



All Saints Catholic Collegiate


Data Protection Policy

POLICY

This policy has been adopted on behalf of all five academies in the All Saints Catholic Collegiate (ASCC)

St. Augustine's Catholic Academy
St. Gregory's catholic Academy
St. Maria Goretti Catholic Academy
Our Lady's Catholic Academy
St. Thomas More Catholic Academy

Approval and review

Committee to approve policy	ASCC Finance & Resources
Date of Board / Academy Committee Approval	06/07/2023
Chair of Board / Academy committee – Name	Mrs A Middleton-Hill
Signature	
Senior Executive Leader	Mrs M Yates
Signature	
Policy review period	12 months
Date of policy review	July 2024

MISSION STATEMENT

***United in faith, love and learning,
we place Christ at the centre of all that we do,
to inspire all members of our community to reach their God-given
potential.***

Version Control			
Version	Date Approved	Page	Reason for Alterations
1	02/07/2020		New version
2	05/07/2022		Amended to reflect UK no longer in EEC Added cybersecurity Cycle changed to 1 year in line with recommendations P16 Data breaches P18 Cybersecurity benchmarking P19 Biometric data P20 – Training and monitoring
3	June 2023		Annual Policy Review

Statement of Intent

1. Legal framework
2. Applicable data
3. Principles
4. Accountability
5. Data protection officer (DPO)
6. Responsibility
7. Lawful processing
8. Consent
9. Sharing data without consent
10. The right to be informed
11. The right of access
12. The right to rectification
13. The right to erasure
14. The right to restrict processing
15. The right to data portability
16. The right to object
17. Automated decision making and profiling
18. Privacy by design and privacy impact assessments
19. Data breaches
20. Data security
21. Publication of information
22. CCTV and photography
23. Biometric Data
24. Data retention
25. DBS data
26. Training and Monitoring
27. Policy review

Statement of intent

The All Saints Catholic Collegiate is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK GDPR.

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

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and The All Saint Catholic Collegiate believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation the [Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (UK GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'

1.3. This policy will be implemented in conjunction with the following other school policies:

- **Freedom of Information Policy**
- **CCTV Policy**
- **Child Protection and Safeguarding Policy**
- **ICO Records Management Policy**

2. Applicable data

2.1. 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 IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

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

3. Principles

3.1. In accordance with the requirements outlined in the UK 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, 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.
- 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, 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 UK 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.

3.2. The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

4. Accountability

- 4.1. The ASCC will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.
- 4.2. The school will provide comprehensive, clear and transparent privacy policies.
- 4.3. Additional internal records of the school’s processing activities will be maintained and kept up-to-date.

4.4. Internal records of processing activities will include the following:

- Name and details of 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

4.5. The school 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.

4.6. Data protection impact assessments will be used, where appropriate.

5. Responsibility

- 5.1. All staff have an individual responsibility to ensure that they comply fully with Data Protection. It is a criminal offence, to knowingly or recklessly obtain or disclose **personal data**. Staff should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under the school's disciplinary procedure. New staff will be informed of the Privacy Notice at appointment; this is available from the Office Manager. **(See Appendix 2)**. Staff should also refer to the Staff Acceptable Use Policy (Appendix 3)
- 5.2. Directors / Academy Representatives (Referred to collectively in this document as "governors") When handling personal information on school business, governors must comply with this policy and be aware of their responsibilities as individuals under the Data Protection Act. They should be mindful that it can be a criminal offence to process **personal data** in a manner which they know that they are not authorised to do. A breach of this policy by a governor is a potential breach of the (governors') Code of Conduct. There will be a designated AR lead for monitoring the schools are complying with Data Protection procedures and completing data protection impact assessments.

6. Data Protection Officer (DPO)

- 6.1. A DPO will be appointed in order to:
- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.
 - Monitor the school's compliance with the UK 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.
- 6.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
- 6.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
- 6.4. The DPO will report to the highest level of management at the school, which is the Senior Executive Leader.
- 6.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.
- 6.6. Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

7. Lawful Processing

- 7.1. The legal basis for processing data will be identified and documented prior to data being processed.
- 7.2. Under the UK 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.
 - For 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.
 - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

7.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by UK GDPR law.
- Processing 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 manifestly made public by the data subject.
- Processing is necessary for:
 - 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 where the data subject is physically or legally incapable of giving consent.
 - The establishment, exercise or defence of legal claims or where 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 UK 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 healthcare 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).

