Data Protection Policy (GDPR Update)

About this policy

The Oxford Diocesan Board of Education (ODBE) aims to ensure that all personal data collected about its staff is stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) and Data (Use and Access) Act 2025.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1. Legislation & Guidance

This policy meets the requirements of the GDPR and the relevant legislation. 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 also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individuals: • 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: • 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	Anything done to personal data, such as collecting, recording, organizing, 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 organization that determines the purposes and the means of processing of personal 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 accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

3. The Data Controller

ODBE processes personal data relating to staff and therefore is a data controller.

ODBE is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

4. Roles & Responsibilities

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

Governing Board

The Oxford Diocesan Board of Education has overall responsibility for ensuring that the organization complies with all relevant data protection obligations.

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 report their activities directly to the ODBE and, where relevant, report to the Board their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data ODBE processes, and for the ICO.

Our DPO's contact details are below:

ODBE Data Protection Officer
Tony Wilson – Director of Education
Oxford Diocesan Board of Education
Church House Oxford
Langford Locks
Kidlington
Oxford OX5 1GF
Email: tony.wilson@oxford.anglican.org

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing ODBE 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
    - If they are unsure whether 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.
    - 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

5. Data Protection Principles

The GDPR is based on data protection principles that ODBE 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 is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how ODBE aims to comply with these principles.

6. Collecting Personal Data

a. 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 ODBE can **fulfil a contract** with the individual, or the individual has asked ODBE to take specific steps before entering a contract
- The data needs to be processed so that ODBE 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 ODBE 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 ODBE or a third party (provided the individual's rights and freedoms are not overridden)
- The individual 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.

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

b. 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 to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized.

7. Sharing Personal Data

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

- There is an issue 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 – 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
- 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, if 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 that affects any of our 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.

8. Subject Access Requests and other Rights of Individuals

a. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that ODBE holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long will the data 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 must be submitted in writing, either by letter or email to the DPO. They 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.

b. 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 member of staff or another individual

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 in accordance with ODBE's Data Protection Complaints Procedure and to the ICO.

c. 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 based on 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.

9. Biometric Recognition Systems

If ODBE uses staff biometric data as part of an automated biometric recognition system, we will

comply with the requirements of the Protection of Freedoms Act 2012.

Staff will be notified before any biometric recognition system is put in place. Staff have the right to choose not to use the biometric system(s).

Staff can object to participation in a biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

10. CCTV

ODBE may use CCTV in various locations around its offices to ensure it remains safe. If we use CCTV 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 the Data Protection Officer (DPO)

11. Photographs & Videos

As part of ODBE's activities, we may take photographs and record images of individuals within our organization.

Uses may include:

- Within ODBE on noticeboards and in magazines, brochures, newsletters, etc.
- Outside of ODBE by external agencies such as, newspapers, campaigns
- Online on our website 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.

If photographs are taken of pupils, we will comply with the relevant school/MAT in respect of their own GDPR policy. 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.

12. Data Protection by Design & 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 ODBE'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 matter; 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 ODBE 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

13. Data Security & 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 encrypted and have secure passwords
- Papers containing confidential personal data must not be left in open plan areas or anywhere else where there is general access
- Where paper-based personal information needs to be taken off site, staff must sign it in and out from the ODBE office
- Passwords that are compliant with ODBE's password policy are used to access computers, laptops and other electronic devices. Staff 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 who store personal information on their personal devices are expected to follow the same security procedures as for ODBE-owned equipment
- 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)

14. 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 the ODBE's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal Data Breaches

ODBE 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 follow the procedure set out in appendix 1.

If appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an organization context may include, but are not limited to:

- Safeguarding information being made available to an unauthorized person
- The theft of an ODBE laptop containing non-encrypted personal data about staff

Training
All staff and Board members will be provided with data protection training as part of their induction process and on an ongoing process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or ODBE's processes make it necessary.

16. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

Policy Reference:	ODBE.SP.011
Description:	This document outlines ODBE's policy on data protection, in line with the GDPR Regulations (25 May 2018) and relevant legislation.
Status:	Statutory Policy
Policy Audience:	Staff, Board members and Public
Contact person:	Data Protection Officer – Tony Wilson
Approved by Oxford Diocesan Board of Education:	*23/05/2018, Updated 04/10/2023, Updated 18/03/26*
Frequency of review:	Every two years (or as legislation changes, whichever is the soonest).
Latest Date for Next Review:	Spring Term 2028
Version	SP.011 version 01

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorized people
- The DPO will alert the Chair of ODBE.
- The DPO will make all reasonable efforts to contain and minimize the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorized reversal of pseudonymization (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

  The DPO will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Board's central systems.

  - Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The

report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will be set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored by the DPO on the Trust's central systems.
- The DPO and Chair of the Board will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 2 – Privacy Notice

The Oxford Diocesan Board of Education is committed to protecting and respecting your privacy. This document sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us.

1. Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. Who are we?

The Board is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

3. How do we process your personal data?

The Board complies with its obligations under the "GDPR" by: -

- keeping personal data up to date;
- by storing and destroying it securely;
- by not collecting or retaining excessive amounts of data;
- by enabling you to exercise your rights in regard to your personal data in accordance with requirements of the GDPR;
- by protecting personal data from loss, misuse, unauthorised access and disclosure; and
- by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes: -

- To administer records of: -
  - ODBE and its Committees;
  - Church School staff and governors
- To promote the interests of the Diocese
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To inform you of updates on financial matters and legal matters; training events through:
  - Mailings (by email &/or hard copy)
  - Newsletters (subscription services to which you must opt in to receive and from which you can unsubscribe at any time)

4. What is the legal basis for processing your personal data?

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and keep you informed about diocesan events;
- Processing is necessary for compliance with a legal obligation;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- Processing is 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

- there is no disclosure to a third party without consent except as set out set out in 5 below

5. Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared between the officers of the Diocese of Oxford.

6. How long do we keep your personal data?

We will keep data in accordance with the guidance set out in the guide "Save or Delete: The Care of Diocesan Records" which is available from the Church of England website at

https://www.churchofengland.org/more/libraries-and-archives/records-management-guides

7. Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- The right to request a copy of your personal data which the Board holds about you;
- The right to request that the Board corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for the Oxford Diocesan Board of Education to retain such data;
- The right to withdraw your consent to the processing at any time
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability);
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable);
- The right to lodge a complaint with the Information Commissioners Office.

8. Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

9. Contact Details

To exercise all relevant rights, queries or complaints please in the first instance contact the Data Protection Officer (Tony Wilson) tony.wilson@oxford.anglican.org. In the event that your complaint regards the actions of the Data Protection Officer this should be addressed to the Chair of ODBE via Penny Bingham penny.bingham@oxford.anglican.org Alternatively, you can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.