



EMMAUS

CATHOLIC ACADEMY TRUST

DIOCESE OF  Salford

EMMAUS CATHOLIC ACADEMY TRUST

Data Protection Policy

September 2026

POLICY DOCUMENT	Data Protection Policy
Legislation/Category: Academy Schools	LEGALLY REQUIRED
Lead Member of Staff:	Director of Governance, Risk and Compliance
Approved by:	Trust Board
Date of approval:	September 2026
Date Last Ratified:	
Date of Renewal:	September 2027

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...

DIOCESE OF  **SALFORD**

Contents

1.	Policy Statement	Page 4
2.	Aims of Emmaus CAT Policies	Page 4
3.	GDPR (Data Protection) Policy Aims	Page 4
4.	Policy Objectives	Page 5
5.	Roles and Responsibilities	Page 5
6.	Data Protection Principles	Page 7
7.	Collecting personal data	Page 8
8.	Sharing personal data	Page 10
9.	Subject access requests and other rights of individuals	Page 10
10.	Parental requests to see the educational record	Page 13
11.	Biometric recognition systems	Page 13
12.	CCTV	Page 14
13.	Photographs and videos	Page 14
14.	Artificial Intelligence	Page 15
15.	Data protection by design and default	Page 15
16.	Data security and storage of records	Page 16
17.	Disposal of records	Page 17
18.	Data Breaches	Page 17
19.	Explicit Processor Contract	Page 17
20.	Complaints and the Right to Challenge Data Use	Page 18
21.	Training	Page 18
	Appendix 1: Definitions	Page 19
	Appendix 2: Associated Documents	Page 21

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 Pupil Allergy Policy 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 whilst 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

This policy is intended to ensure that personal information is dealt with appropriately and securely, in accordance with The Data Protection Act (2018) and Data Use and Access Act (2025). It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

This policy sets out Emmaus Catholic Academy Trust's commitment to data protection and the implementation of a data protection by design approach. Emmaus Catholic Academy Trust will refer to documents and guidance from the Information Commissioner's Office and Department for Education in relation to data protection and data processing.

4. Policy Objectives

Centrally and at a local school level, Emmaus Catholic Academy Trust are data controllers and will comply with our obligations under The Data Protection Act (2018). Emmaus CAT is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that data subjects are aware of their rights under the legislation. This policy seeks to set out how this will be achieved.

All staff of Emmaus Catholic Academy Trust must have a general understanding of the law and understand how it may affect their decisions to make an informed judgement about how information is gathered, used and ultimately disposed of. All staff must read, understand and comply with the expectations of this policy to comply with our obligations under the General Data Protection Regulation and the Data Protection Act (2018).

Everyone has rights with regards to the way in which their personal data is handled and we recognise that, in the course of our work, we will collect, store and process personal data about our pupils, workforce, families and others. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

All members of staff are expected to comply with the expectations of this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action being taken.

The types of personal data that we may be required to handle includes information about pupils, parents, our workforce and other key audiences and partners. The personal data that we hold is subject to certain legal safeguards, as specified within the Data Protection Act (2018) and other Data Protection legislation.

This policy sets out the rules on data protection and the legal conditions that must be satisfied when Emmaus CAT processes personal data. This policy, combined with our privacy policies and other documents referred to hereafter, set out the basis on which the organisation will process any personal data collected from data subjects or provided to us by data subjects directly or via other sources.

5. Roles and Responsibilities

Emmaus Catholic Academy Trust processes personal data relating to parents, pupils, staff, governors, visitors and other key audiences and is therefore a data controller. Emmaus Catholic Academy Trust is registered as a data controller with the Information Commissioner's Office and will renew this registration as required.

- The Board of Directors hold overall accountability for ensuring that this policy is complied with across the organisation.
- The Local Governing Body hold responsibility for compliance in their respective school.
- The CSEL / headteacher acts as a representative of the Data Controller on a day-to-day basis

- All staff are responsible for:
 - Collecting, storing and processing any personal data in accordance with this policy
 - Informing Emmaus CAT of any changes to their personal data
 - Contacting the Data Protection Officer in the following circumstances
 - With any questions about the application of this policy, data protection law, retaining personal data or keeping personal data secure.
 - If they have concerns that the policy is not being followed
 - 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 of the United Kingdom.
 - 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

The role of the Data Protection Officer

Our Data Protection Officer is Data Protection Education.

