office (ICO); and
- Department for Education guidance on data protection in schools.

The Data (Use and Access) Act 2025 does not replace the UK GDPR or Data Protection Act 2018; it amends and builds upon the existing data-protection framework.

2. Purpose

This policy aims to ensure that Ashton Primary School:

- complies with its legal responsibilities;
- protects the rights and privacy of individuals;
- handles personal information appropriately;
- keeps personal information secure;
- only collects and uses information where there is a legitimate purpose for doing so;
- shares information appropriately and securely;
- responds appropriately to requests concerning personal information;
- responds effectively to personal data breaches;
- provides clear information about how personal data is used; and
- maintains appropriate accountability for its data-processing activities.

3. Scope

This policy applies to personal information relating to:

- pupils;
- prospective pupils;
- former pupils;
- parents and carers;
- staff;
- prospective and former employees;
- governors;
- volunteers;
- students undertaking placements;
- contractors;
- visitors;
- external professionals; and
- any other identifiable individual whose personal information is processed by the school.

It applies to personal information held electronically and in paper form.

It also applies to photographs, video and audio recordings where individuals can be identified.

4. Data Controller

For most of the personal information collected, stored and used by the school, Ashton Primary School is the Data Controller.

As Data Controller, the school determines why and how personal information is processed and is responsible for ensuring that this is carried out in accordance with data-protection legislation.

The school is registered with the Information Commissioner's Office as required.

5. Data Protection Officer

As a maintained school, Ashton Primary School is required to have a designated Data Protection Officer (DPO) and this is our School Business Manager (Diane Brooks).

The DPO provides independent advice and oversight regarding the school's compliance with data-protection legislation.

The DPO's responsibilities include:

- advising the school about its data-protection obligations;
- monitoring compliance;
- supporting data audits;
- advising on policies and procedures;
- advising on Data Protection Impact Assessments (DPIAs);
- supporting the management of data breaches;
- advising on individuals' data-protection rights;
- reviewing privacy notices;
- providing or supporting staff training; and
- acting as a point of contact regarding data-protection matters.

The DPO will have appropriate access to senior leaders and the Governing Body.

6. Data Protection Principles

When processing personal information, Ashton Primary School will comply with the principles of data protection.

Personal information will be:

Lawful, fair and transparent
Information will only be processed where there is an appropriate lawful basis and individuals will be provided with appropriate information about its use.

Collected for specified purposes
Information will be collected for clear and legitimate purposes and will not normally be used incompatibly with those purposes.

Adequate, relevant and limited
The school will only collect the information that is reasonably necessary for the purpose.

Accurate
Reasonable steps will be taken to ensure that personal information is accurate and, where necessary, kept up to date.

Kept for no longer than necessary
Personal information will be retained in accordance with the school's retention arrangements and securely disposed of when no longer required.

Secure
Appropriate technical and organisational measures will be used to protect personal information from unauthorised or unlawful processing and accidental loss, destruction or damage.

The school will also demonstrate **accountability** for its compliance with these principles.

7. Personal Data

Personal data is information relating to an identified or identifiable living person.

Examples of information processed by the school include:

- names;
- addresses;
- dates of birth;
- contact details;
- pupil identification numbers;
- attendance information;
- assessment and attainment information;
- behaviour information;
- photographs and videos;
- educational records;
- SEND information;
- family information;
- financial information;
- staff employment information;
- IP addresses and other online identifiers; and
- other information that can identify an individual directly or indirectly.

Information does not necessarily need to contain someone's name to constitute personal data if the individual can still be identified.

8. Special Category Data

Some personal information requires additional protection.

Special category data includes information concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic information;
- biometric information used for identification;
- health;
- sex life; and
- sexual orientation.

Schools routinely process some special category information, including information relating to health, ethnicity and religion.

The school will ensure that an appropriate lawful basis and, where required, an appropriate condition for processing special category information is identified.

9. Criminal Offence Data

Information concerning criminal allegations, proceedings, convictions or offences is subject to additional legal requirements.

The school will only process criminal offence data where it has an appropriate lawful basis and meets the additional requirements of data-protection legislation.

10. Lawful Basis for Processing

The school must have an appropriate lawful basis for each activity involving personal data.

Depending upon the circumstances, this may include processing because:

- it is necessary to comply with a legal obligation;
- it is necessary to perform a task in the public interest or exercise official authority;
- it is necessary for the performance of a contract;
- it is necessary to protect someone's vital interests;
- the individual has provided valid consent; or
- another lawful basis permitted by data-protection legislation applies.

