GROVE WOOD PRIMARY SCHOOL

Data Protection Policy

Date of Policy: October 2025
Date ratified by the Governing Body: 25th November 2025

Index

Data Protection Policy		
Version	**Date**	**Description of change**
1	May 2018	Updated Policy due to GDPR
2	March 2022	Policy reviewed and re-written to be more comprehensive
3	September 2022	• References to UK GDPR • Sentence under Data Security around removable media amended / clarified • Section added on Complaints
4	September 2024	• 2 yearly review • Sharing personal data – paragraph expanded to include Information sharing in an emergency medical or mental health emergency (page 7) • Section added on School Trips / Residentials (Section 12)

5	October 2025	Changes made, in relation to the Data Use & Access Act (DUAA) 2025: • Section 8 – Sharing personal data • Section 9 – Subject Access Requests • Section 19 - Complaints

1. Introduction

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 (DPA 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 GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our Funding Agreement and Articles of Association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.
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. 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 as a data controller with the ICO and will renew this registration annually or as otherwise 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.

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

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. 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 Mrs Sarah Mark and is contactable via the school office on 01268 743445 or at dpo@grovewood.essex.sch.uk

Headteacher: The headteacher acts as the representative of the data controller on a day-to-day basis, and is responsible for promoting a positive Data Protection culture within the school.

All staff, volunteers and contractor 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

6. UK GDPR/Data Protection Principles

The UK 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

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

e.g. 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**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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 which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

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

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.

It is recommended that staff regularly delete old emails or file them if they are still relevant.

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 Data Retention Schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where there is a Recognised Legitimate Interest:

- 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we

are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders
- The notification of contagious diseases
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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 to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Information sharing in an employee medical or mental health emergency

Data Protection law allows us to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm.

During a medical or mental health emergency where there is risk of serious harm to staff or to others, we will share necessary and proportionate information without delay with relevant and appropriate emergency services or health professionals. We may also share necessary and proportionate information with the member of staff's next of kin or emergency contact.

We will use our judgement in each specific situation, sharing only what is necessary and proportionate to the circumstances. We may decide that, whilst it may be necessary and proportionate to provide the emergency services with a full account of the situation, it is only appropriate to provide the member of staff's emergency contact with more limited details.

9. Subject Access Requests and Other Rights of Individuals (See Subject Access Request procedure for further information)

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
- 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.

Subject access requests can be made verbally or in writing (although we would recommend

that they be submitted in writing) , either by letter or email to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO, who will co-ordinate the response to the SAR. For further details, see the school's Privacy Notice available on our website.

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.

Responding to subject access requests

When responding to requests, we:

- Will ask the individual to provide two forms of identification & check regarding proof of relationship to the child.
- May contact the individual to confirm the request was made, and if necessary, to clarify the information required in order to ensure that the information provided meets their requirements rather than providing lots of information that may not be relevant to their query.
- We will conduct a reasonable and proportionate search
- We will not provide information that the requester already holds or has access to.
- Will respond without delay and within one month of receipt of the request: Exceptions to this may be:
    - The one month time limit will begin once we have received the required identification / checks regarding proof of relationship to the child.
    - Where further clarification of the information requested is sought (i.e. if we receive a broad request for all information the school holds). The one month time limit will begin once we have received the requested clarification.
    - when requests are made during school holidays, when the time limit may extend beyond one month or where the reply deadline falls within a school holiday period.
- Will provide the information free of charge in most instances*
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this

within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

*If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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. 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.

11. 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, when your child starts at the school. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, 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

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 "The use of photographs and video recordings" consent form for more information on our use of photographs and videos.

12. School Trips / Residentials

During School Trips and Residentials, certain records are required to be shared with the Residential provider and carried by a member of staff, including the medical details of pupils with complex medical needs, allergies or medication and the emergency contact details of the parents / carers.

During the trip, the records are held in physical form, stored in a secure document folder and kept with a member of staff at all times.

At the end of the school trip or residential, the trip lead will collect all copies of the medical records and emergency contact lists and destroy them in a secure manner.

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
- Completing privacy 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
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. 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 secure when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Any removable media (e.g. Hard Drives, memory sticks) are encrypted and supplied by the school. Staff are not permitted to use anything else.
- 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 Acceptable Use Policy Agreement)
- 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

15. 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 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.

16. 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 our Personal Data Breach procedure. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. 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.

18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and shared with the Governing Board and staff

19. Complaints

If an individual believes that the school has mishandled their personal data or that their data protection rights have been breached, they have the right to make a complaint.

You should raise any concerns with the School's Data Protection Officer – Mrs Sarah Mark on 01268 743445 or email dpo@grovewood.essex.sch.uk, or write to Grove Wood Primary School, Grove Road, Rayleigh, Essex, SS6 8UA. .

Complaints will be acknowledged by the school at the earliest opportunity, but at the latest within 30 days.

The school will take reasonable steps to investigate the concern without undue delay.

The individual who has raised the complaint will be informed of the outcome once the investigation has concluded.

If the individual is unsatisfied with how the complaint has been managed, they can escalate their concern to the Information Commissioner:

https://ico.org.uk/make-a-complaint/data-protection-complaints/

Telephone: 0303 123 1113

.

20. Links with other policies

This Data Protection Policy is linked to the following policies / procedures:

- Freedom of Information Publication Schedule
- Privacy Notices
- CCTV Policy
- Data Breach Procedure
- Subject Access Request Procedure
- Acceptable Use Policy Agreement
- Data Retention Schedule
- Third Party Requests for Information