7.4. Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.

- Consent to process a child's data, the school ensures that the requirements outlined in [7.7](#) and [7.8](#) are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

8. Consent

- 8.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- 8.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 8.3. Where consent is given, a record will be kept documenting how and when consent was given.
- 8.4. The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- 8.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- 8.6. Consent can be withdrawn by the individual at any time.
- 8.7. Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in [7.2](#), the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.
- 8.8. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined in [7.2](#).

9. Sharing Data without Consent

- 9.1. The school may share information without consent in specific circumstances. To determine whether information can be shared with consent, the school will identify one of the other lawful bases for processing:
 - **Contract** – the processing is necessary for a contract held between the school and individual, or because the individual has asked the school to take specific tests before entering into a contract.
 - **Legal obligation** – the processing is necessary for the school to comply with the law (not including contractual obligations).
 - **Vital interests** – the processing is necessary to protect someone's life.

- **Public task** – the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
 - **Legitimate interests** – the processing is necessary for the school's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.
- 9.2. Where the school is able to justify one of the lawful bases outlined in 8.1, an exemption applies, or there is a requirement under another law, information may be shared without consent.
- 9.3. Specifically, the UK GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

10. Data Processors

- 10.1. We contract with various organisations who provide services to the Academy Trust Company, including:

Schools that the pupil's attend after leaving us	We may share pupil information with other people and educational organisations when we have good reason to do so. e.g. <ul style="list-style-type: none"> • Exam results and references
Our local authority	We may share information to meet our statutory requirements e.g. <ul style="list-style-type: none"> • Attendance & Assessments • School census
The Department for Education (DfES)	We may share information to meet our statutory requirements
Management Information System Curriculum software, 3 rd party providers, VLE and other applications CPOMS Staff Safe GDPRis	We may share information to allow the School to carry out a public task in the interest of providing education e.g. <ul style="list-style-type: none"> • Assessing your child to inform teaching and learning • Online course and homework access
Other public agencies	We may share information to safeguard your child's welfare and wellbeing e.g. <ul style="list-style-type: none"> • Police, NHS, Social and health interactions
Payment systems and catering management	We may share information to help the smooth running of the school and effective use of resources
Trips and school trip organisations	We may share information to safeguard your child's welfare and wellbeing

Identity management systems	We may share information to safeguard your child's welfare and wellbeing and to accurately identify your child.
Contact and communication systems	We may share information to monitor pupil use email, the internet (including social media) and mobile electronic devices e.g. iPads. This is to check that they are not misbehaving when using this technology or putting themselves at risk of harm. If you would like more information about this you can read the Pupil Acceptable Use Policy
Information, advice and Guidance	We may share information to allow the School to carry out a public task in the interest of providing education
Paper records	We may share information to allow the School meet our legal obligations, to safeguard our children and to carry out a public task in the interest of providing education e.g. <ul style="list-style-type: none"> • Moderation and assessment of work • Statutory inspections by DFE and Diocese

The Right to be informed

- 10.2. Adults and children have the same right to be informed about how the school uses their data.
- 10.3. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.
- 10.4. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:
- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
 - The purpose of, and the legal basis for, processing the data.
 - The legitimate interests of the controller or third party.
 - Any recipient or categories of recipients of the personal data.
 - Details of transfers to third countries and the safeguards in place.
 - The retention period of criteria used to determine the retention period.
 - The existence of the data subject's rights, including the right to:
 - Withdraw consent at any time.
 - Lodge a complaint with a supervisory authority.
 - The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

- 10.5. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- 10.6. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- 10.7. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 10.8. In relation to data that is not obtained directly from the data subject, this information will be supplied:
 - Within one month of having obtained the data.
 - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
 - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The Right of Access

- 11.1. Individuals, including children, have the right to obtain confirmation that their data is being processed.
- 11.2. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- 11.3. The school will verify the identity of the person making the request before any information is supplied.
- 11.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- 11.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- 11.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 11.7. All fees will be based on the administrative cost of providing the information.
- 11.8. All requests will be responded to without delay and at the latest, within one month of receipt.
- 11.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this

extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

- 11.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- 11.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.
- 11.12. All SARs must be approved by the headteacher prior to the issue to the requester

