This policy explains how The Grange CP School complies with UK Data Protection Law (UK GDPR and the Data Protection Act 2018). It sets out staff responsibilities, the role of the Data Protection Officer (DPO), and the rights of individuals. It also makes clear the responsibilities of the Headteacher and CAFO (Child and Family Officer) in safeguarding and data management.

All staff must:

- Handle personal data securely and lawfully

- Report any data breaches immediately to the DPO

- Only use personal data for legitimate school purposes

- Refer to this policy when collecting, sharing, storing, or deleting data

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 UK data protection law. This policy applies to all personal data, whether in paper or electronic format.

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.

It is based on guidance published by the Information Commissioner's Office (ICO), including the use of surveillance cameras and personal data. It also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005.

Definitions

TERM	DEFINITION
Special categories of personal data	Sensitive data requiring extra protection (e.g. racial or ethnic origin, political opinions, religion, health, genetics, biometrics, sexual orientation).
Personal data	Information relating to an identified or identifiable individual (e.g. name, ID number, location, online identifier).
Processing	Any operation on personal data (e.g. collecting, storing, using, sharing, deleting).
Data subject	The individual whose personal data is held or processed.
Data controller	The organisation that determines the purposes and means of processing (the school).
Data processor	A person or body processing data on behalf of the controller.
Personal data breach	A security breach leading to destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf.

Governing board
Has overall responsibility for ensuring compliance with data protection law

Data protection officer

Oversees compliance, advises staff, and reports annually to governors. The DPO is the first point of contact for individuals and the ICO. Our DPO is Tom Sadler – contactable via the school office (01295 257861).

Headteacher

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

All staff

Must follow this policy, report breaches, and contact the DPO when unsure.

Data protection principles

Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specific, explicit purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Processed securely

Collecting personal data

We will only process personal data where there is a lawful basis (e.g. contract, legal obligation, vital interests, public interest, legitimate interests, or consent). Special category data requires additional conditions, such as explicit consent or substantial public interest.

We will:
- Explain why data is collected at the time of collection
- Keep data accurate and up to date
- Delete or anonymise data when no longer needed (see retention schedule)

Sharing personal data

We will not share personal data without consent unless legally required or permitted (e.g. safeguarding, law enforcement, emergencies). Suppliers/contractors will only be appointed if they can guarantee GDPR compliance, and contracts will ensure lawful processing.

Rights of Individuals

Individuals have the right to:
- Access their personal data (Subject Access Request)
- Rectify or erase data in certain circumstances
- Restrict or object to processing
- Withdraw consent where given
- Data portability (transfer data to another provider)
- Not be subject to solely automated decisions
- Be informed of a data breach if high risk

Parents can request access to their child's educational record within 15 school days.

Subject Access Requests

Requests can be made in any format but should ideally include name, contact details, and the information requested. We will respond within 1 month (extendable to 3 months for complex requests). Proof of ID may be required. Requests should be sent to the DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, not their parents or carers. Parents may request access if the child is judged unable to understand their rights, or if the child consents. Children under 12 are usually considered not mature enough to understand their rights, but this is judged case by case.

Photographs and Videos

We obtain written consent for the use of photographs and videos for school purposes. Parents/carers must not share images of other children on social media without consent. School use may include displays, newsletters, website, and social media. Consent can be withdrawn at any time.

Data Security and Storage of Records

The school will apply robust technical and organisational measures to protect all personal data from loss, misuse, or unauthorised access. This includes:

Physical Security
- Paper records stored in locked cabinets when not in use.
- Offices/classrooms locked when unattended.
- Visitors supervised in areas where personal data is accessible.

Digital Security
- Strong passwords and two-factor authentication used for school systems.
- All devices (laptops, tablets, phones) encrypted and set to auto-lock.
- Data transferred only via secure networks — public Wi-Fi must not be used for personal data.
- Regular patching, updates, and antivirus protection maintained.

Access Controls
- Personal data access restricted to staff who require it for their role.
- User accounts removed immediately when staff leave the school.
- Shared drives and systems audited termly for access permissions.

Monitoring and Auditing
- ICT systems monitored for unusual activity or unauthorised access attempts.
- Annual penetration testing and system audits carried out by the school's IT provider.
- Staff use of systems logged and reviewed if concerns arise.

Artificial Intelligence (AI)
- Staff must not upload or process personal data in AI systems unless they are formally approved by the school and confirmed GDPR-compliant.
- Any AI use must be risk assessed through a Data Protection Impact Assessment (DPIA).
- AI tools must apply the same standards of encryption, access control, and retention limits as other systems.

Third Parties and Cloud Providers

- Only suppliers with demonstrable GDPR compliance and security standards will be used.
- Contracts must specify secure storage, breach notification duties, and limits on sub-processors.
- Data stored in the cloud must be hosted in the UK or countries with equivalent data protection safeguards.

Staff Responsibilities

- Never leave personal data (paper or digital) unattended.
- Always log out or lock devices when not in use.
- Report any suspected security weakness or breach immediately to the DPO.

Secure Transfer of Personal Data

Email

- Only school-issued email accounts may be used.
- Attachments must be password-protected and passwords shared via a separate channel (e.g. phone call, SMS).
- Highly sensitive data should be encrypted using approved software before sending.

Portable Media (USBs, CDs, etc.)

- Avoid use unless essential.
- Devices must be encrypted and signed in/out from the school office.
- Data must be deleted once transfer is complete.

Cloud-based Transfer (e.g. secure portals, shared drives)

- Use only platforms approved by the school/DPO that are GDPR-compliant.
- Access permissions must be minimised and reviewed regularly.
- Audit logs must be enabled where possible.

Paper Records

- Use sealed envelopes marked "Confidential" when sending via internal/external mail.
- Courier or recorded delivery must be used if sending offsite.
- Hand delivery requires records to be signed for on receipt.

Telephone/Verbal Transfer

- Only disclose personal data once the identity of the recipient is verified.
- Avoid discussing personal data in public or open spaces.

Data Sharing Agreements

- Where personal data is shared with external organisations, a formal data sharing agreement must be in place, setting out security expectations, responsibilities, and breach procedures.

Incident Logging

- Any transfer errors (e.g. mis-sent email, lost USB) must be reported immediately to the DPO and logged as a potential breach.

When personal data must be transferred outside the school or between staff, the following

Disposal of Records

Personal data no longer needed will be securely destroyed (e.g. shredding, deletion, wiping devices). Third-party disposal providers must guarantee GDPR compliance.

Personal Data Breaches

All suspected breaches must be reported immediately to the DPO (Tom Sadler). The DPO will investigate, contain, and assess whether to notify the ICO within 72 hours and affected individuals if required. All breaches will be documented and reviewed to prevent recurrence.

Training

All staff and governors receive data protection training on induction and through CPD when legislation or procedures change.

Monitoring Arrangements

The DPO monitors compliance with this policy. It is reviewed annually and approved by the full governing board.

Links with Other Policies

This policy is linked to our Freedom of Information Publication Scheme, ICT/Online Safety Policy, and Safeguarding Policy.

Data Protection Policy 2025-26 APPROVED