Scotforth St Paul's CE Primary and Nursery School

Learning, growing and caring as part of God's family.


Jesus (the gardener) nourishes and tends us as we learn and grow, so that we can all flourish. As a vine, we are one, but all unique and special to Him. We care for each other, as God cares for us.

# Data protection policy

| | | |
|---|---|---|
| **Approved by:** | BHS committee | **Date:** 03.02.26 |
| **Next review due by:** | Spring 2027 | |
| **Changes** | | |
| **03.02.26** | 4. Data Protection fee<br>11A. Biometric recognition systems<br>14A. Artificial Intelligence<br>18. Training<br>20. Links with other policies | |

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance 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

Personal data: Any information relating to an identified, or identifiable, living individual, which may include name (including initials), identification number, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data: Personal data which is more sensitive and needs more protection, including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (where used for identification), health, 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 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

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

Scotforth School is registered with the ICO / has paid its data protection fee to the ICO.

## 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.

5.2 Data protection officer (DPO): The 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 Amanda Malin and is contactable via a.malin@scotforth-st-pauls.lancs.sch.uk.

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; informing the school of any changes to their personal data; and contacting the DPO with any questions about data protection, lawful bases, consent, privacy notices, data subject rights, data transfers outside the UK, and to report suspected data breaches or new activities that may affect privacy rights. Whenever they need help with any contracts or sharing personal data with third parties, staff must contact the DPO.

## 6. Data protection principles

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

• Accurate and, where necessary, kept up to date

• Kept for no longer than is necessary

• 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 six lawful bases to do so under data protection law (contract, legal obligation, vital interests, public task, legitimate interests, consent).

For special categories of personal data, we will also meet one of the special category conditions (explicit consent; employment, social security or social protection law; vital interests; manifestly public; legal claims; substantial public interest; health or social care purposes; public health; archiving/research/statistics).

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

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 processing and ensure we do not handle personal data in ways individuals would not reasonably expect or that have unjustified adverse effects.

7.2 Limitation, minimisation and accuracy: We will only collect personal data for specified, explicit and legitimate reasons, explain these reasons at the point of collection, and inform individuals before any new use. Staff must only process personal data where necessary for their job roles. We will keep data accurate and up to date, rectifying or erasing inaccurate data when appropriate. When staff no longer need personal data, they must delete or anonymise it in line with the school's record retention schedule.

## 8. Sharing personal data

We will not normally share personal data with anyone else without consent, but may do so when required—for example, where safety risks exist, where we must liaise with agencies, or where suppliers/contractors need data to provide services. We will appoint suppliers or contractors that can provide sufficient guarantees of compliance with UK data protection law, put contracts in place to ensure fair and lawful processing, and only share data necessary for the service.

We will share personal data with law enforcement and government bodies where legally required, and with emergency services/local authorities to respond to emergencies affecting pupils or staff. International transfers will be in accordance with UK 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 held about them, including confirmation of processing, a copy of data, purposes, categories, recipients, retention periods, rights, source, automated decision-making, and safeguards for international transfers. Requests can be made in any form; written requests with name, address, contact details, and information requested may help us respond more quickly. Staff must immediately forward any requests to the DPO.

9.2 Children and subject access requests: 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: We may ask for two forms of identification, may contact the individual via phone to confirm the request, will respond without delay and within one month (or up to three months for complex or numerous requests with notice), and will provide information free of charge unless the request is unfounded or excessive. We may withhold information where disclosure could cause serious harm, reveal abuse where disclosure is not in the child's best interests, include another person's personal data that cannot be reasonably anonymised, or is part of certain sensitive documents (e.g., legal proceedings, management forecasts, confidential references, exam scripts).

When we refuse, we will explain why and inform the individual of their right to complain to the ICO or seek enforcement through the courts.