12. The Right to Rectification

- 12.1. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.
- 12.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- 12.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 12.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 12.5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. The Right to Erasure

- 13.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 13.2. Individuals, including children, have the right to erasure in the following circumstances:
 - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
 - When the individual withdraws their consent
 - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
 - The personal data was unlawfully processed

10

- The personal data is required to be erased in order to comply with a legal obligation
 - The personal data is processed in relation to the offer of information society services to a child
- 13.3. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
- To exercise the right of freedom of expression and information
 - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
 - For public health purposes in the public interest
 - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
 - The exercise or defence of legal claims
- 13.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
- 13.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 13.6. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. The Right to Restrict Processing

- 14.1. Individuals, including children, have the right to block or suppress the school's processing of personal data.
- 14.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- 14.3. The school will restrict the processing of personal data in the following circumstances:
- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
 - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual

- Where processing is unlawful and the individual opposes erasure and requests restriction instead
 - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
- 14.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 14.5. The school will inform individuals when a restriction on processing has been lifted.

15. The Right to Data Portability

- 15.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.
- 15.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
- 15.3. The right to data portability only applies in the following cases:
- To personal data that an individual has provided to a controller
 - Where the processing is based on the individual's consent or for the performance of a contract
 - When processing is carried out by automated means
- 15.4. Personal data will be provided in a structured, commonly used and machine-readable form.
- 15.5. The school will provide the information free of charge.
- 15.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- 15.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 15.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.
- 15.9. The school will respond to any requests for portability within one month.
- 15.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

- 15.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The Right to Object

- 16.1. The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
- 16.2. Individuals, including children, have the right to object to the following:
- Processing based on legitimate interests or the performance of a task in the public interest
 - Direct marketing
 - Processing for purposes of scientific or historical research and statistics.
- 16.3. Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.
 - The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- 16.4. Where personal data is processed for direct marketing purposes:
- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
 - The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- 16.5. Where personal data is processed for research purposes:
- The individual must have grounds relating to their particular situation in order to exercise their right to object.
 - Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.
- 16.6. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

17. Automated Decision Making and Profiling

- 17.1. 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 a similarly significant effect on the individual.
- 17.2. The school 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.
- 17.3. When automatically processing personal data for profiling purposes, the school 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 appropriate mathematical or statistical procedures.
 - Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and 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.
- 17.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:
- The school 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.

18. Privacy by Design and Privacy Impact Assessments

- 18.1. The school will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.
- 18.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.
- 18.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.
- 18.4. 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.

- 18.5. A DPIA will be used for more than one project, where necessary.
- 18.6. 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
 - The use of CCTV.
- 18.7. The school 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
- 18.8. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

19. Data Breaches

- 19.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- 19.2. The head teacher of each school will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 19.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- 19.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- 19.5. 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.
- 19.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
- 19.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- 19.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

- 19.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
- 19.10. 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
 - Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- 19.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.
- 19.12. All breaches will be recorded stored and shared via the GDPRiS software
- 19.13. Breaches will be investigated and suggested actions shared to minimise future data breaches

20. Data Security

- 20.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- 20.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 20.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- 20.4. Where data is 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.
- 20.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- 20.6. All electronic devices are password-protected to protect the information on the device in case of theft. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when left unattended.
- 20.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

- 20.8. Staff and governors will ensure there is sufficient security of data, to incorporate passcode or touch ID protection if using their personal devices for school purposes.
- 20.9. All schools have an access controlled entry system and any strangers attempting to gain access should be reported to SLT and site staff immediately.
- 20.10. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password. All staff laptops must be encrypted.
- 20.11. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 20.12. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 20.13. When sending confidential information staff will always check that the recipient is correct before sending.
- 20.14. Document printing: any document containing personal data must be collected immediately and not left on the printer. Remote printing should where possible incorporate the secure release of prints and not automatic.
- 20.15. Where 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 the school premises accepts full responsibility for the security of the data. Materials should only be taken off site when essential to do so and kept to a minimum. Offsite records must be kept secure and stored separately from portable laptops/devices.
- 20.16. Before sharing data, all staff members will ensure:
- They are allowed to share it.
 - That adequate security is in place to protect it.
 - Who will receive the data has been outlined in a privacy notice.
- 20.17. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- 20.18. The physical security of the school's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- 20.19. The ASCC takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

- 20.20. The ASCC advocates the following best practice guidance to minimise the risk of loss of data:

Do not carry loose paper documents as this increase the risk of dropping or losing them. Secure in an appropriate file or container.

