POLICY

Type of Policy:	MAT Policy to adopted in full across all schools	✓
	LGB Policy to be reviewed and approved locally	

Approval Date:	**2023/24 – AUTUMN TERM (TB)**
Review Date:	**2024/25 – AUTUMN TERM**

SOUTH EAST LONDON CATHOLIC ACADEMY TRUST (SELCAT)

DATA PROTECTION POLICY

Our Vision, Mission & Values

To create a family of schools that together, through shared support and challenge, strive to provide a distinctive Catholic education where all children will be empowered, inspired and flourish. We will aim for excellence and to become remarkable places of learning and love.

Our commitment
SELCAT is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles.

The legal basis for processing data at the Trust is that it is necessary to carry out these tasks in the public interest.

The Trust is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them. The requirements of this policy are mandatory for all staff employed by the Trust and any third party contracted to provide services within the Trust.

This policy is intended to ensure that all personal data is processed in compliance with the Principles of the Data Protection Act 1998 and The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation

Notification
Our data processing activities are registered with the Information Commissioner's Office (ICO).

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The Trust has a separate CCTV Policy.

The Trust collects a large amount of personal data every year from both staff and students. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

2. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1) Data must be processed fairly and lawfully.
2) Personal data shall be obtained only for limited purposes.
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4) Personal data shall be accurate and where necessary kept up to date.
5) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

6) Personal data shall be processed in accordance with the rights of data subjects.
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8) Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Responsibilities

3.1 The Trust must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

3.2 The Trust has a legal responsibility to comply with legislation. The Trust, as a corporate body, is named as the Data Controller.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with legislation.

3.3 The Trust is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website.

3.4 Every member of staff that holds personal information has to comply with the data protection policies when managing that information.

3.5 The Trust is committed to maintaining the eight principles at all times. This means that the Trust will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as Subject Access Requests

- train all staff so that they are aware of their responsibilities and of the Trust's relevant policies and procedures

4. Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

5. Justification for personal data

We will process personal data in compliance with all data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

6. Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

7. Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

8. Data portability

A data subject may also request that their data is transferred directly to another system. There is no charge for this service.

9. Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

10. Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Trust will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

11. Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

12. Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

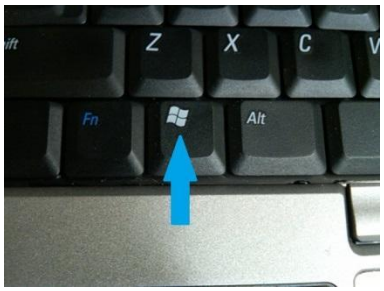
13. Clean Desk Policy

A clean desk policy is one of the simplest ways to protect sensitive information and to reduce the risk of a data breach and/or identity theft. Colleagues should leave their working spaces at the end of the day clear of all papers containing sensitive information such as personal data.

Sensitive information should be locked away in drawers/cabinets as appropriate and in addition should never be disposed of via the rubbish or recycling bins but instead shredded.

14. Computer Systems

If you are away from your computer during the day, then you are required to “lock” your system (Win Key + L)



At the end of the working day you should power down the computer completely.

This prevents unauthorised access to sensitive information by individuals using your credentials.

15. Physical Security

It is important to lock rooms when not in use to deter individuals from gaining unauthorised access to areas that may contain sensitive information.

Changes to Data Protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

DATA SUBJECT ACCESS REQUEST

Application No..... (office use only)

Due Date (office use only)

SECTION 1 Data Subject's details * PLEASE USE BLOCK CAPITALS

Mr/Mrs/Ms/Miss/Dr/Other

Forenames
.....

Surname
.....

Date of Birth
.....

Previous surname or also known as (if applicable)
.....

Date of any change of name
.....

Address
.....

.....

** If you are not the Data Subject and are applying on behalf of someone else, please insert their details above and not your own. Please also complete Section 2*

Please give any other details to help us with our search; for example: any dates which may be relevant, reference numbers on correspondence or applications, names of responsible officers, signatories on letters….

