

Data Protection Policy

Barford Primary School



Responsibility: Head Teacher

Date: August 2026

Approved by Governing Body:

Review date:

August 2027

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	5
6. Data protection principles	8
7. Collecting personal data	8
8. Sharing personal data.....	10
9. Subject access requests and other rights of individuals	11
10. Parental requests to see the educational record	13
11. CCTV	14
12. Photographs and videos	14
13. Data protection by design and default	14
14. Data security and storage of records	16
15. Disposal of records	17
16. Personal data breaches	17
17. Training.....	18
18. Monitoring arrangements.....	18
19. Links with other policies	19
Appendix 1: Personal data breach procedure.....	20

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ➤ Name (including initials) ➤ Identification number ➤ Location data ➤ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ➤ Racial or ethnic origin ➤ Political opinions ➤ Religious or philosophical beliefs ➤ Trade union membership ➤ Genetics ➤ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ➤ Health – physical or mental ➤ Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and will renew this registration annually or as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

- **5.1i** The Board of Governors and management of Barford Primary School are committed to compliance with all relevant UK legislation of personal data, and the protection of the “rights and freedoms” of individuals whose information Barford Primary School collects and processes in accordance with the Data Protection Act 2018.
- **5.1ii** Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy (GDPR 002), along with connected processes and procedures.
- **5.1iii** The GDPR and this policy apply to all of Barford Primary School’s personal data processing functions, including those performed on pupils’, clients’, employees’, volunteers’, suppliers’ and partners’ personal data, and any other personal data the organisation processes from any source.
- **5.1iv** Barford Primary School has established objectives for data protection and privacy, which are in the GDPR Objectives Record (GDPR 003).
- **5.1v** The Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to Barford Primary School’s activities. This register needs to be available on the supervisory authority’s request.
- **5.1vi** This policy applies to all governors, employees and volunteers of Barford Primary School and any other interested parties, such as outsourced suppliers of services. Any breach of Data Protection legislation will be dealt with under the disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.
- **5.1vii** Partners and any third parties working with or for Barford Primary School, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Barford Primary School without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Barford Primary School is committed, and which gives Barford Primary School the right to audit compliance with the agreement.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Kaylee Lilly and is contactable via 0121 464 4228 and klilly@barfordprimary.co.uk.

The school receives independent data protection advice and support from Insight Management Services and Information Governance.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate and relevant national or international security standards.

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout Barford Primary School;
- Measures that consider the reliability of employees (such as references, etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;

- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the international transfers in accordance with UK data protection law
- .

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The school will maintain a register of approved AI applications and services.

5.3 Head Teacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties
 - Staff must not use unapproved AI tools for school business where personal information may be processed.
 - Staff must not enter personal, confidential, safeguarding, SEND, medical, behavioural or HR-related information into any AI platform unless it has

been approved by the school and is being used in accordance with the school's policies and procedures. [\[smoothwall.com\]](https://smoothwall.com), [\[academy.openai.com\]](https://academy.openai.com)

Staff must not upload or input:

- pupil personal information;
- safeguarding records;
- SEND documentation;
- medical information;
- confidential staff information;
- photographs of pupils;
- assessment data;
 - into public AI tools unless specifically authorised and subject to appropriate safeguards.

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any format they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one calendar month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Joanne Davies - Headteacher.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards, displays, prospectuses and newsletters.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website, social media pages and app.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Data Protection Impact Assessments (DPIAs) will be completed before introducing new AI systems, educational platforms or technologies that process personal data or may present a risk to the rights and freedoms of individuals.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the international transfers in accordance with UK data protection law, where different data protection laws will apply
- Maintaining records of our processing activities, including:
 -
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, and the safeguards for those, retention periods and how we are keeping the data secure

14. Artificial Intelligence (AI) and Personal Data

- Barford Primary School recognises that Artificial Intelligence (AI) technologies may be used to support educational, administrative and operational activities.
- The school will ensure that any use of AI complies with:
 - UK GDPR;
 - Data Protection Act 2018;
 - Department for Education guidance;
 - safeguarding requirements; and
 - the school's policies and procedures. [\[smoothwall.com\]](https://smoothwall.com), [\[academy.openai.com\]](https://academy.openai.com)

