ST TERESA
OF CALCUTTA
CATHOLIC ACADEMY TRUST

GDPR Policy

Document Control

Policy Level	Trust/Statutory	Ref No	ADM03
Approved by	Directors	Approved date	29th June 2021
Responsibility	CFO	Next review	Summer Term 2023
Published location			
Version number	Date Issued	Author	Update Information
1.0	1st September 2021		

Contents

1.0 Policy statement

1.1 The Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the EU's General Data Protection Regulation (GDPR). These guidelines still apply following the UK's exit from the EU.

1.2 The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially children's services.

2.0 Scope and Purpose

1.3 This policy is in place to ensure that all staff, governors and directors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the GDPR. All employees and volunteers must be made aware of the Trust policy and procedures and must provide written acknowledge of their understanding of their individual responsibilities in relation to the GDPR.

1.4 All data held by Trust and its schools are the responsibility of the Trust. Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

3.0 Legal Framework

3.1 GDPR defines "personal data" as any information relating to an identified or identifiable natural person; 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 morefactors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

3.2 The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personaldata, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

3.3 The Information Commissioners Office (ICO) can investigate complaints, audit the Trust's use or other Processing of Personal Data and can take action against the Trust(and individually in some cases) for breach of these laws. Action may include makingthe Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent the Trust from carrying on its educational and associated functions. Organisations who breach one or more laws on Personal Data also often receive negative publicity for the breaches which affects the reputation of the Trust and its activities as a result.

3.4 Any breach of or failure to comply with this policy, particularly any deliberate release of Personal Data to an unauthorised third party, may result in disciplinary orother appropriate action.

4.0 Applicable data

4.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g., an Internet Protocol (IP) address. The GDPR applies to both automated personal data and to manual filing systems, where personal data are accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key-coded.

4.2 Sensitive personal data are referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data, and data concerning health matters.

5.0 Principles

5.1 In accordance with the requirements outlined in the GDPR, personal data will be:

- processed lawfully, fairly, and in a transparent manner in relation to individuals
- 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 not be considered to be incompatible with the initial purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, when 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
- kept in a form that 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, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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

5.2 The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

6.0 Accountability

6.1 The Trust will implement appropriate technical and organisational measures to demonstrate that data are processed in line with the principles set out in the GDPR.

6.2 The Trust will provide comprehensive, clear, and transparent privacy policies.

6.3 Additional internal records of the Trust's processing activities will be maintained and kept up to date.

6.4 Records of activities relating to higher-risk processing will be maintained, such as the processing of activities that:

- are not occasional
- could result in a risk to the rights and freedoms of individuals
- involve the processing of special categories of data or criminal conviction and offence data

6.5 Internal records of processing activities will include the following:

- name and details or the organisation
- purpose(s) of the processing

- description of the categories of individuals and personal data
- retention schedules
- categories of recipients of personal data
- description of technical and organisational security measures
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

6.6 The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:
- data minimisation
- pseudonymisation
- transparency
- allowing individuals to monitor processing
- continuously creating and improving security features
- Data protection impact assessments will be used, when appropriate.

7.0 Data protection officer (DPO)

7.1 A DPO will be appointed in order to:
- inform and advise SMCCAT and its employees about their obligations to comply with the GDPR and other data protection laws
- monitor SMCCAT's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members

7.2 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to multi academy trusts.

7.3 The DPO will report to the highest level of operational management at the Trust. The DPO will operate independently and will not be dismissed or penalised for performing his or her task. Sufficient resources will be provided to the DPO to enable that person to meet the requisite GDPR obligations.

