Oxford Diocesan Schools Trust
St Mary's Convent
Denchworth Road, Wantage
Oxford, OX12 9AU
01865 208286
odst.governance@oxford.anglican.org
www.odst.org.uk

Statutory Policy:	Policy provided centrally for adoption by schools with minimal amendment to the core text. Changes are allowed to the text where indicated

Data Protection Policy (updated for GDPR)

South Moreton Primary School

Approved by:	**Estates, Health & Safety**
Date:	**June 2023**
Next review date:	**July 2025**

Adopted by school:	**South Moreton**
Date:	**Sept 25**

Description:	This document outlines ODST's policy on data protection, in line with the GDPR Regulations (25 May 2018)
Status:	Statutory Policy
Policy Audience:	Staff, Pupils & Parents/Carers
Trust Contact:	Chief Executive Officer
Other related School policies & procedures:	Freedom of Information Policy, Equality Policy
Governor Committee:	Estates and Health & Safety
Trust Policy Level:	ODST Statutory Policy: Policy provided centrally for adoption by schools with minimal amendment to the core text. Changes are allowed to the text where indicated
In reviewing this policy, the Governing Board has had regard to the Equality Act 2010 and carried out an equality impact assessment. It is satisfied that no group with a protected characteristic will be unfairly disadvantaged by this policy.	

Contents

Policy Statement

The Oxford Diocesan Schools Trust (ODST) and its schools collect and use personal information so that we can operate effectively and fulfil our purpose as set out in the Objects section of our Trust's Articles of Association.

The information we collect, and use includes information about pupils, parents, employees, governors, suppliers, and visitors.

We are committed to protecting the privacy and security of this personal information at all times, as well as supporting individuals in exercising their rights in relation to their own personal information.

This policy, along with accompanying procedures and associated policies, sets out our commitment and approach to safe data protection practice, as well as our support for individuals in exercising their rights. It applies to all personal data, regardless of whether it is in paper or electronic format.

It is reviewed every two years and updated in line with any changes to data protection legislation.

Legislation

This policy meets the requirements of the UK General Data Protection Regulation (GDPR) and the provisions of the UK's Data Protection Act 2018.

Under the GDPR ODST is classified as a Data Controller and is registered with the UK's supervisory authority, the Information Commissioner's Office (ICO). Our registration is renewed annually.

Contact

If you would like to discuss anything in this policy, please contact the relevant school's headteacher or ODST's Data Protection Officer (DPO) as follows:

Headteacher – Cheryl Sanchez, office.2566@south-moreton.oxon.sch.uk
DPO – Julian Hehir, ODST, julian.hehir@oxford.anglican.org Dpo.odst@oxford.anglican.org

Roles and Responsibilities

This policy applies to **all staff** employed by ODST, as well as to external organisations or individuals working on our site.

Staff who do not comply with this policy may face disciplinary action, which could include dismissal. It is a criminal offence to access personal data held by ODST and our schools for purposes other than trust or school business, or to procure the disclosure of personal data to a third party, or to sell such data.

The **Trust Board** has overall responsibility for ensuring that ODST complies with all relevant data protection obligations.

The **Local Governing Bodies** support the Trust Board by monitoring the data protection compliance of their schools.

The **Data Protection Officer** monitors overall compliance with data protection law, providing support and guidance to schools as required, and developing related policies and guidelines where applicable.

Where relevant, they will report to the board their advice and recommendations on trust and school data protection issues.

At school level the **Headteacher** has responsibility for ensuring the implementation of this policy and liaising with the Data Protection Officer about any data protection issues. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

All Staff

All staff are responsible for ensuring that they process any personal data in accordance with this policy (a definition of processing can be found in Appendix 1). Staff must also inform ODST's HR Team of any changes to their personal data, such as a change of address.

Staff must contact the headteacher whenever they have a query about data protection, including, but not limited to the following:

any questions about the operation of this policy: including retaining personal data; keeping personal data secure; sharing personal data with third parties; or whether there is a lawful basis in place for a particular data processing operation

any concerns that the policy is not being followed

a new project under consideration that involves the processing of personal data

received any requests from individuals for access to their personal information the school is processing.

Data Protection Principles

The UK GDPR sets out seven key principles which form the foundation of this data protection legislation:

Lawfulness, fairness and transparency - Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Storage limitation - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes. This is subject to implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights and freedoms of individuals

Integrity and confidentiality (security) - 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

Accountability - the controller shall be responsible for, and able to demonstrate, accountability with the GDPR principles.

