Information Governance Support Services by Stockport Council

IGSS/P/001

St Thomas More RC College

Data Protection Policy

Information Governance Support Services by Stockport Council

IGSS/P/001

Contents

1. Introduction 1
2. Scope 1
3. Responsibilities 1
   3.2. Data Protection Officer responsibilities 2
   3.3. Staff responsibilities 2
4. Data protection principles 3
5. The lawful basis for processing 3
6. Accountability 4
7. Data protection by design and default 4
8. Data Protection Impact Assessments 4
9. Rights of the data subject 5
10. Data protection breaches 5
11. Consent 6
12. CCTV – [remove if school does not use CCTV] 6
13. Photography 7
14. Data sharing 7
15. Data security and storage of records 8
16. Records management and disposal of records 8
17. Training 8
18. Complaints 9
19. Glossary of terms 9

Document Control 11

1. Introduction

St Thomas More RC College takes its responsibilities with regards to the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) seriously. This policy sets out how the school manages those responsibilities.

St Thomas More RC College is committed to data protection by design and regards the lawful and appropriate processing of personal and special category data as an integral part of its purpose.

This policy sets out the accountability and responsibilities of the school, its staff and its students to comply fully with the provisions of UK GDPR and DPA.

St Thomas More RC College holds and processes personal data about individuals such as employees, students and others, defined as 'data subjects'. Such data must only be processed in accordance with UK GDPR and the DPA.

This policy therefore seeks to ensure that we:

1. Protect personal data and the rights and freedoms of the data subject
2. Are clear about how personal data must be processed and the school's expectations for all those who process personal data on its behalf
3. Comply with the data protection laws, guidance and good practice
4. Protect the school's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
5. Protect the school from risks of personal data breaches and other breaches of data protection law.

The school has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with UK GDPR and the DPA.

2. Scope

This policy applies to all personal data the school processes, regardless of the location where that personal data is stored (e.g. on an employee's own device) or the format of the information (paper, electronic, audio etc).

All school staff, and others processing personal data on the school's behalf, must be aware of and comply with this policy. A failure to comply, may result in disciplinary action.

3. Responsibilities

3.1. School responsibilities

The school, as data controller is responsible for establishing policies and procedures in order to comply with data protection legislation.

The Data Protection (Charges and Information) Regulations 2018 requires every data controller in the UK to pay a fee to the Information Commissioner's Office (ICO).

The school's registration number is Z4632345

3.2. Data Protection Officer responsibilities

The DPO is responsible for:

- Advising the school and its staff of its obligations under UK GDPR
- Monitoring compliance with the UK GDPR and other relevant data protection law, the school's policies with respect to this, and monitoring training and audit activities related to UK GDPR compliance
- To provide advice on data protection impact assessments
- To cooperate with and act as the contact point for the ICO
- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3.3. Staff responsibilities

Staff members who process personal data about students, staff, applicants or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- All personal data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with the school's retention schedule
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Governance Team
- Any data protection breaches are swiftly brought to the attention of Senior Managers and in turn the Information Governance team;
- All mandatory data protection training is completed and refreshed annually.

If staff are unsure about who are the authorised third parties to whom they can legitimately disclose personal data, they should seek advice from the Business Manager and Senior Leadership Team.

4. Data protection principles

St Thomas More RC College aims to comply with all the provisions of the DPA and the GDPR when processing personal data. The GDPR requires personal information to be processed according to seven data protection principles;

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- 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.
- Processed in a manner that ensures appropriate security of the personal data.

The seventh principle requires schools to be accountable and demonstrate how they comply with the principles.

5. The lawful basis for processing

Personal data will only be collected, used and shared where the school has a lawful basis to do so under data protection legislation. The lawful bases for processing are:

1. **Consent:** the individual has given clear consent for the school to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract the school has with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for the school's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

For special categories (see glossary) of personal data, we will also meet one of the special category conditions for processing, which are set out in the UK GDPR and Data Protection Act 2018.

6. Accountability

The school must implement and evidence appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. To demonstrate this, the school has implemented the following:

- Appointed a suitably qualified DPO.
- Implemented Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects (further information may be found below).
- Integrated data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches.
- Trained staff on compliance with Data Protection and keeping records accordingly.
- Regular testing of the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

7. Data protection by design and default

Under UK GDPR, the school has an obligation to consider the impact on data privacy during all processing activities. There is an obligation to consider the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. The school will ensure that:

- Appropriate technical and organisational measures are implemented to minimise the potential negative impact processing can have on the data subjects' privacy.
- Senior managers understand their responsibility for ensuring there is a privacy culture within the school and ensure policies and procedures are developed with Data Protection in mind.
- Privacy and data protection issues are always considered at the design phase of any system, service, product or process.
- Only data that is necessary to achieve a specific purpose is processed. This links to the fundamental data protection principles of data minimisation and purpose limitation.

8. Data Protection Impact Assessments

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest

stage and a Data Protection Impact Assessment (DPIA) will be conducted where applicable. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection requirements are not an after-thought.

A DPIA will be completed (and findings discussed with the information governance team/DPO) in the following circumstances:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling;
- Large scale processing of sensitive (special category) data; and
- Large scale, systematic monitoring of a publicly accessible area.

9. Rights of the data subject

UK GDPR was designed to strengthen the privacy rights of individuals. It offers more control to the data subject over what happens to their personal data. This has been expressed in UK GDPR under the following eight rights:

- The Right to be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- The Right to Automated Decision Making

For more information about your data protection rights and how to exercise them, please see our Data Subject Rights Guidance: is accessible on our website under policy documents.