The lawful basis relates to the specific processing activity, rather than simply to the type of information being processed.

11. Consent

Consent is only one possible lawful basis for processing personal information and will not be used where another lawful basis is more appropriate.

Where the school relies upon consent, it must be:

- freely given;
- specific;
- informed;
- unambiguous; and
- capable of being withdrawn.

Withdrawal of consent will not affect processing that had already lawfully taken place before consent was withdrawn.

The school will maintain appropriate records where consent is relied upon.

12. Children's Personal Information

Children's personal information requires particular care because children may be less aware of the risks and consequences associated with the use of their information.

When processing children's personal information, the school will:

- consider the best interests of the child;
- only collect information that is necessary;
- maintain appropriate security;
- provide age-appropriate information where necessary;
- consider children's developing capacity to understand and exercise their rights;
- ensure information is shared appropriately; and
- consider privacy and data protection when introducing new systems or technologies.

Children have data-protection rights in their own right. How these are exercised in practice will depend upon matters including the child's age, capacity and understanding.

13. Privacy Notices

Ashton Primary School will make appropriate privacy notices available to individuals whose personal information it processes.

These may include separate privacy notices for:

- pupils and parents;
- the school workforce; and
- governors and other governance roles.

Privacy notices will explain, as appropriate:

- what information the school collects;
- why it is collected;
- the lawful basis for processing;
- how the information is used;
- who it may be shared with;
- how long it may be retained;
- individuals' rights; and
- how to raise a concern.

Privacy notices will be regularly reviewed and updated where there are significant changes to the way personal information is processed. DfE guidance states that schools must make their privacy notices freely available.

14. Record of Processing Activities

The school will maintain appropriate records of its data-processing activities.

These records help the school understand:

- what information it holds;
- why it holds it;
- where it is stored;
- who has access;
- who it is shared with;
- the lawful basis for processing;
- relevant security arrangements; and
- how long it should be retained.

These records support the school's ability to demonstrate compliance with the accountability principle.

15. Data Minimisation

Staff should only collect, access and use personal information that is necessary for their professional responsibilities.

Staff must not collect information simply because it might be useful at some point in the future.

Where possible, information should be anonymised or pseudonymised where individuals do not need to be identified.

16. Accuracy

The school will take reasonable steps to ensure personal information is accurate and up to date.

Parents, carers and staff are encouraged to notify the school promptly of changes to information such as:

- addresses;
- telephone numbers;
- emergency contacts;
- names;
- medical information; and
- other relevant circumstances.

Where inaccurate information is identified, appropriate action will be taken to correct it.

17. Data Retention

Personal information will not be retained indefinitely simply because the school has the ability to store it.

The school will maintain and follow an appropriate **retention schedule**.

Retention periods will take account of:

- statutory requirements;
- safeguarding requirements;
- employment requirements;
- limitation periods;
- educational requirements;
- guidance on school records; and
- other legitimate operational needs.

The DfE advises schools to review the data they hold and securely dispose of information they no longer require.

18. Secure Disposal

Personal information must be disposed of securely when it is no longer required.

Paper documents containing confidential or personal information should be placed in confidential waste or appropriately shredded.

Electronic records should be securely deleted in accordance with the school's IT and retention arrangements.

Staff must not place confidential documents in ordinary waste or recycling bins.

19. Information Security

The school will implement appropriate technical and organisational measures to protect personal information.

These may include:

- password protection;
- appropriate access permissions;
- multi-factor authentication where appropriate;
- secure networks and systems;
- encryption where appropriate;
- secure backups;
- device security;
- filtering and monitoring;
- locked storage;
- secure disposal;
- staff training; and
- appropriate cyber-security arrangements.

Access to information should be based upon an individual's role and legitimate need.

20. Passwords and Accounts

Staff must:

- keep passwords confidential;

- use appropriately secure passwords;
- not share accounts with other individuals;
- use multi-factor authentication where provided;
- lock devices when unattended;
- immediately report suspected account compromise; and
- follow the school's Acceptable Use and IT-security arrangements.

Staff must never knowingly allow another person to access confidential information using their account.

21. Email and Electronic Communication

Staff must take particular care when sending personal information electronically.

