Cotsford Primary School

Data Protection Policy

including Potential Breach Procedure

April 2026

Issue date	**April 2026**
Approved by governing body	Yes
Review Cycle	Every 2 years or as legislation or need arises
Next review date	April 2028
Staff responsible	Data Protection Officer
Circulation Details	All staff, Governors

1. Aims

Cotsford Primary 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 UK data protection law.

The school recognises its responsibility to process personal data in a fair, lawful and transparent manner and to protect the rights and freedoms of individuals.

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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, including name (including initials), identification number, location data or online identifiers such as username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	More sensitive data requiring additional protection, including information about: • 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	Any operation performed on personal data, including collection, organising, structuring, storage, adapting, altering, retrieving, using, sharing, erasing or deletion. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held processed
Data controller	A person or organisation determining the purposes and means of processing personal data (the school)
Data processor	A third-party processing data on behalf of the school
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

4. The data controller

Cotsford Primary School processes personal data relating to pupils, parents, staff, governors, visitors and others and is therefore a data controller.

The school is registered with the Information Commissioner's Office (ICO) and pays the required data protection fee.

5. Roles and responsibilities

This policy applies to all staff employed by the school, as well as to external organisations or individuals working on the school's behalf, including contractors, agency staff and volunteers.

Failure to comply with this policy may result in disciplinary action.

5.1 Governing body

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

5.2 Data Protection Officer (DPO)

The DPO is responsible for:

- Overseeing the implementation of this policy
- Our compliance with data protection law, and developing related policies and guidelines where applicable. These include the:
    - Acceptable Use Policy,
    - Record Keeping and Retention Policy,
    - Photographic and Video Policy
    - Policy and Freedom of Information statements

- Monitoring compliance with data protection legislation
- Providing guidance to staff on data protection matters
- Acting as the first point of contact for data subjects and the ICO

The DPO will:

- Carry out regular compliance audits
- Report findings and recommendations to the governing body
- Maintain oversight of data protection practices across the school

DPO Contact Details:
Aimee Burns
Email: p2532.admin@durhamlearning.net
Telephone: 0191 5864660

5.3 Headteacher

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
- Only accessing data where necessary for their role
- Reporting any data breaches immediately
- Keeping their own personal data up to date

Staff must contact the DPO if:

- They have any questions about this policy or have concerns that it is not being followed
- They are unsure whether or not they have a lawful basis for using the personal data in a particular way
- If they need help with any contracts or sharing personal data with third parties
- A data breach has occurred

6. Data protection principles

The UK GDPR is based on the following principles. Personal data must be:

- Processed lawfully, fairly and transparently
- 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 kept up to date
- Retained only as long as necessary
- Processed securely

The school will demonstrate compliance with these principles at all times.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The school will only process personal data where a lawful basis applies, including:

- 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 category data, an additional condition will be met, such as:

- 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.

Privacy notices will be provided to individuals at the point of data collection.

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

The school will not normally share personal data without consent unless required to do so by law however 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 UK 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 UK data protection law.

9. Subject access requests and individual rights

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 form, they must immediately forward it to the DPO.

Our procedure for handling of subject access requests is set out in Appendix 1.

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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

9.3 Responding to 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 1 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

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 access to educational records

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 follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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.

See our CCTV policy for further information.

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 for photographs and videos to be taken of our pupils for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used and will set this information out in photograph consent forms.

There may be a need to obtain one off consent during the year for specific events not covered by our photo consent form.

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. It may be necessary for us to prevent any photography by parents if we feel this is necessary to safeguard our pupils at particular events or in certain circumstances.
See our Photographic and Video Policy for further information.

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

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- On Class Dojo

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.

See our Photographic and Video Policy for more information on our use of photographs and videos.

13. Use of Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and

Google Bard. School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, school will treat this as a data breach, and will follow the personal data breach procedure.

14. 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)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- 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 UK, where different data protection laws may 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, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. Data security and storage

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 that are at least 10 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 (see our Online Safety and Acceptable Use Policies)
- 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)

16. Disposal of records

Personal data will be securely disposed of when no longer required.

- Paper records are shredded within school - we also use a third party to safely dispose of bulk records on behalf of the school. When we do this, we require the third party to provide sufficient guarantees that it complies with date protection law.
- Digital files are overwritten or permanently deleted.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

All breaches must be reported immediately.

The school will:

- Investigate breaches
- Notify the ICO within 72 hours where required
- Take action to prevent recurrence

18. Training

All staff and governors will receive:

- Data protection training as part of their induction process
- Ongoing updates as required

19. Monitoring arrangements

The DPO will monitor compliance and review this policy annually.

The governing body will approve the policy.

20. Links with other policies

This policy links to:

- Safeguarding Policy
- Acceptable Use Policy
- Online Safety Policy
- Record Keeping and Retention Policy
- CCTV Policy
- Data Breach Policy & Procedure
- Freedom of Information Scheme
- Photograph and Video Policy

Appendix 1: Subject Access Request Procedure

Individuals can submit a subject access request (SAR) to the school in any form. There are designated forms that can be filled in for such requests and these are available in school. However, requests can also be made verbally or in writing in other formats, for example via email.

The school may need to undertake checks where necessary on the identity of the individual making the request before releasing the information if this is not clear.

The process to be followed in the event of a member of staff receiving a SAR is as follows;