Do not carry paper records in any bag containing valuables, as these are often the primary target for thieves

Ensure paper records are not in transit for any longer than is necessary

Ensure paper records are not away from the office for longer than is necessary and return them as soon as possible

Do not leave bags or cases containing paper records visible in a car; if it is unavoidable to store paper records in a car, lock them in the boot

Do not leave paper records stored in the boot of an unattended vehicle

When travelling on public transport ensure that the contents of paper records are not visible

When travelling on public transport keep bag/case containing paper records close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of loss or theft

Treat paper records as you would your cash. Remember personally identifiable information about individuals is valuable in the wrong hands and if sensitive personal information is compromised the Academy Trust Company could suffer a heavy fine

Ensure confidential paper waste created away from the office environment is securely disposed of using a cross cut shredder or ensure this is safely returned to the Academy Trust Company premises for secure destruction.

- 20.21. The I.T contractors and specialist staff are responsible for continuity and recovery measures are in place to ensure the security of protected data.
- 20.22. Any member of staff found to be breach of the above security will be subject to disciplinary action
- 20.23. The trust will benchmark its systems and procedures against the government Cyber security checklist and report annually to the BOD

21. Publication of Information

- 21.1. The ASCC publishes on its website outlining information that will be made routinely available, including:

- Policies and procedures
 - Annual reports
 - Financial information
- 21.2. Information specified under the Freedom of Information Act will be made available quickly and easily on request.
- 21.3. The ASCC will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 21.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV and Photography

- 22.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 22.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- 22.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 22.4. All CCTV footage will be stored for security purposes in line with each schools system installed; the head is responsible for keeping the records secure and allowing access.
- 22.5. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- 22.6. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
- 22.7. Precautions, as outlined in the Safeguarding Policy, are taken when publishing photographs of pupils, in print, video or on the school website.
- 22.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR. The schools request that parents do not publish images onto social media platforms taken at school events of other children/pupils.

23. Biometric Data

- 23.1 Where pupils' biometric data is used as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners

instead of paying with cash. The school will comply with the requirements of the [Protection of Freedoms Act 2012](#).

23.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

23.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

23.4 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the school will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

23.5 Where staff members or other adults use the school's biometric system(s), the school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

24. Data retention

24.1. Data will not be kept for longer than is necessary. The ASCC in line with ICO recommendations uses the Information and Records Management Society's 'Toolkit for Schools'.

24.2. Unrequired data will be deleted as soon as practicable.

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

24.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. Registered Contractors only are used to facilitate the disposal on behalf of the ASCC.

25. DBS data

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

25.2. Data provided by the DBS will never be duplicated.

25.3. 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.

25.4. DBS data will be managed via the Staff safe software and all users to have dual authentication

26. Training and Monitoring

- 27.1 All staff and governors are provided with data protection training as part of their induction process. This will be completed via the training modules for the GDPRiS portal
- 27.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary
- 27.3 The DPO will report to the BOD annually on data breaches, subject access requests and training

27. Registration

- 25.1. St Thomas More Catholic Academy
St Gregory's Catholic Academy
St Maria Goretti Catholic Academy
St Augustine's Catholic Academy
Our Lady's Catholic Academy

are registered as a Data Controllers on the Data Protection Register held by the Information Commissioner.

28. Policy Review

- 28.1. This policy is reviewed annually.
- 28.2. Changes to the policy may occur at any time and where appropriate we will notify data subjects of the changes.
- 28.3. The next scheduled review date for this policy is July 2024.

DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a 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
Data Controllers	Are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	Are those of our workforce (including Governors and volunteers) whose work involves processing personal data? Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	Is 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 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. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by [Academy Trust Company/School] such as staff and those who volunteer in any capacity including Governors [and/or Trustees/Members/parent helpers]

Acceptable Use Policy

Can be obtained from the Senior Operations Manager