Before sending an email containing personal information, staff should:

- check the recipient carefully;
- ensure all recipients need the information;
- consider whether the information needs to be sent;
- use BCC where appropriate when communicating with multiple unrelated recipients;
- use secure systems where required;
- check attachments before sending; and
- consider whether additional security or encryption is necessary.

Particular care must be taken when sending special category, safeguarding or other highly sensitive information.

22. Paper Records

Paper records containing personal information must be handled securely.

Staff should:

- store confidential documents appropriately;
- avoid leaving records unattended;
- not leave sensitive information visible to unauthorised individuals;
- ensure information is transported securely where this is necessary; and
- dispose of records using confidential waste arrangements.

23. Working Away from School

Where staff need to access personal information away from school, they must follow the school's security arrangements.

Staff should avoid:

- downloading information unnecessarily;
- storing school information permanently on personal devices;
- leaving documents or devices unattended;
- allowing family members or other unauthorised individuals to access school information; or
- discussing confidential information where they can be overheard.

Only approved systems and storage arrangements should be used for school information.

24. Photographs and Videos

Photographs and videos of identifiable pupils constitute personal information.

The school will ensure that photographs and videos are:

- taken for legitimate purposes;
- stored securely;
- shared appropriately;
- used in accordance with relevant permissions where consent is the lawful basis being relied upon; and
- deleted when no longer required in accordance with school arrangements.

Staff should normally use **school-authorised devices** to take photographs or videos of pupils.

Personal devices must not be used to photograph or record pupils unless specifically authorised under an exceptional school arrangement.

The school's Social Media Policy and relevant consent arrangements provide further guidance.

25. Class Dojo and Tapestry

Ashton Primary School uses Class Dojo for communication with parents and carers.

Tapestry is additionally used within EYFS and The Burrow to share children's learning and experiences with families.

Personal information shared through these systems must be appropriate and necessary.

Staff must:

- use school-authorised accounts;
- ensure information is shared with the correct parent/carer;
- avoid unnecessarily sharing sensitive information;
- maintain professional boundaries;
- report incorrect access or accidental disclosure promptly; and
- follow school safeguarding and communication procedures.

Tapestry and Class Dojo must not be treated as substitutes for appropriate safeguarding recording systems.

26. Artificial Intelligence

The use of artificial intelligence presents particular data-protection considerations.

Staff must not enter identifiable, confidential or sensitive pupil, family or staff information into public or unapproved AI systems.

This includes:

- pupil names;
- dates of birth;
- addresses;
- identifiable photographs;
- medical information;
- safeguarding records;
- child protection information;
- identifiable SEND documentation;
- EHCPs;
- behaviour records;
- professional reports;
- family circumstances; and
- staff confidential information.

Removing a person's name does not necessarily mean information has been effectively anonymised.

Any use of AI must comply with the school's Artificial Intelligence Policy and relevant data-protection requirements. The DfE now provides specific school resources on protecting children's privacy when using AI.

27. Data Sharing

There are many circumstances where it is necessary and lawful for the school to share personal information.

This may include sharing with:

- the Department for Education;
- Lancashire County Council;
- other schools and educational settings;
- health professionals;
- social care;
- safeguarding partners;
- police;
- SEND professionals;
- examination or assessment organisations;
- service providers;
- contractors; and
- other organisations where there is a lawful basis.

Before sharing information, staff should consider:

Who needs the information?
Why do they need it?
What information is actually necessary?
Is there a lawful basis for sharing it?
How can it be shared securely?

28. Safeguarding and Data Protection

Data-protection legislation does **not** prevent the appropriate sharing of information to safeguard a child.

Where information needs to be shared to protect a child or another person, staff should follow safeguarding procedures and seek advice from the Designated Safeguarding Lead where appropriate.

Staff must not allow uncertainty about data protection to prevent necessary safeguarding action.

Information sharing should nevertheless remain necessary, proportionate, relevant and appropriately secure.

The ICO provides specific guidance on sharing personal information to safeguard children and young people within education.

29. Sharing Information with Parents

Parents will routinely receive information relating to their child.

However, parental responsibility does not automatically mean that a parent is entitled to every piece of information held by the school in every circumstance.

Consideration may need to be given to:

- the child's own data-protection rights;
- the child's age and understanding;
- information about third parties;
- safeguarding considerations;
- court orders;
- confidentiality; and
- applicable education legislation.

Complex requests should be referred to the DPO where appropriate.

30. Subject Access Requests

Individuals have the right to request access to personal information held about them.