They can be contacted at dpo@dataprotection.education

Emmaus Catholic Academy Trust is accountable as the Data Controller. To promote compliance in this area, Data Protection Education act as the CAT's Data Protection Officer in order to provide independent advice, monitoring, auditing and reporting.

Any questions about the operation of this policy or any concerns that this policy has not been followed should be referred to the DPO in the first instance.

Emmaus Catholic Academy Trust is committed to retaining a Data Protection Officer and shall ensure that the Data Protection Officer is involved in a proper and timely manner in all issues which relate to the protection of personal data. Emmaus CAT shall support the DPO in performing the responsibilities outlined below and it is expected that the DPO shall maintain his/her expert knowledge.

The Data Protection Officer shall not receive any instructions regarding the exercise of their tasks, nor shall they become dismissed or penalised by the Data Controller or the Data Processor for performing their duties.

The Data Protection Officer shall report to a member of the Executive Leadership Team as needed and provide a report to the Board of Directors on at least an annual basis.

Data subjects may contact the Data Protection Officer with regard to all issues related to the processing of their personal data and to exercise their rights under the regulations. The Data Protection Officer shall be bound by confidentiality and must maintain data security by protecting the confidentiality, integrity and availability of all personal data, defined as follows:

Confidentiality: means that only people who have a need to know and are authorised to use personal data can access it.

Integrity: means that personal data is accurate and suitable for the purpose for which it is processed.

Availability: means that only authorised users can access personal data when they need it for authorised purposes.

The Data Protection Officer shall fulfil the following responsibilities:

- Review all data processing activities
- Conduct regular audits and issue recommendations
- Assist with Data Protection Impact Assessments (DPIA) and monitoring performance
- Monitoring and advice relating to Subject Access Requests (SARs) and data breaches
- Assisting our community with the maintenance of records
- Monitoring and advice relating to Freedom of Information and other information requests
- Cooperating with and acting as the contact point for the Information Commissioner's Officer.
- Act as the contact point for data subjects to deal with requests and complaints
- Providing training for staff of Emmaus CAT.

6. Data Protection principles

Emmaus CAT accepts that we will comply with the data protection principles in relation to any processing of personal data. The Data Protection principles provide that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject and their rights
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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
- Processed in a manner that ensures appropriate security of personal data and;
- Must not be transferred to people or organisations situated in other countries without adequate protection.

7. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Emmaus CAT can fulfil a contract with the individual, or the individual has asked Emmaus CAT to take specific steps before entering into a contract
- The data needs to be processed so that Emmaus CAT can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life
- The data needs to be processed so that Emmaus CAT, as a public authority, can perform a task in the public interest, or exercise its official authority
- The data needs to be processed for the legitimate interests of Emmaus 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims

- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. These conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 central/school's record retention schedule.

8. Sharing personal data.

We are not ordinarily allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- There is an issue with a pupil, or a parent or 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 that can provide sufficient guarantees that they comply with UK data protection law
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

Subject access requests (SARs)

By law, individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the central team/school 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- The 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. However, during times of school closure (e.g. school holidays) this will be actioned immediately once it is accessed, which is most likely to be once school reopens.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request 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 below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our primary schools may 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.

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 secondary schools may not be granted without the express permission of the pupil. Again, this is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests.

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via telephone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary. These timeframes continue to apply when the school is closed during holidays.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO, or that they can seek to enforce their subject access right through the courts.

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 9), individuals also have the right to:

- Withdraw their consent to processing at any time
- Receive certain information about the data controller's processing activities

- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a personal 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.

10. 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 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it, however, the fee must not exceed the cost of supply.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. 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 and the UK GDPR.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Emmaus CAT 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 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 a 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 Emmaus CAT will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around our school sites to make sure they remain safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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 use of CCTV and CCTV systems should be directed to the Data Protection Officer in the first instance, who may pass on certain queries about the systems used to the Emmaus CAT Head of IT.

13. Photographs and videos

As part of our central and school activities, we may take photographs and record images of individuals within our central team/schools.

In some circumstances, Emmaus CAT has a lawful basis for sharing photographs and videos. This includes matters of safeguarding, assessment and educational administration.

We will obtain written consent from parents/carers, for photographs and videos to be taken of their child, for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parents/carers and the pupil.