9.4 Other rights: Individuals have the right to withdraw consent, request rectification/erasure/restriction, prevent use for direct marketing, object to processing based on public interest/official authority/legitimate interests, challenge automated decisions/profiling, be notified of a data breach (in certain circumstances), make a complaint to the ICO, and request data portability (in certain circumstances). Requests to exercise rights should be submitted to the DPO, and staff must immediately forward such requests 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 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.

Any enquiries about the CCTV system should be directed to Amanda Malin (School Business Manager).

## 11A. Biometric recognition systems

Scotforth School does not use biometric recognition systems for pupils, staff, or other adults. If this position changes, the school will comply with the Protection of Freedoms Act 2012, obtain appropriate consents, and provide alternative access methods for anyone who does not consent.

## 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 and in school magazines, brochures, newsletters, etc.; outside of school by external agencies such as the school photographer, newspapers; and 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.

## 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; only processing personal data that is necessary for each specific purpose; completing data protection impact assessments for high-risk processing or new technologies (with DPO advice); integrating data protection into internal documents including this policy, related policies and privacy notices; regularly training members of staff and keeping attendance records; conducting reviews and audits to test privacy measures; putting appropriate safeguards in place for transfers outside the UK; and maintaining records of our processing activities.

## 14A. Artificial intelligence (AI)

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 other similar tools. Scotforth 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 is 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, Scotforth School will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

## 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, staffroom tables, or elsewhere with 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 devices; encryption software is used to protect portable devices and removable media; 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; and we carry out due diligence and take reasonable steps to ensure third parties store shared personal data securely and adequately protect it.

## 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 and will require sufficient guarantees of compliance with data protection law.

## 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 1. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Examples include: publishing a non-anonymised dataset on the school website, safeguarding information being made available to an unauthorised person, and the theft of a school laptop containing non-encrypted personal data about pupils.

## 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 (CPD), where changes to legislation, guidance or the school's processes make it necessary.

## 19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the full governing body.

## 20. Links with other policies

This data protection policy is linked to our Freedom of information publication scheme and Privacy notices. It should be read alongside relevant policies such as our online safety/ICT acceptable use policy, CCTV policy, child protection and safeguarding policy, and our policy on the use of photographs and videos.

## 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) by emailing bursar@scotforth-st-pauls.lancs.sch.uk.

The DPO will investigate the report and determine whether a breach has occurred, considering whether personal data has been lost, stolen, destroyed, altered, disclosed or made available where it should not have been, or made available to unauthorised people. Staff and governors will co-operate with the investigation; it will not be treated as a disciplinary investigation.

If a breach has occurred or is likely, the DPO will alert the headteacher and the chair of governors, make reasonable efforts to contain and minimise the impact (with support from relevant staff or external providers where necessary), assess potential consequences, and determine whether the breach must be reported to the ICO and the individuals affected (using the ICO's self-assessment tool). Decisions will be documented and stored on the school's computer system.

Where the ICO must be notified, the DPO will report via the ICO website ("report a breach" page) or through its breach report line (0303 123 1113) within 72 hours of awareness, setting out the required information. If all details are not yet known, the DPO will report as much as possible within 72 hours, explain any delay, and submit remaining information as soon as possible.

Where required to communicate with individuals affected, the DPO will notify them in writing with a clear description of the breach, contact details, likely consequences, and measures taken. The DPO will consider notifying relevant third parties (e.g., police, insurers, banks) who can help mitigate loss.

The DPO will document each breach regardless of reporting, including facts and cause, effects, actions taken, and steps to prevent recurrence (e.g., more robust processes, further training). Records of breaches will be stored on the school's computer system. The DPO and headteacher will meet to review what happened and how to prevent future incidents, as soon as reasonably possible.

Actions to minimise the impact of data breaches will be reviewed and amended after any breach. Examples include: attempting to recall emails containing sensitive information sent in error; requesting unauthorised recipients to delete information and confirm deletion; and conducting internet searches to ensure information has not been made public.