GDPR Data Protection Policy

Policy reviewed by:	**Safety and Wellbeing Committee**
Meeting:	**Autumn**
Review frequency:	**2 Year**
Approved:	**December 2025**
Next Review:	**December 2027**

This is Selly Oak Trust School's GDPR and Data Protection Policy on how it looks after Student, Staff and Governor personal information in accordance with the Data Protection Act 1998.

The school needs to keep certain information about its governors, employees, students and their parents to allow it to carry out its functions as a school and to monitor performance, achievements and health and safety. In doing so, the school will comply with the terms of the Act to ensure that personal information is treated in a manner that is fair and lawful. The school Data Protection Registration can be viewed at:-
http://forms.informationcommissioner.gov.uk/search.html)

As a school in order for staff to fulfil the requirements of a contract we need to adhere to Article 5 of the GDPR. We do not require permission from staff to use/share their personal data, but we have a statutory obligation to ensure it is secure.

Article. 5 GDPR Principles relating to processing of personal data:

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational

measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 4 - GDPR Definitions:

For the purposes of this Regulation:

1. 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. 'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.

4. 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

5. 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

6. 'Filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

As a School:

- We have a privacy notice on our website relating to GDPR ,
- We have updated our consent for parents for photo /video permission,
- no longer permit the staff to use USB sticks to transfer information from school to home – staff can access their files via the cloud,
- Staff using email on their phones have high security settings and data is password protected , staff using PC's must have their PC's locked when not in use,
- Emails transferring from school to outside agencies which contain personal information are password protected documents,
- Completed Data Protections impact assessment (DPIA)– this is a detailed log of the information /systems we hold/share about staff and students,
- Up to date with our Anti-Virus software,
- Updating our staff exit procedure to include the removal of any emails from personal devices.

The school will ensure that all staff or others who gather and use personal information on the school's behalf will always follow these principles. In order to ensure that this happens, the school has developed this data protection policy. Data protection statements will be included in the school prospectus and on any forms that are used to collect personal information.

The Data Controller and the Compliance Officer

Selly Oak Trust School as a body corporate is a 'data controller' under the Act. To assist the school in carrying out its obligations under the Act properly, it has appointed a data protection Compliance Officer who will help governors, staff and parents deal with day-to-day queries about looking after and properly using personal information. Any member of the governing body, staff, student or any other individual who considers that this policy has not been followed in respect of personal data about himself or herself may, in the first instance, raise the matter with the Data Protection Compliance Officer (Sarah Simmons, Strategic Business Manager).

If you are not satisfied about any aspect of how the School gathers and holds personal information, in addition to the rights contained in this policy you have a right to discuss and/or complain to the Office of the Information Commissioner (www.informationcommissioner.gov.uk/) whose address is:

Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF
Tel: 01625 545700

Data Gathering:

- All personal information relating to governors, staff, students or other people with whom the school has contact, whether held on computer or in paper files, are covered by the Act.

- Only relevant personal information may be collected and the person from whom it is collected should be informed of the intended use of the data and of any possible disclosures of that information which may be made. Wherever possible, the school will try and get consent from the relevant data subject (or their parent or legal guardian) to hold and use that information.

- Where the school collects information which is of a more sensitive nature (for example details of any medical conditions which students have and which the school needs to know about), the school will obtain explicit consent from the parents and/or students in respect of its holding of that information.

Data Checking:

The school will issue regular reminders to staff and parents to ensure that the personal information which it holds is up to date and accurate. Governor personal details will be maintained by the Headteacher's PA and the Governor Support Service, Dudley Metropolitan Borough Council.

Staff details are maintained by Sarah Simmons, Strategic Business Manager, and Michaela Edwards, HR Recruitment and Induction Lead.

Responsibility of Parents:

Students and their parents should ensure that all personal information provided to the school is accurate and up to date. They should ensure that changes of address etc. are notified to the school. The school cannot be held responsible for any errors unless the parent/carer has informed the school of such changes.