A Subject Access Request (SAR) may be made verbally or in writing and does not have to use the words "subject access request".

Any member of staff receiving what may constitute a SAR should forward it promptly to the appropriate person within school.

The school will:

- identify the information requested;
- verify identity where appropriate;
- locate relevant information;
- consider whether any exemptions apply;

- protect the rights of third parties; and
- respond within the applicable statutory timescale.

Staff must not attempt to deal with a complex Subject Access Request independently.

31. Pupil Educational Records

In addition to rights under data-protection legislation, parents of pupils attending maintained schools may have separate rights to access their child's educational record under education legislation.

These are distinct from Subject Access Requests under UK GDPR.

Requests will be dealt with according to the appropriate legal framework.

32. Other Individual Rights

Depending upon the circumstances and lawful basis for processing, individuals may have rights including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure in certain circumstances;
- the right to restrict processing in certain circumstances;
- the right to data portability where applicable;
- the right to object in certain circumstances; and
- rights relating to automated decision-making.

These rights are not absolute and do not apply in every circumstance.

Requests should be referred to the DPO where advice is required.

33. Data Protection by Design and Default

The school will consider privacy and data protection from the beginning when introducing new systems, technologies, projects or ways of working.

This includes considering:

- what personal information is required;
- why it is needed;
- who will have access;

- how it will be secured;
- how long it will be retained;
- whether information will be shared;
- whether children require additional protection;
- whether a supplier will process information;
- where information will be stored; and
- whether a Data Protection Impact Assessment is required.

Data protection by design and default is a legal requirement, and changes introduced through the Data (Use and Access) Act 2025 place additional emphasis on considering children's higher protection needs.

34. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms.

A DPIA may also be appropriate when introducing:

- significant new technology;
- new monitoring systems;
- biometric systems;
- substantial processing of sensitive information;
- new AI systems;
- systems involving automated decision-making;
- extensive data sharing; or
- other processing presenting increased privacy risks.

The DPO should be consulted where a DPIA may be required.

35. Educational Technology and Third-Party Providers

Before introducing a new digital service or educational technology that processes personal information, the school should consider:

- what information the provider collects;
- why it is collected;
- where it is stored;

- who can access it;
- whether information is shared with others;
- retention arrangements;
- security arrangements;
- contractual terms;
- whether information is used for advertising, profiling or product development;
- arrangements for deleting information;
- international transfers where applicable; and
- the provider's responsibilities under data-protection legislation.

Staff must not independently introduce services requiring pupil personal information without appropriate school approval.

36. Personal Data Breaches

A personal data breach may include:

- sending information to the wrong person;
- losing paperwork;
- losing a device containing personal information;
- unauthorised access to an account;
- accidentally publishing information;
- cyber attacks;
- inappropriate disclosure;
- loss or destruction of records; or
- any other incident affecting the confidentiality, integrity or availability of personal information.

All actual or suspected personal data breaches must be reported immediately to the appropriate senior leader and/or DPO.

Staff should not attempt to conceal or independently resolve a breach without reporting it.

37. Responding to a Data Breach

When a breach occurs, the school will:

1. take immediate action to contain the breach where possible;

2. establish what has happened;
3. identify the information and individuals affected;
4. assess the potential risk;
5. record the breach;
6. seek advice from the DPO;
7. determine whether the ICO must be notified;
8. determine whether affected individuals must be informed; and
9. identify action required to prevent recurrence.

Where notification to the ICO is legally required, it must be made within the applicable statutory timescale.

38. Data Protection Complaints

Individuals who have concerns about the way the school has handled their personal information should initially raise these with the school.

The school will ensure that data-protection concerns and complaints are considered promptly and appropriately.

Where a person remains dissatisfied, they may raise their concern with the school's DPO and/or the Information Commissioner's Office as appropriate.

The Data (Use and Access) Act 2025 places additional emphasis on organisations having clear and accessible processes for data-protection complaints.

39. Staff Responsibilities

Protecting personal information is the responsibility of all staff, not solely the Headteacher, office staff or DPO.

Staff must:

- follow this policy;
- complete required training;
- only access information they legitimately need;
- keep information confidential;
- use approved systems;
- maintain secure passwords;
- protect devices and paperwork;

- check recipients before sharing information;
- follow retention and disposal procedures;
- report breaches immediately;
- seek advice where uncertain; and
- maintain appropriate professional confidentiality.