8.0 Lawful processing

8.1 The legal basis for processing data will be identified and documented prior to data being processed.

8.2 Under the GDPR, data will be lawfully processed under the following conditions:
- the consent of the data subject has been obtained
- processing is necessary for:
    - compliance with a legal obligation
    - the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
    - the performance of a contract with the data subject or to take steps to enter into a contract
    - protecting the vital interests of a data subject or another person
    - the purposes of legitimate interests pursued by the controller or a third party, except when such interests are overridden by the interests, rights, or freedoms of the data subject. (This condition is not available to processing undertaken by SMCCAT in the performance of its tasks)

8.3 Sensitive data will be processed only under the following conditions:

- explicit consent of the data subject has been obtained, unless reliance on consent is prohibited by EU or Member State Law
- processing is carried out by a not-for-profit body with a political, philosophical, religious, or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- processing relates to personal data:
- carrying out obligations under employment, social security or social protection law, or a collective agreement
- protecting the vital interests of a data subject or another individual when the data subject is physically or legally incapable of giving consent
- the establishment, exercise, or defence of legal claims or when courts are acting in their judicial capacity
- reasons of substantial public interest on the basis of Union or Member State law, which is proportionate to the aim pursued and which contains appropriate safeguards
- the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medicinal products or medical devices
- archiving purposes in the public interest, or scientific and historical research purposes, or statistical purposes in accordance with article 89(1)

9.0 Consent

9.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity, or pre-ticked boxes.

9.2 Consent will be accepted only when it is freely given, specific, informed, and an unambiguous indication of the individual's wishes.

9.3 When consent is given, a record will be kept documenting how and when consent was given.

9.4 The Trust ensures that consent mechanisms meet the standards of the GDPR. When the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

9.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

9.6 Consent can be withdrawn by the individual at any time.

9.7 When a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except when the processing is related to preventative or counselling services offered directly to a child.

10.0 The rights of data subjects

10.1 GDPR sets out the following rights applicable to data subjects:

- The right to be informed;

- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights with respect to automated decision-making and profiling.

10.2 Keeping Data Subjects Informed – Privacy Notices

The Trust shall ensure that the following information is provided through the publication and sharing of Privacy Notices. The Trust utilise the DfE's Model Privacy Notices and are published on the Trust and Trust schools' websites.

10.3 Data Subject Access

10.3.1 A person may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. The Trust is normally required to respond to SARs within one month of receipt (this can be extended byup to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

10.3.2 All subject access requests received must be forwarded to the Headteacher of the school it relates to, who will obtain advice from the Trust's data protection officer.

10.3.3 The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

10.4 Rectification of personal data

10.4.1 If a person informs the Trust that personal data held by the Trust is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the caseof complex requests, and in such cases the data subject shall be informed of the needfor the extension).

10.5 Erasure of Personal Data

10.5.1 Data subjects may request that the Trust erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Trust to hold that personal data with respectto the purpose for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Trust holding andprocessing their personal data (and there is no overriding legitimate interestto allow the Trust to continue doing so);;
- The data subject objects to the Trust holding and processing their personaldata (and there is no overriding legitimate interest to allow the Trust to continue doing so);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Trust to comply witha particular legal obligation**.**

10.5.2 Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the person's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

10.5 Restriction of Personal Data Processing

A person may request that the Trust ceases processing the personal data it holds about them. Unless the Trust has reasonable grounds to refuse, all requests shall be complied with and shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

10.6 Data Portability

10.6.1 Where a person has given their consent to the Trust to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the legal right under GDPR to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

10.6.2 Where technically feasible, if requested, personal data shall be sent directly to another data controller.

10.6.3 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

10.7 Objections to Personal Data Processing

10.7.1 Where a person objects to the Trust processing their personal data based on its legitimate interests, the Trust shall cease such processing forthwith, unless it can be demonstrated that the Trust's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

10.7.2 Where a person objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing forthwith.

10.7.3 Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under GDPR, 'demonstrate grounds relating to his or her particular situation'. The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

11.0 Automated decision making and profiling

11.1 Individuals have the right not to be subject to a decision when:

- it is based on automated processing, e.g., profiling
- it produces a legal effect or similarly significant effect on the individual

11.2 The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision

and challenge it.