- Before introducing AI systems that process personal data, the school will assess:
 - data protection implications;
 - safeguarding risks;
 - security arrangements;
 - contractual terms and conditions;
 - retention and deletion arrangements;
 - whether a Data Protection Impact Assessment (DPIA) is required. [\[smoothwall.com\]](https://smoothwall.com), [\[schoolsine...land.co.uk\]](https://schoolsine...land.co.uk)
- Personal data must only be processed through AI systems that have been approved by the school.
- Staff must not enter personal, confidential, safeguarding, SEND, medical, behavioural or HR-related information into any AI system unless the system has been approved by the school and appropriate data protection and safeguarding assessments have been completed. [\[smoothwall.com\]](https://smoothwall.com), [\[academy.openai.com\]](https://academy.openai.com)
- AI-generated outputs must always be reviewed by a member of staff before use. Staff remain responsible for the accuracy, suitability and appropriateness of any AI-generated content used for teaching, communication, administration or decision-making.
- The school will maintain appropriate oversight of AI systems and ensure that any AI-related incidents, safeguarding concerns or personal data breaches are reported and managed through established procedures.
- AI-related safeguarding concerns, including AI-generated imagery, impersonation, deepfakes, online abuse, bullying, harassment and inappropriate content, will be managed in accordance with the school's Safeguarding and Child Protection Policy.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the school office
 - Passwords **11 or more characters**
 - **3 words that are not associated**
 - **Includes capital and a special character**
 (E.G. Rainbow-Mat-Pencil1)
- that are at least 11 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Multi-factor authentication (MFA) will be enabled on school systems wherever available and appropriate

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

- The school will make all reasonable endeavours to prevent personal data breaches.
- In the event of a suspected personal data breach or significant data protection incident, the school will follow the procedure set out in Appendix 1.
- Where required under UK data protection legislation, the school will report personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. [\[schoolsine...land.co.uk\]](https://schoolsine...land.co.uk)
- Personal data breaches may also arise through the use of Artificial Intelligence (AI) systems. This may include the unauthorised disclosure, processing, retention or sharing of personal data through AI platforms, chatbots, image-generation tools or other AI-enabled services. Such incidents will be investigated in accordance with Appendix 1 and may be reported to the ICO where required. [\[smoothwall.com\]](https://smoothwall.com), [\[schoolsine...land.co.uk\]](https://schoolsine...land.co.uk)
- Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the school website.
 - Safeguarding information being disclosed to an unauthorised person.
 - The loss or theft of a school device containing personal data.
 - Personal data being sent to an incorrect recipient.
 - Identifiable pupil or staff information being entered into an unapproved AI platform.
 - Safeguarding, SEND, behavioural or medical information being uploaded to an AI system without authorisation.
 - The creation or distribution of AI-generated or manipulated images, audio or video that may cause harm, distress or reputational damage to a pupil, parent, governor or member of staff.
 -
 - AI-generated content that discloses personal information relating to pupils, parents, carers or staff.
 - The unauthorised creation, storage or distribution of AI-generated images, audio or video involving members of the school community. [\[smoothwall.com\]](https://smoothwall.com), [\[academy.openai.com\]](https://academy.openai.com), [\[schoolsine...land.co.uk\]](https://schoolsine...land.co.uk)
- The school will maintain records of all personal data breaches and significant near-miss incidents and will review these regularly to identify trends, improve practice and reduce future risks.

17. AI data breaches

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

All staff will receive training on the safe and lawful use of AI technologies, including:

- data protection risks;
- safeguarding risks;
- AI bias and accuracy;
- confidentiality requirements;
- approved school AI systems.

Training records will be maintained as part of the school's compliance programme.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every **year** and shared with the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Information Security Policy
- Freedom of information publication scheme
- Online Safety Policy
- ICT Safety Policy
- Safeguarding and Child Protection Policy
- CCTV Policy
- Parent, Child, Governor and Visitor Privacy Notices
- AI policy
- Acceptable Use policy
- Staff code of conduct

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) and complete the Data Breach reporting form.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Head Teacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's Computer system and in the Data Protection Folder, which is locked away in a filing cabinet in the School Office.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

➤ If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

➤ Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

➤ The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

➤ The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the School's Computer System and in the Data Protection folder, which is locked away in the School Office.