This **Data Protection Policy**, along with our privacy notices and additional policies and procedures referenced in section 25, sets out how ODST aims to comply with these principles.

Lawfulness, fairness and transparency

Lawfulness - We will always ensure we have a valid lawful basis for our processing of personal data. There are six lawful bases we can rely on under the UK GDPR:

Contract - the processing is necessary for a contract with an individual, or because they have asked for specific steps to be taken before entering into a contract.

Legal obligation - the processing is necessary to comply with the law (not including contractual obligations).

Vital interest - the processing is necessary to protect someone's life.

Public task - the processing is necessary to perform a task in the public interest or for our official functions as a school, and the task or function has a clear basis in law.

Legitimate interests - the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Consent - the individual has given clear and informed consent for their personal data to be processed for a specific purpose. The individual can change their mind at any time and withdraw their consent. If this happens the processing will be stopped.

Some personal data is considered more sensitive under the GDPR, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sex life or sexual orientation.

For these **special categories** of personal data, we will also identify one of the special category conditions for processing set out in the GDPR:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law).

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1 part 1, paragraphs 1, 8 and 18. These relate to the processing of special category data for employment purposes, safeguarding and equality of opportunity/treatment.

Our Appropriate Policy Document provides more information about this processing.

Criminal Convictions and Offences

The UK GDPR also gives extra protection to **criminal offence data**. As well as ensuring a valid lawful basis for the processing of criminal offence data under the GDPR, we will also identify an additional condition set out in Schedule 1 of the UK DPA 2018.

Under Article 6 of the GDPR, lawful bases we rely on to process this data are:

Performance of our **public task**
Performance of a **contract**.

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1:

Part 2, para 6(2)(a)
Part 1, para 1.

These relate to the processing of criminal offence data for statutory and employment purposes respectively. See Part 3 of *Keeping Children Safe in Education* September 2023 for more information.

Our Appropriate Policy Document provides more information about this processing.

Fairness and transparency

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

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

This will normally be through our **privacy notices**:

Our **Privacy Notice for Pupils** sets out how we process pupil personal data to support teaching and learning, to provide pastoral care and to assess the performance of our services.

Our **Privacy Notice for Parents** sets out how we process the personal data of parents and carers to support the education and learning of pupils and provide pastoral care.

Our **Workforce Privacy Notice** sets out how we process the personal data of staff, agency staff and contractors to fulfil our obligations as an employer.

Our **Privacy Notice for Governors** sets how we process governors' personal data to support them in fulfilling their governance role.

All our Privacy Notices also include information on the rights of the individuals whose data we are processing and who to contact to discuss any aspect further.

Purpose limitation

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data (usually through our privacy notices).

If we want to use personal data for reasons other than those given when we first obtained it, we will identify and document a new lawful basis; although this may not be necessary if our new purpose is compatible with the original purpose. We will inform the individuals concerned before we do so and seek consent where necessary.

Data minimisation

We will only collect the minimum amount of personal data necessary for our purposes. Staff will only process personal data where it is necessary to perform their roles.

Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs us of a change of circumstances, their records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, we will immediately
mark the record as potentially inaccurate, or "challenged".

Storage limitation

When our trust no longer needs the personal data it is processing, it will be deleted or anonymised. This will be done in accordance with our ODST Data Retention Policy.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an outside company to convert paper records to electronic files and shred documents on site.

Where details of individuals are stored for long-term archive, historical or statistical reasons, this will be done within the requirements of the GDPR.

Security

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.

All members of staff are required to sign to confirm that they have read and understood this Data Protection Policy.

All members of staff are required to sign an acceptable user agreement which is renewed annually. The acceptable user agreement is linked to the E-safety Policy and covers such aspects as:

Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information being kept securely when not in use
Papers containing personal information being kept secure and not being left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
Staff ensuring that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended
Staff adhering to school policies and procedures when taking data off site and when working remotely or at home
Strong passwords being used to access school systems, online resources, laptops and other electronic devices. The National Cyber Security Centre recommends that these must be at least 8 characters long containing letters and numbers; or preferably passphrases (e.g., 3 unconnected words).

Encryption software being used to protect all portable devices and removable media
Staff not storing personal information on their personal devices and being expected to follow the same security procedures as set out for any school owned equipment
GDPR compliant cloud storage being used for all online data storage
The use of USB devices not being allowed to store personal data.

