

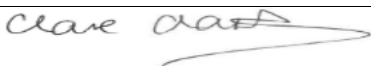


'Christ at the centre, children at the heart'

Our Lady of Walsingham Catholic MAT

Company No: 08444133

Registered Office: Fordham Road, Newmarket, Suffolk, CB8 7AA

Approved by the Trust Board:	May 2026
Signed by Trust CEO:	
Review Date:	May 2027

## Data Protection Policy

### 1. Introduction

This policy applies to all employees, workers and contractors.

The Governing Body/ Directors of the Our Lady of Walsingham Catholic Multi Academy Trust (OLOW CMAT) are committed to being transparent when processing personal data (which may be held on paper, electronically, or otherwise) about any data subject and meeting its data protection obligations. We recognise the need to treat it in an appropriate and lawful manner, in accordance with the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 (DPA 2018) and provisions of the Data (Use & Access) Act 2025 (DUAA 2025). The purpose of this policy is to set out the OLOW CMATs commitment to data protection, individual rights, and obligations in relation to personal data.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action, including dismissal.

The Chief Executive Officer (CEO) is responsible for ensuring compliance with the data protection legislation and this policy through the appointed Data Protection Officer (DPO). Any questions about the operation of this policy or concerns that there has been a breach of this policy should be referred in the first instance to the DPO.

## 2. Responsibilities

The Governing Body/Directors must:

- Manage and process personal data properly.
- protect the individual's rights to privacy.
- provide an individual with access to all personal information held on them.

The Governing Body/Directors have a legal responsibility to comply with the law, including the UK General Data Protection Regulations. The individual with overall responsibility for this policy is the CEO. The Directors have appointed Schools Choice as its data protection officer. Their role is to inform and advise the board on its data protection obligations. They can be contacted at [data.protection@schoolschoice.org](mailto:data.protection@schoolschoice.org). Questions about this policy, or requests for further information, may be directed to them.

The Governing Body/Directors are required to notify the Information Commissioner of the processing of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website.

The Governing Body/Directors' DPO is responsible for drawing up guidance on good data protection practice and promoting compliance with the guidance through advising employees on the creation, maintenance, storage and retention of their records which contain personal information.

Every employee that holds, or has access to, information about identifiable living individuals must comply with data protection legislation in managing that information. All employees are responsible for acting in accordance with the policies, procedures and guidelines and within the provisions of the UK General Data Protection Regulations. **Individuals may be liable for breaches of the Regulations.**

### 3. Definitions

In this policy, unless otherwise stated or unless the context otherwise requires, each term will have the meaning set out below:

**Data protection** means practices and operations relating to the fair and lawful treatment of Personal Data and an understanding of the regulatory requirements relating to data privacy.

**Personal data** is data which relates to a living individual who can be identified:

- from this data; or
- from this data and other information, which is in the possession of the Data controller

Examples of personal data can include, but are not limited to:

- names
- addresses
- telephone numbers
- dates of birth
- National Insurance numbers
- employee numbers
- named email addresses
- account details
- CCTV images
- photographs
- personal opinions
- internet browsing history
- static/dynamic IP addresses

**Special Categories of personal data** (also known as sensitive personal data) includes:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- the processing of genetic data.
- biometric data for uniquely identifying an individual.
- data concerning health or data concerning an individual's sex life.
- sexual orientation.
- medical information.

Additionally, although not sensitive under data protection legislation, financial data and information relating to criminal convictions should also be treated with additional safeguards due to their associated risks.

**Data processing** in relation to information or data, means obtaining, recording or holding the information/data or carrying out any operation or set of operations on the information/data, including:

- organisation, adaptation, or alteration of the information/data.
- retrieval, consultation or use of the information/data.
- disclosure of the information or data by transmission, dissemination or otherwise making available.
- alignment, combination, blocking, erasure or destruction of the information or data; or
- storage of information or data, whether electronically or manually (paper based).

**Data subject** an individual who is the subject of personal data.

**Data controller** means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data is, or is to be, processed.

**Data processor** in relation to personal data means any person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Relevant filing system** means any paper-based records which are structured in a way which is either:

- By reference to the individual by name or code;
- By reference to criteria relating to individuals.

#### **4. Principles relating to processing of personal data**

In line with UK GDPR, anyone processing personal data must comply with the following principles. It is our policy that personal data must be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- 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 it is processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- 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 ('integrity and confidentiality').

The Governing Body/ Directors shall be responsible for, and must be able to demonstrate compliance with, these principles.

The Governing Body/ Directors should tell individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the Governing Body/Directors processes special categories of personal data or criminal records data to perform obligations to exercise rights in employment law, this is done in accordance with the UK General Data Protection Regulation.

## **5. Purposes of Information and Length of Time Retained**

Personal data will be held in accordance with the Governing Body/Directors' Policy on Retention of Personal Information. We will not keep personal data longer than necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required. Individuals will be informed of retention periods within Trusts Privacy Notices.

The Governing Body/Directors will state the purposes for which it holds personal information and will register with the Data Protection Commissioner all the purposes for which it processes personal data.

## **6. Nature of Information**

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

## **7. Disclosure of Information**

Personal data will be used only for the purpose for which it was gathered unless the consent of the data subject concerned has been obtained to a new or varied use.

Routine disclosures will be specified on the Data Protection register and, in the organisation's, own Data Protection publication scheme and consent will be deemed to have been given to routine disclosures so included.

In other cases, the explicit consent of the data subject will be obtained in writing. Confirmation of consent by telephone is acceptable if a written request has been received which implies the consent of the data subject.