Subject to the above, any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, recipients are informed of the corrected data.

Data Storage:

The school shall ensure that:

- Any personal information held in respect of students is kept securely,
- The personal information is not disclosed either orally or in writing or electronically or by any other means accidentally or otherwise to any unauthorised third party.

Personal information shall:

- In respect of manual data, be stored by the school in a secure and safe manner. It shall be kept in a locked filing cabinet, drawer or safe where it is inaccessible to anyone who does not have a legitimate reason to view or process that information.
- In relation to electronically stored information, to be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.
- Computer workstations in administrative areas be positioned so that they are not visible to casual observers waiting either in the office or the reception hatch.

Your right of access to personal information held about you/your child.

All people for whom the school holds personal information on are entitled to: -

- Know what information the school holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date if the school's information is or becomes out of date.
- Know what the school is doing to comply with its obligations under the Act.
- A right under the Act to access certain personal data being kept about them either. If the school sees a written request from a data subject (a child or their parents / legal guardians) to see any or all personal information that the school holds about them, the school will respond within 40 days, as required by the Act. The maximum charge for this is

£150. Please note that the charges and timings of disclosures to students/parents of educational records are different (see below).

- The Act gives all students, regardless of age, the right of access to their school student records. Requests to see or receive copies of records should be made in writing to the Headteacher.

- In addition to the right to be given a copy of the educational record, students are entitled to be given a description of the personal information which makes up the record, together with details of the purposes for which the information are processed, the sources of the information (if known) and the individuals or organisations to which the information may have been disclosed.

- A period of up to 40 calendar days or 15 School days (whichever is the greater) is allowed in which to respond to a subject access request. The equivalent period for other types of records is up to 40 days. If asked to provide a hard copy of the record, a fee may be charged according to the number of pages. See below for the scale of charges. Students may be asked for information to verify their identity if it is necessary, for instance in the case of former students who may not be currently known to the school. They may also be asked for information necessary to locate the data held about them. For instance, a student may be asked to supply the dates between which he or she attended the school.

- Only in exceptional cases will the school be able to withhold some of the information which is requested by a student. For example, information does not have to be disclosed by the school where that information might cause harm to the physical or mental health of the student or a third party. Also, information which may identify third parties (for example other students, although not teachers), and information which forms part of some court reports are exempt from disclosure by the school. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

- If students are incapable of understanding or exercising their own rights under the Act, (for instance because they are too young or because of the special educational need parents and carers can, of course, make subject access requests on their behalf.

- Parents have an independent right of access to student records (under the Education Student Information (England) Regulations 2000). Because of this, the students themselves have no right to prevent their parents from obtaining a copy of their school record.

- Subject Access Fees – access by students and/or parents' carers

No of Pages	Minimum Fee
1-19	£10
20-29	£20
30-39	£30
40-49	£40
50-59	£50
60-69	£60
70-79	£70
80-89	£80
90-99	£90
100-149	£100
150+	£150

Disclosing information to third parties:

- Personal information will only be disclosed to organisations or individuals for whom consent has been given to receive the data

Further information on the Act, how it works and your rights under it are available from the Office of the Information Commissioner (the organization which oversees the Act) at: www.informationcommissioner.gov.uk/gdpr

GDPR and CCTV:

Our CCTV policy balances robust safeguarding for vulnerable pupils with GDPR/Data Protection laws, focusing on specific purposes (safety, crime prevention, asset protection) there is limited access to footage, and we avoid privacy invasion (toilets cubicles and changing rooms).

Core Principles for Special Schools:

Vulnerable Learners: Policies reflect heightened duty of care, often requiring stricter controls and more training for staff handling sensitive footage of vulnerable students.
Lawful Basis: Justified under GDPR viewer consent for watching CCTV for the purpose of (see below) is justified.
Purpose Limitation: Only for safety, crime prevention, safeguarding, student or staff incidents of misconduct, acts of crime, property protection; not for the purpose of general student/staff monitoring.