11.3 When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact
- using mathematical or statistical procedures
- implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and to minimise the risk of errors
- securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

11.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual
- the processing is necessary for reasons of substantial public interest on the basis of Union / Member State Law

12.0 Privacy by design and privacy impact assessments

12.1 The Trust will act in accordance with the GDPR by adopting a privacy-by-design approach and implementing technical and organisational measures that demonstrate how the Trust has considered and integrated data protection into processing activities.
Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

12.2 DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation, which might otherwise occur.

12.3 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

12.4 A DPIA will be used for more than one project, when necessary.

- High-risk processing includes but is not limited to the following:
- systematic and extensive processing activities, such as profiling
- large-scale processing of special categories of data or personal data, which is in relation to criminal convictions or offences

12.5 The Trust will ensure that all DPIAs include the following information:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented in order to address risk

12.6 When a DPIA indicates high-risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

13.0 Data Breaches

13.1 The term 'personal data breach' refers to a breach of security that has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

13.2 The Headteacher will ensure that all staff members are made aware of and understand what constitutes a data breach as part of their CPD training.
13.3 When a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

13.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of them.

13.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

13.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

13.7 A 'high-risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

13.8 Effective and robust breach detection, investigation, and internal reporting procedures are in place, which facilitate decision making in relation to whether the relevant supervisory authority or the public need to be notified. Within a breach notification, the following information will be outlined:

- the nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- the name and contact details of the DPO
- an explanation of the likely consequences of the personal data breach
- a description of the proposed measures to be taken to deal with the personal data breach
- when appropriate, a description of the measures taken to mitigate any possible adverse effects

13.9 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

14.0 Data security

14.1 Confidential paper records will be kept in a locked filing cabinet, drawer, or safe, with restricted access.

14.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

14.3 Digital data are coded, encrypted, or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

14.4 When data are saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer, or safe when not in use.

14.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. The Trust does not permit the use of memory sticks for any of the data that it is accountable for.

14.6 All electronic devices are password-protected to protect the information on the device in case of theft.

14.7 When possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
14.8 Staff and governors are encouraged not not use their personal emails for school purposes. All staff and governors will have a Trust email address that should be used for all school / Trust work.

14.9 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

14.10 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

14.11 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

14.12 When personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from Trust premises accepts full responsibility for the security of the data. Before sharing data, all staff members will ensure that:

- they are allowed to share them
- adequate security is in place to protect them
- who will receive the data has been outlined in a privacy notice

14.13 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.

14.14 The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a timely basis. If an increased risk of vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

14.15 The Trust takes its duties under the GDPR seriously, and any unauthorised disclosure may result in disciplinary action.

14.16 The DPO is responsible that continuity and recovery measures are in place to ensure the security of protected data.

15.0 Publication of information

15.1 SMCCAT publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- policies and procedures
- minutes of meetings
- annual reports
- financial information

15.2 Classes of information specified in the publication scheme are made available quickly and easily on request.
The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.
When uploading information to a Trust website, staff are considerate of any metadata or deletions that could be accessed in documents and images on the site.

16.0 CCTV and Photography

16.1 The Trust understands that recording images of identifiable individuals constitutes the processing of personal information, so it is done in line with data protection principles.

16.2 The Trust notifies all pupils, staff, and visitors of the purpose for collecting CCTV images via notice boards, letters, and email.

16.3 Cameras are placed only where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

16.4 All CCTV footage will be kept for 15 days for security purposes; the school is responsible for keeping the records secure and allowing access.

16.5 The Trust will always indicate its intentions for taking photographs of pupils and will secure permission before publishing them.

16.6 If the Trust wishes to use images / video footage of pupils in a publication, such as a Trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

16.7 Precautions are taken, in line with school policy, when publishing photographs of pupils in print, video, or on a Trust website.

16.8 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

17.0 Data Retention

17.1 Data will not be kept for longer than is necessary.

17.2 Unrequired data will be deleted as soon as practicable.

17.3 Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons but also to enable the provision of references or academic transcripts.

17.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

18.0 DBS Data

18.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

18.2 Data provided by the DBS will never be duplicated.

18.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.