Accountability

ODST has put in place appropriate technical and organisational measures to meet the requirements of the accountability principle These include:

The appointment of a data protection officer who reports directly to our highest management level
Taking a 'data protection by design and default' approach to our activities
Maintaining accurate documentation of our processing activities, such as the purposes of processing personal data, data sharing and retention. We also document the lawful bases and conditions we are relying on for our purposes, including how and when consent was obtained, as appropriate
Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
Implementing appropriate security measures in relation to the personal data we process
Carrying out data protection impact assessments for our high-risk processing (see section 6).

We regularly review our accountability measures and update or amend them when required.

Data Protection Impact Assessments

The GDPR requires us to carry out Data Protection Impact Assessments (DPIAs) for any type of processing that is likely to result in a high risk to individuals' interests; for example, when introducing new technologies, or using biometric data for identification purposes.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk can result from either a high probability of some harm, or a lower possibility of serious harm.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

As part of our data protection by design and default approach we will carry out a DPIA for any other major project which requires the processing of personal data.

We follow the ICO's guidelines and our DPIAs:

Describe the nature, scope, context and purposes of the processing
Assess necessity, proportionality and compliance measures
Identify and assess risks to individuals
Identify any additional measures to mitigate those risks.

Sharing Personal Data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors who 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, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with the international transfer rules in the GDPR.

Where we share personal data on an ad hoc or 'one off' basis, we will record the details including our purpose and lawful basis for doing so.

Subject Access Requests

Under the GDPR, anyone whose personal data we are processing, e.g., staff, pupils and parents\carers etc, has a right to make a 'subject access request' to gain access to information our trust holds about them. This includes:

Confirmation that their personal data is being processed
Access to a copy of the data
The purposes of the data processing
The categories of personal data concerned
Who the data has been, or will be, shared with
How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
The source of the data, if not the individual
Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be made by contacting any member of staff, but it is helpful if they are made to the relevant school office or the DPO.

They can be made in person, verbally, in writing, and by email. The following information will be required:

Name of individual
Relationship of the requester to the individual, if appropriate
Correspondence address
Contact number and email address
Details about the information requested

Completion of a subject access request form can be useful, but this cannot be insisted upon.

If a member of staff receives a subject access request, they must immediately forward it to their school office.

Children and Subject Access Requests

A child's personal data always belongs to them rather than 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.

The UK's Information Commissioner's Office generally regards children aged 12 and above to be mature enough to understand their rights and the implications of a subject access request. However, we will always consider this on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

May ask the individual to provide 2 forms of identification, if necessary
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 reveal the following information in response to Subject Access Requests:

Information that might cause serious harm to the physical or mental health of the subject or another individual
Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
Information contained in adoption and parental order records
Certain information given to a court in proceedings concerning the child
Any references that have been provided or received in confidence.

If the request is considered unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be considered to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it (see section 6), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom
- 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)

If staff receive such a request, they must immediately forward it to the school office.

Parental Requests to access their Child's Educational Record

Parents of pupils in academies and trusts do not have the same right as parents in maintained schools to access their child's educational record. This is because The Education (Pupil Information) (England) 2005 Regulations do not apply to academies and trusts.

Any requests from parents for their child's information must be considered as a subject access request under the GDPR.

This is without prejudice to the obligation on the Trust under the Education (Independent School Standards) Regulations 2014 to provide an annual report to every parent (unless they agree otherwise in writing). This report must include each registered pupil's progress and attainment in the main subject areas taught.

CCTV

On some of our school sites CCTV is used to enhance site security. Cameras are positioned in various locations. They are clearly visible and accompanied by prominent signs explaining CCTV is in use. Further information on our use of CCTV is set out in our CCTV Policy and any queries should be directed to the relevant school office.

Biometric Recognition Systems

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This can include a person's fingerprints, facial shape, retina and iris patterns and hand measurements. All biometric data is considered special category data under the GDPR.

Where we use biometric data, we will ensure that it is treated with appropriate care and that we comply with the GDPR principles.

Where biometric data is used as part of an automated biometric recognition system, e.g., cashless catering or photo ID card systems, we will comply with the additional requirements of the Protection of Freedoms Act 2012 (sections 26 - 28). The school will:
- Ensure that each parent* is notified of the school's intention to use their child's biometric data as part of an automated biometric recognition system
- Ensure the written consent of at least one parent is obtained for all pupils under the age of 18 before the data is taken from the pupil and used

Not process the biometric data of a pupil (under the age of 18) where:
- the pupil objects or refuses to participate in the processing of their biometric data (their objection or refusal can be verbal; it does not have to be in writing)
- no parent has consented in writing to the processing (this must be a written consent)
- a parent has objected in writing even if another parent has given their consent.

Parents and pupils can change their minds and withdraw consent at any time. We will make sure that any biometric data already captured is deleted.

We will provide alternative means of accessing services for those pupils who are not using an automated biometric system, e.g., pupils would be able to pay for school meals in cash.

When notifying parents about the intention to take and use their child's biometric information as part of an automated biometric system, we will include:

Details about the type of biometric data to be taken

- How it will be used
- The parents' and pupil's right to refuse or withdraw their consent at any time
- Our duty to provide reasonable alternative arrangements for those pupils who will not be using the automated biometric system.

**'parents' includes not only the biological mother or father (or the adoptive parents) but any individual with parental responsibility for the child, as set out in Part 1 of the Children Act 1989.*

Where staff members or other adults use the 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 or withdraw their consent. Consent can be withdrawn at any time and any biometric data already held will be deleted.

Photos and Videos

As part of our educational activities, we may take photographs and record images of individuals. We will always clearly explain to pupils and/or parents (as appropriate) how the photograph or video will be used.

We will obtain consent for photographs and videos to be taken of pupils for marketing and promotional materials.

Uses may include:

- In school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media page.

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 individual, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

Personal Data Breaches

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

When a personal data breach has occurred, we will assess the likelihood and severity of the resulting risk to the rights and freedoms of the individuals involved. If it's likely that there will be a risk, then we are required by law to notify the ICO.

Data Breach Register

We record all breaches of personal data, regardless of whether they are reported to the ICO. Our data breach register includes the details of the breach, its effects and any remedial action taken. Remedial action may include a review of relevant systems or policies and procedures; additional training for staff; or other corrective steps, as appropriate.

Data Breach Response Plan

Each breach will be considered on a case-by-case basis and our Data Breach Response Plan sets out in more detail the procedures we will follow.

If any member of staff believes a breach of personal data has occurred, or might have occurred, they are required to let the headteacher know immediately.

Training

Our staff are provided with data protection training as part of their induction process, and this is refreshed at least annually. We take a blended approach, so training may be formal CPD - face to face or online delivery; through INSET days, staff meeting updates and discussion, 1:1 reviews, newsletters etc.

Uptake of training is monitored, and procedures are in place to ensure that all staff complete the required training.

Concerns and Complaints

We will always endeavour to resolve any concerns an individual may have about our processing of their personal data informally. However, if this is not possible, the individual will be advised to use our school's complaints procedure. If, after this, the individual remains concerned, they will be advised how they can raise those concerns with the ICO.

Monitoring Arrangements

The Trust Board is responsible for monitoring and reviewing this policy. It will be reviewed every two years.

Links with Other Policies and Procedures

This Data Protection Policy is linked to:

Privacy Notice for Pupils
Privacy Notice for Parents
Workforce Privacy Notice
Privacy Notice for Governors
Use of Email Policy/Acceptable User Agreements
Data Retention Policy
Guidance for Staff on Subject Access Requests
Data Breach Response Plan
Appropriate Policy Document
E-Safety Policy
CCTV Policy
Child Protection Policy/Safeguarding Policy
Freedom of Information Publication Scheme

Appendix One - Definitions

Term	Definition
Personal data	Data from which a person can be identified (i.e., distinguished from other individuals); such as: Name (including initials) Identification number Location data email address, telephone number, car registration number Online identifier, such as a username, IP addresses, cookie identifiers photographs, video recordings This includes data that, when combined with other readily available information, leads to a person being identified.
Special category personal data	Personal data which is more sensitive and is therefore afforded more protection under the GDPR. Data such as: Racial or ethnic origin Political opinions Religious beliefs, or philosophical beliefs Where a person is a member of a trade union genetic data biometric data (when used for identification purposes) Physical and mental health Sexual orientation and sex life Data relating to criminal convictions is afforded similar special protection.
Processing	Any operation carried out on personal data, such as collecting, recording, storing, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The living individual whose personal data is held or processed.
Data controller	A person, or organisation, that determines the purpose for which, and the way, personal data is processed.

Data processor	A person, or other body, other than an employee of the data controller, who processes the data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches can be the result of accidental or deliberate causes.