- The DPO and Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Head Teacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system.
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

AI-Related Incidents

Where an AI-related incident occurs, staff must:

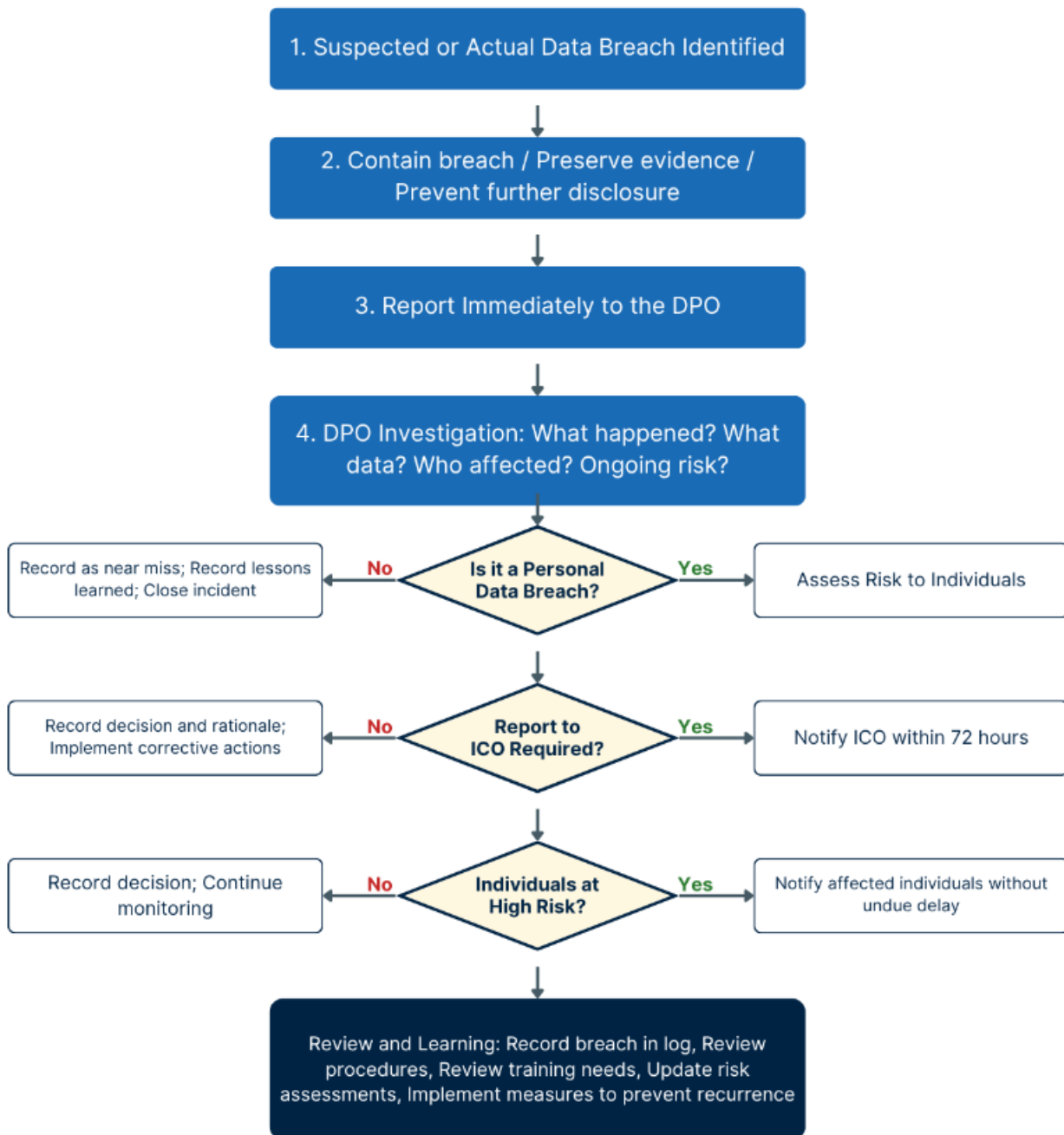
- Immediately stop using the AI system concerned.
- Preserve relevant evidence, including prompts, responses, screenshots and outputs.
- Report the incident immediately to the Data Protection Officer (DPO) and Headteacher.
- Record what information may have been uploaded, generated, disclosed or retained.
- Not attempt to delete evidence unless instructed to do so by the DPO.