Key Policy Components:

Siting & Coverage:

Cover entrances, corridors, grounds, restorative center, dining hall. Toilet area on the middle floor outside of cubicles.

The CCTV systems are only used for visual purposes not sound.

Access & Security:

The Headteacher, ICT Manager, Assistant Head (Behaviour) and Data Protection Officer have access to CCTV footage. Any other person(s) requesting footage must seek authority from the Headteacher.
Secure storage (NVR/DVR) with cybersecurity. Key staff have received Cyber Security Training.
Record & log all disclosures: CCTV usage for the purpose of the above should be logged.
Data Handling: Footage is set for a maximum period of 31 days then securely erased.
Obscure other people's faces when releasing footage to individuals.
Staff Training: Key staff have been trained in cyber security, GDPR, Data Protection, privacy, and handling sensitive situations.
Review: Reviewed to ensure ongoing necessity and compliance, triggered by legal changes.
Heightened Safeguarding: CCTV supports existing safeguarding policies, especially crucial for students with complex needs.
Proportionality: Camera use is proportionate and doesn't unnecessarily intrude on a student's citation of privacy, even in public areas of the school.
This policy complies with UK GDPR and the Data Protection Act 2018.

Appendix – SIPS Education document

'Data Protection and Coronavirus, Guidance on what you may need to Know'
[The ICO is the Information Commissioner's Office]

The ICO recognises the unprecedented challenges faced during and post the pandemic.

They know you might need to share information quickly or adapt the way you work. Data protection will not stop you from doing that. It's about being proportionate - if something feels excessive from the public's point of view, then it probably is.

SIPS are here to help your school. If you need any advice, please call us on 0121 296 3000

Please see Addendum – Cyber Security Standards for Schools on the following page.

Data Protection Policy addendum January 2025

Cyber Security Standards for Schools:

Cyber incidents and Cyber-attacks have significant operational and financial impacts on schools. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group or organisation outside or inside the school and can lead to:

- Safeguarding issues due to sensitive personal data being compromised.
- Impact on student outcomes.
- A significant data breach.
- Significant and lasting disruption, including the risk of repeated. future cyber incidents and attacks, including school closure.
- Financial loss.
- Reputational damage.

Annually - All staff will be made aware of the risks associated with their hardware, software and data to properly mitigate and defend against any potential cyber incidents or attacks including: -

- Understanding how to keep students, staff and the wider school community safe.
- Understanding how prepared the school is in response to a cyber incident or attack.
- Highlighting weaknesses and put processes in place to help reduce risk.
- Securing systems to make sure they are more resilient to cyber incidents and attacks.
- Preparing a cyber response plan to be implemented quickly in the event of a serious incident to minimise any impact to the school or college.

Protecting user accounts and related data is a critical line of defence against cyber incidents and attacks. The Headteacher will ensure that:

- Personal data and digital technology are as safe and secure as they can be.
- Students, staff and third parties only have access to the things they need.

ICT support will work with:

- Any digital technology suppliers to make sure they are also compliant with this standard.
- The data protection officer (DPO) who will, if needed, undertake a data protection impact assessment (DPIA) and provide advice on data protection legislation compliance
- The Strategic Business Manager and HR Lead for setting up a process for movers, starters and leavers.

How to report a cyber security attack:

Cyber incidents can take many forms, such as denial of service, malware, ransomware or phishing attacks.

Types of activities that are commonly recognised as being a cyber incident are:

- Breaches of a system's security policy that affects its integrity or availability.
- Attempts to gain unauthorised access to a system or to data
- Changes to a system's firmware, software or hardware without the system owner's consent.
- Malicious disruption.

If the cyber incident is an emergency, then call 999, if one of the following applies:

- There is danger to life.
- Serious injury has been caused to a person.
- Serious damage has been caused to property.

If you do not need the emergency services, then attacks should be reported at this link Where to report a cyber incident - GOV.UK

At least one governor has completed the Cyber Security Training.
At least one member of the Senior Leadership Team and the ICT Manager have completed the Cyber Security Training.