Deliberate, reckless or serious breaches of this policy may be dealt with under the school's disciplinary procedures.

40. Headteacher Responsibilities

The Headteacher has overall operational responsibility for ensuring that appropriate data-protection arrangements are implemented within school.

The Headteacher will work with the DPO, Governing Body and relevant staff to ensure that:

- appropriate systems and procedures are maintained;
- staff receive training;
- risks are identified;
- breaches are appropriately managed;
- policies and privacy notices are reviewed; and
- data protection forms part of the school's wider governance and risk-management arrangements.

41. Governing Body Responsibilities

The Governing Body has strategic oversight of the school's data-protection arrangements.

Governors will seek assurance that:

- the school complies with relevant legislation;
- appropriate policies and procedures are in place;
- a DPO has been appointed;
- staff receive appropriate training;
- significant risks are appropriately managed; and
- data-protection arrangements are regularly reviewed.

Governors must themselves handle personal information obtained through their role securely and confidentially.

42. Staff Training

All staff who handle personal information will receive appropriate data-protection training.

Training will normally include:

- basic data-protection principles;
- confidentiality;
- secure handling of information;
- cyber security;
- email security;
- recognising Subject Access Requests;
- recognising and reporting data breaches;
- safeguarding and information sharing;
- use of photographs and video;
- AI and emerging technologies; and
- responsibilities when working away from school.

Training should be refreshed periodically and when significant changes occur.

43. Monitoring and Audit

The school and DPO will undertake proportionate monitoring of data-protection arrangements.

This may include:

- data audits;
- reviewing access permissions;
- reviewing privacy notices;
- reviewing data breaches;
- checking retention arrangements;
- reviewing third-party systems;
- reviewing Records of Processing Activities;
- staff training records; and
- reviewing policies and procedures.

44. Related Policies and Documents

This policy should be read alongside the school's:

- Privacy Notices;
- Records Retention Schedule;
- Record of Processing Activities;
- Subject Access Request Procedure;
- Personal Data Breach Procedure;
- Child Protection and Safeguarding Policy;
- Online Safety Policy;
- Acceptable Use Policy;
- Artificial Intelligence Policy;
- Social Media Policy;
- Parent and Carer Communication Policy;
- Mobile Phone Policy;
- Staff Code of Conduct;
- Freedom of Information Policy; and
- IT and Cyber Security procedures.

45. Monitoring and Review

This policy will be reviewed annually, or sooner where:

- data-protection legislation changes;
- ICO or DfE guidance changes;
- the school introduces significant new technology;
- the school's processing activities significantly change;
- a serious data breach identifies a need for review; or
- the DPO recommends changes.

The Governing Body will approve significant amendments to this policy.

Appendix 1 – Staff Data Protection Checklist

Before using or sharing personal information, staff should ask:

Do I need this information?
Only collect or access information required for the task.

Am I allowed to use it for this purpose?
Information should only be processed for an appropriate and lawful purpose.

Does this person need to receive it?
Only share information with people who have a legitimate need to know.

Am I sharing more than necessary?
Share the minimum information required.

Is the method secure?
Consider how the information is being sent, stored or transported.

Have I checked the recipient?
Always double-check email addresses, attachments and recipients.

Does this contain particularly sensitive information?
Take additional care with safeguarding, SEND, medical, family and staff information.

Should this be recorded on an approved school system?
Do not create unnecessary duplicate records.

Am I using an approved system?
Do not upload school information to unapproved apps, websites or AI services.

What happens when this information is no longer required?
Follow the school's retention and secure-disposal arrangements.

Has something gone wrong?
Report any actual or suspected data breach immediately. Do not hide mistakes.

Appendix 2 – Data Breach Quick Response

If personal information is **lost, sent to the wrong person, accessed inappropriately, disclosed accidentally or otherwise compromised:**

1. ACT
Take reasonable immediate action to stop or contain the breach where possible.

2. DO NOT CONCEAL IT
Mistakes can often be managed effectively when reported quickly.

3. REPORT IT IMMEDIATELY
Inform the Headteacher / designated school contact and Data Protection Officer.

4. PRESERVE INFORMATION
Do not delete relevant emails, logs or other evidence unless instructed.

5. PROVIDE THE FACTS
Explain what happened, what information was involved, who may be affected and what action has already been taken.

The school/DPO will determine whether further action, including notification to the ICO or affected individuals, is required.