EMMAUS
CATHOLIC ACADEMY TRUST

DIOCESE OF SALFORD

GDPR (Data Protection) Policy and Procedures

July 2024

Humility • Faithfulness • Service

POLICY DOCUMENT	GDPR Policy 2024 - 2025
Legislation/Category: Academy Schools	LEGALLY REQUIRED
Lead Member of Staff:	Executive Administrative Manager
Approved by:	Emmaus Trust Board
Date of approval:	15 July 2024
Date of Renewal:	July 2026

EMMAUS CATHOLIC ACADEMY TRUST

The Diocese of Salford provides Catholic Academy Trusts, schools, and colleges for the following reasons:

1. **To assist in the mission of making Christ known to all people;**
2. **To assist parents and carers, who are the prime educators of their children, in the education and religious formation of their children;**
3. **To be of service to the local Church – the Diocese – the Parish and the Christian home;**
4. **To be of service to society.**

Emmaus Catholic Academy Trust Vision:

To provide great Catholic education across Greater Manchester.

Journey with Emmaus CAT…

Contents

1. Policy Statement

Our core purpose is to create a healthy Catholic organisation serving the pupils in our Catholic schools, communities, families, and parishes across Greater Manchester. We are aligned in our mission to work collegially to ensure that we have great schools, strong in faith, serving society. Schools where every pupil has an equal opportunity to thrive and receive the very best Catholic education and formation. Our guiding principles and this GDPR (Data Protection) Policy and Procedures exist to ensure that each Emmaus CAT school has a clear and compelling vision for all of its pupils, focused on creating an inclusive environment, tailored to the needs and abilities of each and every pupil. At Emmaus CAT we will succeed with our philosophy of aligned autonomy, the belief that talent is key and the sharing of curriculum knowledge and academic rigor.

2. Aim of Emmaus CAT Policies

The aim of this, and all Emmaus CAT policies is to support the seven major themes of Catholic Social Teaching, which include;

- The dignity of work and the rights of the worker;
- Solidarity with all people;
- A preferential option for the poor;
- Stewardship and care for creation;
- The call to community and participation;
- The sacredness of life and the dignity of the human person;
- Human rights and the responsibility to protect them;

as well as ensuring that national legislation and guidance are implemented across all our schools. Our policies should not be viewed in isolation, but along with our guiding principles, as integral to all aspects of school improvement. With our policies we aim to create an effective partnership with parents and carers, the prime educators of their children, to ensure that all children reach their potential whist setting high expectations and aspirations, in a positive and supportive environment. All Emmaus CAT policies will clearly define and communicate the core principles which underpin our Catholic culture, mission and vision.

3. GDPR (Data Protection) Policy Aims

Our Catholic Academy Trust (CAT) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

4. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

5. Definitions

TERM	DEFINITION
Personal Data	Any information relating to an identified, or identifiable individual. This may include the individual's: • Name (including initials) • Identification number • Location Data • Online identifier, such as a username It may also include factors specific to the individuals physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patters), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject	The identified or identifiable individual whose personal data is held or processed
Data Controller	A person or organisation that determines the purposes and the means of processing personnel data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data

6. The data controller

Our CAT processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The CAT is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required

7. Roles and responsibilities

This policy applies to all staff employed by our CAT, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary actions.

7.1 Local Governing Body

The local governing body has overall responsibility for ensuring that our CAT complies with all relevant data protection obligations.

7.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on CAT data protection issues. The DPO is also the first point of contact for individuals whose data the CAT processes, and for the ICO. Our data protection officer is Shane Williams, Global Policing, and can be contacted via 0161 510 2999 or data@globalpolicing.co.uk.

7.3 Headteacher/Chief Executive Officer

The headteacher/Chief Executive Officer acts as the representative of the data controller on a day-to-day basis.

7.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the CAT/School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

8. Data Protection principles

The GDPR is based on data protection principles that our CAT must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- This policy sets out how the CAT aims to comply with these principles.

9. Collecting personal data

9.1 Lawfulness, fairness and transparency We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the CAT can fulfil a contract with the individual, or the individual has asked the CAT to take specific steps before entering into a contract
- The data needs to be processed so that the CAT can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the CAT, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the CAT or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

9.2 Limitation, minimisation and accuracy We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the CAT's record retention schedule. Data retention Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of the CAT

may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be required. Staff records will remain accessible to the Executive Administrative Manager only at the CAT Central Officer.

10. Sharing personal data.

We will not normally share personal data with anyone else, but may do so where:

• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

• We need to liaise with other agencies – we will seek consent as necessary before doing this

• Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will 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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

11. Subject access requests and other rights of individuals

11.1 Subject access requests Individuals have a right to make a 'subject access request' to gain access to personal information that the CAT holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data • The purposes of the data processing
- The categories of personal data concerned • Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual Subject access requests should include:
    - Name of individual
    - Correspondence address
    - Contact number and email address
    - Details of the information requested If staff receive a subject access request they must immediately forward it to the DPO.

11.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or cars. For a parent or carer to make a subject access requires with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access request from parents or carers of pupils at our CAT may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

11.3 Responding to subject access requests.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances) Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 academic days of receipt of a written request.

13. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The CAT/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. Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, parents can credit their account and the pupils can 'pay' for their school dinner by giving lunch staff their name at each transaction. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s). Where staff members or other adults use an school's biometric system(s), we 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 CAT/school will delete any relevant data already captured.

14. CCTV

We use CCTV in various locations around the CAT and school sites to make sure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to Alison Smith, Executive Administrative Manager via admin@emmauscat.com

15. Photographs and videos

As part of our CAT activities, we may take photographs and record images of individuals within our CAT/school. We obtain written consent from parents/carers, for photographs and videos to be taken of pupils, for communication, marketing and promotional materials. Uses may include:

- Within CAT/school, on notice boards and in CAT/school magazines, brochures, newsletters, etc.
- Outside of the CAT, by external agencies such as the CAT's photographer, newspapers, campaigns
- Online on our CAT/school website or social media pages

Consent can be refused or withdrawn at any time by parents, if this is requested in writing. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with the pupil's full names, contact details or any other personal information about the child, to ensure they cannot be identified. See our e-safety and safeguarding policy for more information on our use of photographs and videos.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the CAT/school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our CAT/school and DPO and all information we are required to

share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

17. Data security and storage of records

We will 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 hard drives that contain personal data are kept under lock and key 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
- Where personal information needs to be taken off site, staff must sign it in and out from the CAT/school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access CAT/school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for CAT-owned equipment - (Password encrypted)
- 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 8)

18. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of data will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the CAT/school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal data breaches

The CAT will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will investigate immediately. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a CAT context may include, but are not limited to:

- A non-anonymised dataset being published on the CAT's website which shows the exam results of pupils eligible for the pupil premium.

- Safeguarding information being made available to an unauthorised person.
- The theft of a CAT laptop containing non-encrypted persona data about pupils

20. Training

All staff and governors are provided with data protection training, as part of the revision of the CAT's policy, or as part of the induction process, for new staff. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the CAT's processes make it necessary.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our CAT's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the Local Governing Body (LGB).

22. Links with other policies

This data protection policy is linked to our:

- Freedom of information
- Child Protection and Safeguarding Policy