.....

.....

I DECLARE THAT I AM THE DATA SUBJECT AND THAT THE INFORMATION GIVEN ON THIS FORM IS CORRECT TO THE BEST OF MY KNOWLEDGE.

Signature..... Date.....

SECTION 2 Applicant's details * PLEASE USE BLOCK CAPITALS

** Please complete this section with your details if you are acting on behalf of someone else (the Data Subject). The Data Subject must consent to us disclosing their information to you by countersigning your application.*

I confirm that I am acting on behalf of the Data Subject and have submitted proof of my authority to do so.

Mr/Mrs/Ms/Miss/Dr/Sir/Other

.....

Relationship to Data Subject

.....

Surname

.....

Forenames

.....

Address

.....

.....

Signature of authorised representative.....

Signature of data subject.....

The information you have provided will be held and used by SELCAT for the purpose of searching our records and processing your enquiry. The search process may require us to share this information with partner organisations and other local authorities or agencies that provide services on our behalf.

Please read these notes carefully before completing the details on the form

1. **Who may apply for information?** Only the individual who the personal information is about (*the Data Subject*). This means that you can only apply for your own personal information *(referred to as a Data Subject Access Request)*. You cannot apply for information about anyone else; neither can anyone else apply for information about you. You may wish to nominate someone to be your authorised representative and the information can then be released to them with your consent. Please see paragraph 6 below for access to your child's personal information.

2. **What does it cost?** Information is provided free of charge, however SELCAT reserves the right to charge a reasonable fee when a request is manifestly unfounded, excessive or repeated. The fee will be calculated based on the administrative cost of providing the information, and will be communicated to the Data Subject prior to the request being fulfilled.

3. **How soon will I get an answer?** Within 30 calendar days of SELCAT receiving your written request and proof of identity.

   It is important to be as specific as possible when requesting your personal information. If we do not have enough information to begin our search, we will contact you and ask you for more details. In these circumstances, the 30 day response time will begin from the day we receive sufficient information from you to proceed.

4. **Will I be able to understand it?** Yes. We must provide the personal information we hold in a form that you can understand, explaining any abbreviations.

5. **Identification.** We must not knowingly give personal information to the wrong person and we must do our best to ensure that the personal information we have been asked for is given only to the person to whom this information refers, or their authorised representative. Therefore, where we have been unable to confirm your identity, we will be asking you for proof of both your identity and address before we hand any information over to you. If we are posting information, we will send it to the person that the information is about, or their authorised representative. Your signature at the bottom of the form declares that you are that person requesting your own information, or you have authorised someone else to act on your behalf.

6. **Children.** Children have the same rights of access to their own personal information as adults, and the same rights of privacy. There is no minimum age in English law, but current practice accepts that in general, a child of or over the age of 12 years is considered capable of giving consent. When a subject access request is received from a child, we will assess whether the child has the capacity to understand the implications of their request and of the information provided as a result of that request. If the child does understand, then their request will be dealt with in the same way as that of an adult. If a parent or legal guardian makes a request on behalf of a child, the request will only be complied with when we receive assurances that the child has authorised the request and that their consent was not obtained under duress or on the basis of misleading information. If the child does not understand, then a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the best interests of the child.

   Requests to see or receive copies of educational records should be made in writing to the Headteacher accompanied by a Data Subject Access Request.

7. Please complete and return this form to the address below

As part of the acknowledgement you will be asked if necessary for proof of identity (e.g. copy of passport or photo driving licence), proof of current address (e.g. copy of recent utility bill or the address section of your last bank statement) and if you are applying on someone else's behalf, proof that they have given consent for you to be doing this.

Send to:

Data Protection Officer
SELCAT
DPO@selcat.org

Shirley Court
c/o Coloma Convent Girls' School
Upper Shirley Road
Croydon
CR9 5AS