Access to personal data will be refused if the data user is uncertain whether the person requesting access, including another employee, is entitled to it. In such a case, the request must be referred to the Data Protection Officer for consideration before the request is rejected. Data Breach

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, the DPO will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, all affected individuals will be informed of the breach and provided with information including the type of data and likely consequences of the breach, plus mitigating steps taken.

Any breach of the policy will be fully investigated, and remedial steps taken to ensure a similar breach cannot happen again.

A record of all data breaches, regardless of their size or effect, will be retained within the Breach Register, as set out in Appendix 1 of this Policy, available from the DPO.

## **8. Individual rights**

As a data subject, individuals have several rights in relation to their personal data.

### **Subject access requests**

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers.
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing.
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under the age of 12, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise.

If the individual requests additional copies, the organisation reserves the right to charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to [admin@olow.org.uk](mailto:admin@olow.org.uk). In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the

organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

## **Other rights**

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to [admin@olow.org.uk](mailto:admin@olow.org.uk)

## **9. Data Security and Impact Assessment**

The trust has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. The organisation will determine and maintain an appropriate level of security (and back-up) for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate individuals. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Some of the processing that the trust carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the trust will carry out a data privacy impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks

## **10. Monitoring Activities**

The organisation will record and monitor usage of all company IT equipment, user activity, voice traffic, email, and internet usage as deemed necessary.

Those responsible for undertaking the monitoring will observe the strictest confidentiality when undertaking these activities. The report will be made directly to the relevant setting Lead Designated safeguarding Lead who will determine any action that may need to be taken.

Monitoring of IT equipment, electronic data, telephone calls, emails, internet access, network access and remote access will be carried out to ensure that usage is in accordance with the Trust's policies, procedures and guidelines.

## **11. Biometric Data**

Biometric technologies are those which automatically measure people's physiological or behavioural characteristics. Examples include automatic fingerprint identification, iris and retina scanning, face recognition and hand geometry, and their use is becoming increasingly popular in educational settings.

Before the first processing of biometric information, the Trust will notify each data subject:

- Of its intention to process biometric information.
- That the data subject may object at any time to the processing of the information.

All processing will be in line with the Trusts Protection of Biometric Information policy.

## **12. Freedom of Information/Environmental Information Regulations**

The Trust as a public authority is subject to The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and all requests for information that is not personal information must be treated as a FOI or EIR. These requests must be fully responded within 20 working days by law. The information will be provided unless the governing body/trust can provide an exemption or exception under the FOI act or EIR respectively.

**In line with FOI Trust is required to have a publication scheme showing what information is held and how you can access this.**

### **Request for Data by Public Authorities**

Requests for personal data may come from public authorities, including but not limited to the following:

- the Police;
- the Department of Work and Pensions;
- the UK Border Agency;
- HM Revenue & Customs;
- Local Authorities;
- DVLA.

Requests received from a public authority will only be processed when submitted in writing, including electronic communication. Such requests for data usually require that the organisation does not inform, or gather consent from, the data subject when responding to the request. When a request is received, this should first be referred to the DPO who will ensure that the request is valid.

Data can only be disclosed without the knowledge and consent of the data subject where it is processed for either the:

- prevention or detection of crime;
- apprehension or prosecution of offenders; or
- assessment or collection of tax or duty.

Additionally, it must be shown that informing or gathering consent from the data subject would likely prejudice the crime or taxation purposes.

Where these conditions are not met, the DPO may decide to not disclose the data. Where the DPO decides the records should not be disclosed or only partially disclosed, they must record in writing their reasons. A public authority may have a Court Order issued for the disclosure of documents. Any objections should be recorded along with the Court Order however the data should be disclosed.

### **13. Individual Responsibilities**

Individuals are responsible for helping the Trust keep their personal data up to date. Individuals should let the Trust know if data provided to the Trust changes, for example if an individual moves house.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, the school relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Trust) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Trust's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Trust's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

All staff are responsible for ensure that information is managed according to this policy.

### **14. Training**

All new and existing employees who handle personal data will receive training on data protection procedures, which includes information about the standards the organisation expects its employees to observe in the use of personal data.

### **15. References**

The Governing Body/Directors will comply with DfE guidance on references as amended from time to time, in particular in relation to safeguarding children and safer recruitment in education.

### **16. Review of Policy**

This policy shall be reviewed as necessary. We reserve the right to change this policy at any time. Where **appropriate**, we will notify data subjects of those changes by mail, email and/or staff notice board. Other related documents:

This policy is supported by the following documents

- Bring Your Own Device Policy
- Protection of Biometric Information Policy
- IT Acceptable Use Policy
- Privacy Notices
- Data Retention Policy
- Code of Conduct/Disciplinary Policy

## **17. Relevant Contacts:**

### **Data Protection Officer**

Please refer any queries, issues or requests received to the Data Protection Officer:

Sarah Ingram

Data Protection Service Lead

Schools Choice

Concertus House, 2 Friars Bridge Rd, Ipswich, IP1 1RR.

01473944579

Sarah.ingram@schoolschoice.org

### **ICO contact details**

If you require more information about the data protection legislation, or are unhappy with the way **OLOW CMAT** has dealt with your data please contact:

The Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

[www.ico.org.uk](http://www.ico.org.uk)

# Appendix A

## Breach Register

Number	Details	Effects and Consequences	Remedial Action Taken	Reported to ICO Y/N	Reported to Data Subject Y/N	Rationale