

Data Protection Policy



Person Responsible for Policy:
Claire McKinney (Head Teacher)

Date of Adoption by Governing Body:
Summer 2025

Date of next review:
Summer 2026

1. Introduction

- 1.1. The School's Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and associated legislation, and guidance from the Information Commissioner's Office (ICO).
- 1.2. The DPA gives individuals rights over their personal data and protects the use of personal data.
- 1.3. The School is registered with the ICO as a Data Controller for the processing personal information.

2. Purpose

- 2.1. The School Data Protection Policy has been produced to ensure its compliance with the DPA 2018.
- 2.2. The Policy incorporates guidance from the ICO, and outlines the approach to its responsibilities and individuals' rights under the DPA 2018.

3. Scope

- 3.1. This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the School), third parties and others who may process personal information on behalf of the School.
- 3.2. The Policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the relevant School to ensure the data is processed in accordance with the DPA 2018 and that students and staff are advised about their responsibilities.

4. Data covered by the Policy

- 4.1. Special category personal data is personal data consisting of information relating to:
 - Racial or ethnic origin
 - Political opinions,
 - Religious or philosophical beliefs
 - Membership of a trade union
 - Physical or mental health or condition
 - Sexual life or sexual orientation
 - Commission or alleged commission of any offence
 - Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5. The Six Data Protection Principles

- 5.1. The DPA 2018 requires the School, its staff, and other organisations who process personal information on behalf of the school, to comply with the six data protection principles.
- 5.2. The principles require that personal data shall:

- Be obtained and processed fairly, lawfully and in a transparent manner
- Be obtained for a specified and lawful purpose and shall not be processed in a manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purpose
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage

6. Responsibilities

- 6.1. The School has a designated Data Protection Officer (DPO) to support and advise on day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations.
- 6.2. All new members of staff will be required to undertake mandatory Data Protection Awareness training as part of their induction, and existing staff will be requested to undertake refresher training on a regular basis.
- 6.3. Employees of the School are expected to:
 - Familiarise themselves and comply with the six data protection principles
 - Ensure any processing of personal data is accurate and up to date
 - Ensure their own personal information is accurate and up to date
 - Ensure that they only have access to data they need in order to do their daily jobs and inform their manager and the ICT team if they notice that they can access data they shouldn't be authorised to
 - Keep personal data for no longer than is necessary

- Ensure that any personal data they process is secure and in compliance with the School's information related policies and strategies
 - Acknowledge data subjects' rights (e.g. right of access to all their personal data held by the School) under the DPA 2018, and comply with requests to exercise those rights
 - Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the
 - Obtain consent where necessary to collect, share or disclose personal data
 - Contact the DPO for advice if they have concerns or are in doubt about data protection requirements to avoid any infringements of the DPA 2018.
- 6.4. Students of the School are expected to:
- Comply with the six data protection principles
 - Comply with any security procedures implemented by the School.

7. Obtaining, Disclosing and Sharing

- 7.1. Only personal data that is necessary for a specific reason related to the provision of education or employment by the School should be obtained. Under DPA, there are six lawful bases for processing personal information:
- The data needs to be processed so that the School can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract (e.g. employment)
 - The data needs to be processed so that the Trust can comply with a legal obligation (e.g. Education Act 2006, Children's Act 2004)
 - 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 Trust, as a public authority, can perform a task in the public

interest, and carry out its official functions (e.g. deliver education)

- 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 (e.g. school trips, photos)

For special categories of personal data, as identified at 4.2, School will also meet one of the special category conditions for processing which are set out in the Article 9 of the GDPR and Ch.2, Para. 10 of the Data Protection Act 2018.

Where the school relies upon a condition in Article 9(2)(g) for processing special category information - necessary for reasons of substantial public interest - it will maintain an appropriate policy document.

- 7.2. Students, staff and governors are informed about how their data will be processed via the School's Privacy Notices.
- 7.3. Upon acceptance of employment at the School, members of staff also agree to the processing and storage of their data.
- 7.4. Data must be collected and stored in a secure manner.
- 7.5. Personal information will not be disclosed to a third party organisation without the prior consent of the individual concerned unless required by law (see 7.6 below). This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the School.
- 7.6. The School may have a duty to disclose personal information in order to comply with a legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any queries or concerns regarding

requests to disclose personal data should be directed to the DPO at Data.Protection@sunderland.gov.uk.

- 7.7. Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.
- 7.8. Where a third party processes information on behalf of the School, School will only use organisations that provide sufficient guarantees that they have technical and organisational measure in place to safeguard the information. All such processing will be governed by a contract.

8. Retention, Security and Disposal

- 8.1. Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they should inform the Head Teacher or the School's DPO
- 8.2. Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with principle 2 and principle 4 of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.
- 8.3. In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.
- 8.4. In accordance with the School's Flexible Working Scheme, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others (see also 9.5).

- 8.5. All departments should perform regular review of their data to ensure that it is destroyed in accordance with the Retention Schedule when it is no longer required.
- 8.6. Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to the School's I.T provider for safe disposal. Hardware should be appropriately rendered redundant and disposed of in compliance with the School's I.T service provider contract and to ensure it conforms with DPA and GDPR requirements.

9. Transferring Personal Data

- 9.1. Any transfer of personal data must be carried out securely in line with the framework provided by the following:
 - Data Protection Act 2018 and GDPR
 - Caldicott: To Share or not to Share – The Information Governance Review 2013
 - The ICO Code of Practice on Data Sharing 2015
 - Information Sharing Advice for Safeguarding Practitioners 2015.
- 9.2. Email communications should be assessed for risks to individuals' privacy. Wherever possible, sending personal data via encrypted email should be the preferred transit medium, with a password provided to the recipient by a separate medium.
- 9.3. Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly, and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.
- 9.4. Personal email accounts should not be used to send or receive personal data for work purposes.
- 9.5. Staff and governors are not permitted to store personal information locally on personal devices (i.e. on the local

hard drives of phones, USBs, laptops); only school-approved devices should be used. Personal devices should only be used for cloud-based access to school systems.

- 9.6. Staff must not devise or implement their own local, tacit methodologies and systems for recording pupils' personal information. All recording should be on appropriate school systems subject to a documented authorisation/approval process.

10. Data Subjects Right of Access (Subject Access Requests)

- 10.1. Under the DPA 2018, individuals (including staff and students) have the right to request access to their personal data held by the School. This applies to data held in both paper and electronic format, and within a relevant filing system.
- 10.2. The School may, with the advice of the DPO, use its discretion under the DPA 2018 to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.
- 10.3. Any individual who wishes to exercise this right should make the request in writing or via the submission of a Subject Access Request Form.
- 10.4. The School may not charge a fee. It will only release any information upon receipt of a valid request, along with proof of identity, or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information, or reason for refusing a request, will be provided within the statutory timescale of 1 calendar month from receipt of a valid request.

11. Reporting a Data Security Breach

- 11.1. It is important the School responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School systems, unauthorised use of personal data, accidental loss or equipment failure.

Any data breach should be reported to the DPO at Data.Protection@sunderland.gov.uk immediately upon its discovery and if it relates to an IT incident (including information security), should also be reported to the Head Teacher and in certain circumstances to the School's I.T provider. Please refer to the Data Breach Policy for more information.

- 11.2. Any breach will be investigated in line with the procedures within the Data Breach Policy. In accordance with that Policy, the School will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

12. Policy retention and review

- 12.1. This policy will be reviewed annually in November each year.
- 12.2. A copy of the policy in place from time to time will be retained until the end of the period of 6 months beginning on the day processing under that version of the policy ceases.