Any photographs or videos taken by parents and carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where we take photographs and videos, uses may include:

- Within the central office/school on noticeboards and in Emmaus magazines, brochures and newsletters
- Outside of the central office/schools by external agencies such as the Emmaus CAT's photographer, newspapers and campaigns

- Online via our central or school websites and/or social media pages

Consent can be refused or withdrawn at any time. 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 any other personal information about the child, to ensure they cannot be identified.

14. Artificial Intelligence

We recognise that Artificial Intelligence (AI) tools are increasingly easy to access which staff, pupils and parents/carers are familiar with. Emmaus CAT recognises that AI has many uses to aid learning but can also pose a risk to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Emmaus CAT will treat this as a data breach.

More information about our approach towards the use of Artificial Intelligence can be found in our Artificial Intelligence Policy.

15. 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
- Completing data protection impact assessments (DPIA) where the central team/school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies – following advice from the DPO.
- 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 central/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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the United Kingdom and the safeguards for those, retention periods and how we are keeping the data secure.

16. 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, 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 central/school office
- Passwords made up of four random, unrelated words, or that are at least 10 characters long containing letters and numbers are used to access central/school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff are encouraged to use a school or Emmaus CAT device when working with CAT data, especially when this data could be defined as personal and/or sensitive. In circumstances where a personal device must be used, data should not be stored or downloaded to the device itself.
- Where staff, pupils or governors store personal information on their personal devices, they are expected to follow the same security procedures as for Emmaus-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.

The Emmaus CAT IT Acceptable Use Policy provides further clarification regarding these matters.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date 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 Emmaus CAT's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Data Breaches

All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach becomes recognised.

Emmaus CAT will implement a Data Breach Procedure to ensure any personal data breaches, including the facts relating to the data breach, its effects and the remedial action taken, are recorded in a data breach log and acted upon accordingly.

Individuals who are affected by a data breach will be notified in the event that it poses a high risk to their rights and freedoms. Individuals will also be informed of their right to escalate complaints to the ICO if they feel organisational handling was inadequate, in line with the Data Use and Access Act 2025.

The log shall be monitored and assessed by the Data Protection Officer. It enables them to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in identifying new data handling processes and training requirements.

In the case of a personal data breach resulting in a likely risk to the rights and freedoms of an individual, and after consultation with the Data Protection Officer, Emmaus CAT will, without undue delay and, where feasible, within 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office. Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

19. Explicit Processor Contract

Emmaus Catholic Academy Trust contract with various organisations who provide services to us including (but not limited to):

- Payroll providers – for the purpose of paying employees.

- Parent payment systems – to enable parents to pay for school meals and educational visits.
- A Management Information System – to track contact information, pupil attendance and assessment.
- Pupil Assessment Systems – to support us with the tracking and monitoring of pupil achievement.
- Communication Systems – to enable us to communicate effectively with parents and pupils.
- HR Systems – for the effective management of all aspects of our workforce
- A Safeguarding System – to capture records in the interests of safeguarding children.
- School meals providers

20. Complaints and the Right to Challenge Data Use

Individuals may complain if they believe their data has been mishandled or their rights infringed. If you believe that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, you can raise this by emailing dpo@dataprotection.education

Upon receiving a complaint, we will acknowledge receipt within five working days of receipt and provide a substantive response within one calendar month.

If, following our complaints process, you remain dissatisfied, individuals may escalate to the Information Commissioner's Office and if you remain dissatisfied, to the Data Rights Tribunal.

21. Training

Emmaus CAT shall ensure that all members of staff receive data protection training, including training on information handling appropriate to their role, in order to ensure data protection competence in their role. This training shall be completed annually.

Appendix 1: Definitions

For the purposes of this policy, the following definitions apply:

TERM	DEFINITION
Emmaus Catholic Academy Trust	The central team and our family of schools.
Personal data	Any information relating to an identified, or identifiable, living individual, whether identified directly or indirectly. 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 individual's 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 patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual, and also includes transmitting or transferring personal data to third parties.

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 personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
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. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.



Appendix 2: Associated Documents

This policy should be read in conjunction with:

- Privacy Notices
- Record of Processing Activities (ROPA)
- Lawful Basis Schedules
- Retention Schedules
- Appropriate Policy Document (APD) for Special Category Criminal Offence Data.

Which are available upon request.

