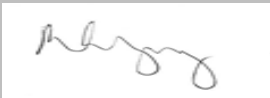





## Data Protection Policy

**Author / staff lead: Mrs Louise Barnard**

**Abstract: This policy is based on the model policy from Turn IT On and reflects the schools approach to data management including adherence to UK GDPR.**

Approved by:	Mrs M Young Chair of Governors	
Approved by:	Mrs J Watson Headteacher	
Last reviewed on:	20/02/2023	
Next review due by:	19/02/2025	
Policy number:	LRS0019	

## Aims

Lent Rise School aims to ensure that all data collected about staff, students, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR). This policy applies to all data, regardless of whether it is in paper or electronic format.

## Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (UK GDPR), and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

This policy also complies with other Academy Funding Agreements and Articles of Association.

## Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none"><li>• Contact details</li><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious beliefs, or beliefs of a similar nature</li><li>• Where a person is a member of a trade union</li><li>• Physical and mental health</li><li>• Sexual orientation</li><li>• Whether a person has committed, or is alleged to have committed, an offence</li><li>• Criminal convictions</li></ul>
Processing	Obtaining, recording, storing, altering or destruction data
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, other than an employee of the data controller, who processes the data on behalf of the data controller

## **The Data Controller**

Lent Rise School processes personal information relating to students, staff, parents, students' emergency contacts and visitors, and, therefore, is a data controller.

Lent Rise School is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

## **Data Protection Principles**

The UK GDPR is based on the following data protection principles, or rules for good data handling:

- Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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.
- 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; 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.
- 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 subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

## **Roles and responsibilities**

The Governing Body has overall responsibility for ensuring that Lent Rise School complies with its obligations under the UK GDPR.

Day-to-day responsibilities rest with the Headteacher. 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.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the UK GDPR may expose the Trust to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines.

Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the UK GDPR could damage our reputation and have serious consequences for the Trust and for our stakeholders.

Data breach reporting is mandatory under the UK GDPR and all staff are aware of their obligation to report data breaches without delay.

## **The Governing Body**

Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Governors should be trained on the Trust's data protection processes as part of their induction and annually and should be informed about their responsibilities to keep Personal Data secure.

This includes:

- Ensure that Personal Data which comes into their possession as a result of their Governor duties is kept secure from third parties, including family members and friends;
- Using a Trust email account for any Trust-related communications;
- Ensuring that any Trust-related communications or information stored or saved on an electronic device or computer is password protected and encrypted;
- Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties.
- Governors will be asked to read and sign an Acceptable Use Agreement.

## **Data breaches**

Data breach reporting is mandatory under the UKGDPR and all staff and governors are aware of their obligation to report data breaches without delay. All data breaches should be reported to Jill Watson or Louise Barnard in the first instance.

## **Privacy/Fair Processing Notice**

### **Students and parents**

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about students from other organisations including, but not limited to, other schools, Local Authorities, the Department for Education and the National Health Service.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on student characteristics, such as ethnic group or Special Educational Needs and Disabilities
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about students with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to the section of this policy on Subject Access Request.

We are required, by law, to pass certain information about students to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

### **Staff**

We process data relating to those we employ to work at, or otherwise engage to work at, our School. The purpose of processing this data is to assist in the running of the school, including to:

- enable individuals to be paid
- facilitate safer recruitment practice
- support the effective performance management of staff
- improve the management of workforce data across the education sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable monitoring of people with, and without, Protected Characteristics under the Equality Act

- support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- contact details, next of kin
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics/protected characteristics
- medical information
- outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. This may include advisers such as our Occupational Health and our Human Resources advisers.

We are required, by law, to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Headteacher.

### **Authorised disclosures**

The Trust will only disclose data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of Personal Data. The Trust will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities
- the Department for Education
- the Department of Health
- NHS Test and Trace
- Public Health England
- the Education & Skills Funding Agency
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme which is administered by Buckinghamshire Council
- Bucks HR Services
- HMRC
- the Police or other law enforcement agencies

- Our legal advisors and other consultants
- Insurance providers / the Risk Protection Arrangement
- occupational health advisors
- exam boards;
- the Joint Council for Qualifications;
- NHS health professionals including educational psychologists and school nurses;
- Education Welfare Officers;
- Courts, if ordered to do so;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;
- confidential waste collection companies;
- Others as listed on the school's Information Asset Register

## **Biometric Data**

Note that in the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system we will comply with the requirements of the Protections of Freedom Act.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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 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. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## **Subject Access Requests**

Under the UK GDPR, Staff, Students and Parents\Carers have a right to request access to information the school holds about them. This is known as a Subject Access Request.

Subject Access Requests must be submitted in writing, either by letter or email. Requests should include:

- The subjects name
- A correspondence address
- A contact number and email address
- Details about the information requested

The Trust 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
- Subject Access Requests for all or part of the student's educational record will be provided within 15 school days.

If a Subject Access Request does not relate to the educational record, we will respond within 1 calendar month.

We reserve the right to charge for requests which are deemed to be excessive.

We may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

### **Parental Requests to see the Educational Record**

As an academy parents of students at Lent Rise school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

For a parent to make a subject access request, the child must either be unable to understand their rights (such as children under the age of 12 and the implications of a Subject Access Request or have given their consent.)

If parents ask for copies of information, they will be required to pay the cost of making the copies.

### **Data Accuracy**



Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances his/her computer records will be updated as soon as is practicable.

Data Checking Sheets for students and staff will be provided to data subjects every 12 months so they can check its accuracy and make any amendments as follows:

Where a data subject challenges the accuracy of his/her data the school will immediately mark the record as potentially inaccurate, or “challenged”. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body under the formal Complaints Procedure.

### **CCTV (see CCTV policy for more information)**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO’s code of practice for the use of CCTV.

We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

### **Storage of records**

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office. Staff must adhere to school policies and procedures when taking data off site.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, online resources, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Encryption, anonymisation and pseudonymisation will be used to protect the data.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.
- Governors are required to use school email addresses and use cloud storage for sharing information and data.
- UK GDPR compliant cloud storage will be used for all online data storage.

### **Disposal of Records**

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely according to specific information type directions as laid out in the Information Asset Register.

## **Training**

Our staff and governors are provided with data protection training as part of their induction process and this is refreshed annually.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary to keep staff up to date.

## **Monitoring Arrangements**

The Headteacher is responsible for monitoring and reviewing this policy.

The School Data Protection Leads Jill Watson and Louise Barnard check that the school complies with this policy by, among other things, reviewing school records at least annually or more frequently if required.

This document will be reviewed **every 2 years**.

At every review, the policy will be approved by the Governing Body.

## **Contact**

### **Data Protection Officer**

The Data Protection Officer (the "DPO") is responsible for ensuring the Trust is compliant with the GDPR and with this policy. This post is held by Darrell Smith, TurnITOn DPO, [dpo@turniton.co.uk](mailto:dpo@turniton.co.uk). In addition, a DPO lead will be appointed by the Trust. Any questions or concerns about the operation of this policy should be referred in the first instance to the GDPR leads at the school, Jill Watson and Louise Barnard.

## **Policy update information**

This policy is reviewed annually and updated in line with data protection legislation.