10. Data protection breaches

St Thomas More RC College is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. Potential incidents include:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use

- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any suspected data protection incident will be brought to the attention of the school's Information Governance Team and DPO, who will investigate and decide if the incident constitutes a data protection breach.

If a reportable data protection breach occurs, the school is required to notify the ICO as soon as possible, and no later than 72 hours after becoming aware of it. Any member of the school who encounters something they believe may be a data protection incident must report it immediately.

More information can be found on our website under the policy documents tab.

11. Consent

UK GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement between the school, parents and pupils.

UK GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

St Thomas More RC College will keep clear records to demonstrate where consent has been given.

12. CCTV –

St Thomas More RC College understands that recording images of identifiable individuals is processing personal information and must be done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via the Privacy Notice.

All CCTV footage will be kept for 30 days for security purposes.

For more information regarding how we use CCTV please view our CCTV Policy available on our website.

13. Photography

St Thomas More RC College takes images/video footage of pupils throughout their school life. Photographs/video footage often consist of personal data and must be managed under data protection principles.

The school ensures it gathers parent/guardian consent in order to process images of pupils for school purposes such as, internal displays, school website, prospectus, or recordings of school plays.

Images captured by individuals for their domestic purposes, and videos made by parents for family use, fall outside the scope of UK GDPR.

A consent form for the particular usage of images will be sent to parents when the pupil starts at the school.

14. Data sharing

St Thomas More RC College will usually only share data with third parties when they have a legal or statutory obligation, or have the consent of parents/pupils.

Suppliers and Contractors

The school may share personal data with suppliers and contractors where this is necessary to support the delivery of services to staff and pupils. Before sharing any personal data, the school will:

- Ensure suppliers and contractors can demonstrate compliance with data protection legislation.
- Put appropriate contractual arrangements, data processing agreements, or data sharing agreements in place to ensure personal data is processed lawfully, fairly and securely.
- Only share the minimum personal data necessary for the supplier or contractor to carry out their duties.
- Take reasonable steps to ensure personal data remains secure and is only used for the agreed purpose.

Law enforcement and government bodies

We may also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

15. Data security and storage of records

St Thomas More RC College will aim to 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 servers that contain personal data are kept locked away when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to choose strong passwords and never reveal their passwords to others.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- All users of school systems must comply with the school's acceptable use policy to help protect personal information from unauthorised access, disclosure or loss.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 14)

16. Records management and disposal of records

The school maintains records management and retention arrangements to ensure information is retained only for as long as necessary and disposed of securely when no longer required.

Personal data is only kept for as long as is required under legislation or business need. The school refers to a records retention schedule to determine when records no longer need to be retained.

Once personal data is no longer needed it is confidentially disposed of using secure methods.

17. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of staff members' continuing professional development, on an annual basis.

18. Complaints

St Thomas More RC College takes all data protection complaints seriously and will investigate concerns relating to the collection, use, sharing, retention or security of personal information. Staff receiving a data protection complaint must ensure it is promptly referred to the Information Governance Team and/or Data Protection Officer (DPO). The school will maintain records of complaints and any actions taken, using lessons learned to improve compliance and information handling practices. If complainants remain dissatisfied, they have the right to complain to the Information Commissioner's Office (ICO)

19. Glossary of terms

Term	Description
Data	information which is stored electronically, on a computer, or in certain paper-based filing systems.
Processing	any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Data subjects	all living individuals about whom we hold personal data.
Personal data	data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
Data controller	person/business who determines the purposes for which personal data will be processed, and the manner in which it will be processed.

Data processor	person/business that processes personal data on behalf, and in accordance with the instructions, of a data controller.
Special category data	information about a person's race, ethnic origin, political opinions, religion, trade union membership, genetics, biometrics (where used for ID), health, sexual life, or sexual orientation.
Consent	an agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Data Protection Officer (DPO)	person appointed as such under UK GDPR. A DPO is responsible for advising the school on its obligations under data protection, for monitoring compliance with data protection law, providing advice, cooperating with the ICO and acting as a point of contact with the ICO. The school's data protection officer can be contacted at igschoolsupport@stockport.gov.uk
Personal Data Breach	any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject.
Data Protection by Design and Default	involves implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UK GDPR.

Document Control

Title	Data Protection Policy
Document Owner	Information Governance – Stockport Metropolitan Borough Council
Document Status	For School Approval
Links with other policies, procedures, or guidance	Personal Data Breach Policy Data Subjects Rights guidance Records Management Policy Data Protection Complaints Procedure
Target Audience	School workforce
Distribution	Website, hard copy
File Classification	Public
Current Version	7.0

Revision and Approval

Reviewed by	SMBC IG Team
Issue Date	01/09/2026
Approved by (school)	TBC
Approval date	TBC
Next review date	01/09/2028
Any changes made	New Complaints section inserted (s.18) Data Sharing updated (s.14) Records Retention section updated (s.16) Data Security updated for cyber considerations (s.15)

Change History

Version	Author	Issue Date	Review date	Changes made?
V1	IG Team	15.06.2018	1.09.2019	No Changes
V2	IG Team	01.09.2019	01.09.2020	No Changes
V3	IG Team	23.09.2020	01.09.2021	Annual review
V4	IG Team	10.11.2021	01.09.2022	New legislation – dp charges
V5	IG Team	28.10.2022	01.09.2024	Major review to most chapters
V6	IG Team	16.09.2024	01.09/2026	Ch.2. Scope added