



LISAL

Data Protection Policy

Version date: Spring 2025

Document review period: Spring 2027



CONTENTS

Contents

1. Aims 1
 2. Legislation and guidance 2
 3. Definitions 2
 4. The data controller 3
 5. Roles and responsibilities 5
 6. Data protection principles 6
 7. Collecting personal data 6
 8. Sharing personal data 6
 9. Subject access requests and other rights of individuals 6
 10. Parental requests to see the educational record 6
 11. Biometric recognition systems 6
 12. CCTV 7
 13. Photographs and videos 7
 14. Data protection by design and default 7
 15. Data security and storage of records 7
 16. Disposal of records 7
 17. Personal data breaches 7
 18. Training 7
 19. Monitoring arrangements 8
 20. Links with other policies 8
- Appendix 1: Personal data breach procedure 9



Appendix 2: Privacy Notice 13

Appendix 3: Useful Links 17

Appendix 4: Declaration Form 18



1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors, and other individuals is collected, stored, and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the Data Protection Act 2018, based on guidance published by the Information Commissioner's Office (ICO).

3. Definitions

Term	Definition
Personal data	Information relating to an identified or identifiable individual.
Special categories of personal data	More sensitive information requiring additional protection.
Processing	Any action taken with personal data.
Data subject	The individual whose personal data is held or processed.
Data controller	Person or organization determining the



	purposes and means of processing personal data.
Data processor	Entity processing personal data on behalf of the data controller.
Data protection officer (DPO)	Assists with monitoring compliance and advises on data protection obligations.

4. The data controller

Our school processes personal data and is registered with the ICO. We do not require a DPO as we are not a public authority.

5. Roles and Responsibilities

This policy applies to all staff and external parties working on our behalf. Non-compliance may result in disciplinary action.

5.1 Board of Trustees

Responsible for ensuring compliance with data protection obligations.

5.2 School Management Team

Acts as the representative of the data controller on a daily basis.



5.3 All Staff

Responsible for collecting, storing, and processing personal data in accordance with this policy.

6. Data Protection Principles

Personal data must be processed lawfully, fairly, and transparently. This policy outlines how the school complies with these principles.

7. Collecting Personal Data

We will only process personal data with a lawful basis under data protection law. We will collect data for specific, legitimate purposes and ensure its accuracy and relevance.

8. Sharing Personal Data

Personal data will only be shared when necessary, with appropriate safeguards in place.

9. Subject Access Requests and Rights of Individuals

Individuals have the right to access their personal data and exercise other data protection rights. Requests must be submitted in writing to the School Manager.

10. Parental Requests to See the Educational Record

Parents may request access to their child's educational record in writing to the School Manager.

11. Biometric Recognition Systems

Our school does not use biometric systems.



12. CCTV

We do not currently use CCTV but will adhere to ICO guidelines if implemented in the future.

13. Photographs and Videos

Consent is obtained for taking photographs and videos, especially for children under 12. Consent can be refused or withdrawn at any time.

14. Data Protection by Design and Default

We integrate data protection into all processing activities, ensuring compliance with data protection principles.

15. Data Security and Storage of Records

Personal data is protected from unauthorised access or disclosure. Secure measures are in place for data storage.

16. Disposal of Records

Personal data no longer needed will be securely disposed of.

17. Personal Data Breaches

In the event of a data breach, we will follow the procedure outlined in Appendix 1 and report to the ICO if necessary.

18. Training

All staff and trustees receive data protection training as part of their induction and ongoing professional development.



19. Monitoring Arrangements

The School Manager is responsible for monitoring and reviewing this policy, which will be reviewed every 2 years.

20. Links with Other Policies

This policy is linked to our Acceptable Use (ICT) Policy, Code of Conduct, Use of Image Policy, and Online Safety Policy.



