1. Why GDPR Matters

The Trust is committed to keeping all personal information safe and secure, in line with UK law.
Everyone who works for the Trust must follow these rules when handling personal data.
Breaches of these rules can lead to disciplinary action and, in some cases, criminal charges.

Ref Main Policy Introduction

2. What is Personal Data?

Personal data means any information that can identify a person, such as:
- Name, address, phone number, email
- Student or staff records
- Health or disability information
- Photos, CCTV images, or video/audio recordings

Special category data includes sensitive information like race, religion, health, or biometric data.

Ref Key terms used in the

3. Your Responsibilities

Only collect and use personal data if you have a clear reason and permission.
Only use data for the purpose it was collected.
Keep data accurate and up to date.
Store data securely (e.g., locked cabinets, password-protected files).
Do not share data with anyone who isn't authorised.
Report any data breaches or concerns to the Data Protection Officer (DPO) immediately.

Ref The Rules for Processing Personal Data, Security of Data, Disclosure of Data policy

4. Using Technology and AI

If you use AI or automated systems that process personal data, the same rules apply.
Staff and individuals must be informed if their data is processed by AI, especially if decisions are made automatically.
Any new system or process involving personal data may require a Data Protection Impact Assessment (DPIA).

Ref Processing personal data with AI

5. Data Subjects' Rights

Everyone whose data is held by the Trust has rights, including:
- To know what data is held and why
- To access their data
- To correct inaccurate data
- To have data erased (in some cases)
- To object to how their data is used
- To complain if they think their data rights have been breached

Ref Data Subjects' Rights

6. Data Security

Keep all personal data secure and only accessible to those who need it.
Do not leave personal data unattended or visible to unauthorised people.
Follow Trust procedures for storing, deleting, and disposing of data.

Ref Security of Data, Retention and Disposal of Data

7. If Something Goes Wrong

If you think data has been lost, stolen, or shared by mistake, report it to the DPO (James Beighton) straight away.
The Trust must report serious data breaches to the Information Commissioner's Office within 72 hours.

Ref Personal Data Breaches

8. Where to Get Help

For questions or concerns, contact the Data Protection Officer (DPO) at sars@leadacademytrust.co.uk.

Do	Don't
Only collect and use personal data if you have a clear reason and permission. Use data only for the purpose it was collected. Keep data accurate and up to date. Store data securely (locked cabinets, password-protected files). Report any data breaches or concerns to the Data Protection Officer (DPO) immediately. Inform individuals if their data is processed by AI or automated systems. Follow Trust procedures for storing, deleting, and disposing of data. Respect data subjects' rights (access, correction, erasure, objection). Use only Trust-approved systems and software for storing or processing data. Seek advice from the DPO if unsure about data handling.	Don't collect or keep unnecessary personal data about students or staff. Don't use personal data for unrelated activities or share it informally. Don't ignore requests to correct inaccurate information. Don't leave personal data unattended, visible, or accessible to others. Don't try to handle data breaches yourself or delay reporting. Don't use new systems or apps that process personal data without approval. Don't dispose of documents containing personal data in regular bins. Don't ignore or dismiss requests from individuals about their data rights. Don't use personal email or unapproved apps for school data. Don't guess or assume what is allowed—always check if unsure.