The DPO will:

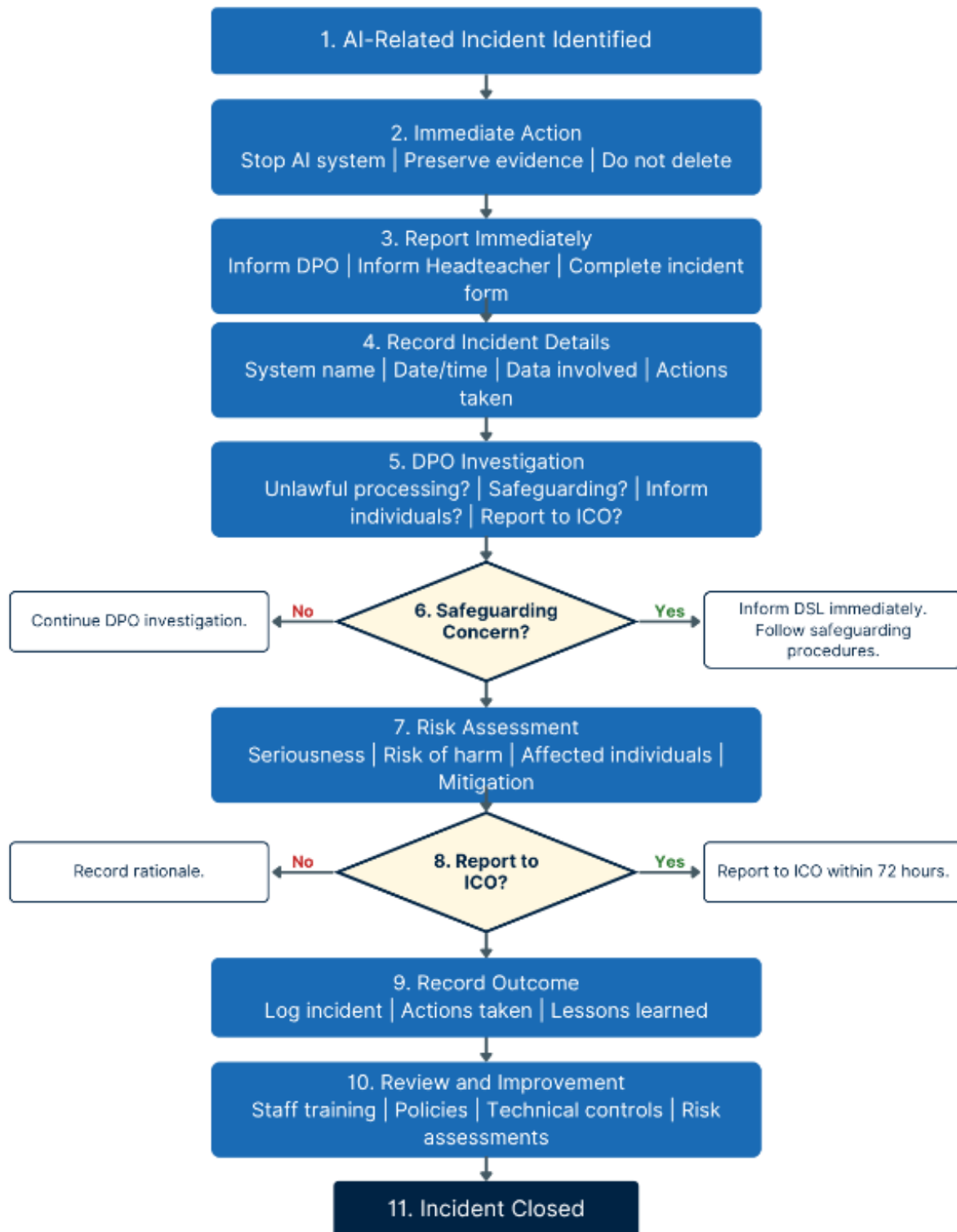
- Assess whether personal data has been processed unlawfully.
- Assess whether safeguarding concerns exist.
- Determine whether affected individuals need to be informed.
- Determine whether the incident meets the threshold for reporting to the Information Commissioner's Office (ICO).
- Consider whether the AI provider should be contacted to remove or delete information.
- Record the incident within the school's breach register.
- Review whether further staff training, policy amendments or technical controls are required.

Where an AI-related incident involves pupils, deepfakes, inappropriate imagery, bullying, harassment or any safeguarding concern, the Designated Safeguarding Lead (DSL) will be informed immediately and appropriate safeguarding procedures will be followed.

Personal Data Breach Process



AI-Related data breach Response Process



Data Breach Form

Barford Primary School

CONFIDENTIAL

This form must be completed immediately upon discovering or suspecting a personal data breach, AI-related incident or significant information security incident by the Data Protection Officer (DPO).

SECTION 1: REPORTER DETAILS

Name of Person Reporting: _____

Role/Job Title: _____

Date Reported: _____

Time Reported: _____

Email Address: _____

SECTION 2: INCIDENT DETAILS

Date Incident Occurred (if known): _____

Time Incident Occurred (if known): _____

Date Incident Discovered: _____

Time Incident Discovered: _____

Type of Incident

- ☐ Personal Data Breach
- ☐ AI-Related Incident
- ☐ Information Security Incident
- ☐ Cyber Security Incident
- ☐ Safeguarding Concern
- ☐ Near Miss
- ☐ Other

Please specify:

SECTION 3: DESCRIPTION OF INCIDENT

Please provide a detailed description of what happened.

SECTION 4: INFORMATION INVOLVED

Tick all that apply.

- ☐ Pupil Data
- ☐ Parent/Carer Data
- ☐ Staff Data
- ☐ Governor Data
- ☐ Visitor Data
- ☐ Safeguarding Information
- ☐ SEND Information
- ☐ Medical Information
- ☐ Financial Information
- ☐ Assessment Data
- ☐ Personnel Records
- ☐ Photographs
- ☐ Videos
- ☐ Other

Please provide details:

SECTION 5: NUMBER OF PEOPLE AFFECTED

Estimated number of individuals affected:

Names of affected individuals (if known):

SECTION 6: AI INCIDENT DETAILS

(Complete only if AI was involved)

Name of AI Platform Used:

☐ Microsoft Copilot

☐ Other

Please specify:

Did the incident involve:

☐ Personal Data

☐ Safeguarding Information

☐ SEND Information

☐ Medical Information

☐ Staff Information

☐ Assessment Information

☐ Photographs

☐ AI-Generated Images

☐ AI-Generated Audio

☐ Deepfake Content

☐ Other

Details:

Were prompts, outputs or screenshots preserved?

☐ Yes

☐ No

SECTION 7: IMMEDIATE ACTIONS TAKEN

Please describe any actions already taken to contain or minimise the incident.

SECTION 8: NOTIFICATIONS

Have the following individuals been informed?

Data Protection Officer (DPO)

☐ Yes

☐ No

Date/Time: _____

Headteacher

☐ Yes

☐ No

Date/Time: _____

Designated Safeguarding Lead (DSL)

☐ Yes

☐ No

☐ Not Applicable

Date/Time: _____

SECTION 9: EVIDENCE

Evidence available:

☐ Screenshots

☐ Emails

☐ Documents

☐ AI Prompts

☐ AI Outputs

☐ Messages

☐ Photographs

☐ Other

Please specify:

Location of evidence:

Incident Reference Number

Date Received

Investigation Summary

Has a Personal Data Breach Occurred?

☐ Yes

☐ No

☐ Further Investigation Required

ICO Notification Required?

☐ Yes

☐ No

Date Reported: _____

ICO Reference Number: _____

Individuals Notified?

☐ Yes

☐ No

Date: _____

Safeguarding Referral Required?

☐ Yes

☐ No

DSL Notified:

☐ Yes

☐ No

Date: _____

Actions Taken

Lessons Learned / Preventative Actions

☐ Staff Training

☐ Policy Review

☐ Technical Controls

☐ Additional Monitoring

☐ System Changes

☐ Provider Review

☐ Other

Details:

Incident Closed

Date Closed: _____

DPO Signature: _____

Headteacher Signature: _____

All incidents, including near misses, must be reported. Prompt reporting allows the school to assess risks, protect individuals, comply with UK GDPR and Data Protection Act 2018 requirements, and identify lessons learned to prevent recurrence.