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 school office

- The office staff will investigate the report, and determine whether a breach has occurred. To decide, the office staff will consider whether personal data has been accidentally or unlawfully:

- o Lost
- o Stolen
- o Destroyed
- o Altered
- o Disclosed or made available where it should not have been
- o Made available to unauthorised people

- The office staff will alert the Senior Management Team and the chair of trustees

- The Management Team and Trustees will make all reasonable efforts to contain and minimise 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 Management Team and Trustees will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The Management Team and Trustees 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 Management Team and Trustees 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:

- o Loss of control over their data
- o Discrimination



- o Identify theft or fraud
- o Financial loss
- o Unauthorised reversal of pseudonymisation (for example, key-coding)
- o Damage to reputation
- o Loss of confidentiality
- o 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 Management Team and/or Trustees must notify the ICO.

- The Management Team and/or Trustees will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored under 'GDPR' in the Clerical shared drive.

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

- o 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

- o The name and contact details of the Management Team and/or Trustees dealing with the breach

- o A description of the likely consequences of the personal data breach

- o 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 Management Team and/or Trustees will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information, submitting the remaining information as soon as possible



- Management Team and/or Trustees will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, they will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of Management Team and/or Trustees dealing with the breach
 - 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
- Management Team and/or Trustees will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- Management Team and/or Trustees 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 under 'Data Protection' in the Admin Store.
- The Management Team and/or Trustees 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 School Office as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the office staff or management team will ask the IT committee to recall it
- In any cases where the recall is unsuccessful, the office staff or management team 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 Management Team and/or Trustees will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Management Team and/or Trustees 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. For example:
 - Non-anonymised staff pay information
 - A school laptop containing non-encrypted sensitive personal data being stolen or hacked



APPENDIX 2: PRIVACY NOTICE

Our contact details

Name: The School Office

Address: Lune Road, Lancaster LA15QU

Website: www.lisal.org

Phone Number: 01524 381876

Date: 26/03/2025

E-mail: enquiries@lisal.school

The type of personal information we collect

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name, contact details for parents, children, emergency contacts, customers and suppliers)
 - Names and contact details
 - ID in the form of passports, certificates or financial documents
 - Medical, educational, health and safety and dietary information (including attendance)
 - Photographic and video imagery

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- To administer children to and from our school and comply with our obligations to Lancaster County Council
- To create financial agreements for school fees
- To conduct recruitment related processes
- To enable us to administer our website and perform marketing functions



We also receive personal information indirectly, from the following sources in the following scenarios:

- Schools previously attended by pupils to provide continuity of care for children joining our school from another setting.
- Previous employers, disclosure and barring service or referees when employing new staff or vetting volunteers
- Other professional organisations for example Social Services, NHS or the Police may share relevant information with us so that we can support your child and/or families needs.

We use the information that you have given us in order to:

- Understand your child's and/or family's medical, educational or safeguarding needs.
- Complete our employment and vetting processes
- Enable us to meet our health and safety requirements

We may share this information with:

- Other schools as part of your child transfer to another school
- Other professional organisations, for example Social Services, Police, NHS, Lancashire County Council or a Safeguarding representative (for example, LADO).

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:

(a) Your consent. You are able to remove your consent at any time. You can do this by contacting: enquiries@lisal.school

(b) We have a contractual obligation to process this information.

(c) We have a legitimate interest in processing this information.

How we store your personal information

Your information is securely stored.

We keep all personal information collected either in a locked filing cabinet or electronically and protected by passwords. All personal information is



retained for a reasonable period or as long as the law requires. At which time we will then dispose of your information by shredding paper copies and erasing data stored electronically.

Any data on devices which are being disposed of will have their data erased using a data disposal and shredding company/device to ensure all personal data is non-recoverable.

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at either enquiries@lisal.school, 01524 381876 or Lancaster Independent School for Alternative Learning, Lune Road, Lancaster, LA1 5QU if you wish to make a request.



How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at Lancaster Independent School for Alternative Learning, Lune Road, Lancaster, LA1 5QU or email gabi@lisal.school for data protection queries.

You can also complain to the Information Commissioner's Office (ICO) if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>



APPENDIX 3: USEFUL LINKS

Useful links:

[General Data Protection Regulation \(GDPR\)](#)

[Data Protection in schools](#)

[The Data Protection Bill](#)



APPENDIX 4: DATA PROTECTION DECLARATION

I _____ (full name) confirm I have read and

understand the LISAL Data Protection Policy. If I have any questions I should speak to the School Manager or consult the policy in the office binder where further information is held.

Signed:

Date:

