



RESPECT. RESILIENCE. INTEGRITY.

Data Protection, Privacy and Information Governance Policy

DATE APPROVED

24 September 2026

NEXT DOCUMENT REVIEW

July 2027

Policy Owner:	Kathryn McAuley, Data Protection Lead
Confirmed by	Life Changing Education Ltd, acting through Krystian Liptrot, Chair of the proprietor board and company
Approval Status:	Approved
Date Approved:	24 September 2026
Date Implemented:	24 September 2026
Next document review	July 2027 (governors advise; proprietor decides)
Applies to:	Pupils, families, staff, applicants, visitors, contractors and others whose personal data is processed by the Academy. Registered site: Unit 4, Howarth Court, Oldham Gateway, Gateway Crescent, Chadderton, Oldham, OL9 9XB.

LCE ACADEMY

Contents

Version Control	4	14 Special Educational Needs Information	14
1 Statement of Intent	4	15 Speech and Language Therapy Information	14
2 Purpose	5	16 Information Sharing	14
3 Scope	5	17 Confidential Conversations	15
4 Legal Framework	6	18 Email and Electronic Communication	16
5 Data Protection Principles	6	19 Academy Devices	16
6 Definitions	7	20 Personal Devices	16
7 Roles and Responsibilities	8	21 Remote Working	17
8 Lawful Bases for Processing	10	22 Information Technology Security	17
9 Special Category Data	10	23 Internet Filtering and Monitoring	18
10 Processing Personal Information	11	24 Contractors and Third-Party Processors	18
11 Pupil Records	11	25 Confidential Waste and Secure Disposal	18
12 Staff Records	12	26 Individual Rights	19
13 Safeguarding Records	13	27 Subject Access Requests	19

28	Access to non-personal information and transparency	20
29	Data Protection Impact Assessments (DPIAs)	20
30	Personal Data Breaches	20
31	Managing Data Breaches	21

32	Record Retention	21
33	Staff Training	22
34	Monitoring Compliance	22
35	Complaints	23
36	Monitoring and Review	23



Version Control

Version	Date	Author	Review Date
3.0	22 September 2026	Kathryn McAuley, Data Protection Lead	July 2027



Statement of Intent

LCE Academy is committed to protecting the privacy, dignity and rights of all individuals whose personal information we hold.

As a specialist independent SEMH school, we process significant amounts of sensitive and confidential information relating to children, families, staff, visitors and external professionals. This information enables us to safeguard children, deliver high-quality education, meet statutory duties and provide appropriate support for every pupil.

The Academy recognises that effective information management is fundamental to safeguarding, educational provision and maintaining the confidence of our pupils, families, commissioners and wider community.

We are committed to ensuring that all personal information is:

- Collected lawfully.
- Processed fairly and transparently.
- Used only for legitimate purposes.
- Kept accurate and secure.
- Shared appropriately.
- Retained only for as long as necessary.
- Disposed of securely.

Every member of staff has a responsibility to protect personal information and to ensure that confidentiality is maintained whilst recognising that information must be shared where this is necessary to safeguard children or comply with legal obligations.

The Academy recognises that data protection legislation supports appropriate information sharing and should never prevent staff from taking action to protect a child from harm.

2

Purpose

The purpose of this policy is to:

- Ensure compliance with UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.
- Protect the rights and freedoms of individuals.
- Promote consistent and secure handling of personal information.
- Support effective safeguarding through lawful information sharing.
- Reduce the risk of data breaches.
- Provide staff with clear expectations regarding information governance.
- Promote public confidence in the Academy's handling of personal information.

3

Scope

This policy applies to all personal information processed by LCE Academy regardless of format.

This includes information held:

- Electronically.
- In paper records.
- Within emails.
- On Academy devices.
- Within approved cloud-based systems.
- On secure mobile devices where authorised.

The policy applies to:

- Pupils.
- Parents and carers.
- Staff.
- Volunteers.
- Governors.
- Proprietor.
- Contractors.
- Agency staff.
- Visitors.
- External professionals.
- Applicants for employment.

The policy also applies to anyone processing information on behalf of the Academy.

For data-protection purposes, Life Changing Education Ltd is the data controller for LCE Academy and is also the sole legal proprietor of the school. Krystian Liptrot is Chair of the proprietor board and company and application signatory. Kathryn McAuley is the Academy's Data Protection Lead and coordinates day-to-day compliance, requests, complaints, incidents and advice. Sam Gray, Headteacher, is accountable for operational implementation. The proprietor records and reviews the Article 37 DPO-needs assessment and appoints an independent DPO if the legal threshold is met; current contact details and roles are published in privacy notices. Privacy information for pupils is provided in an age-appropriate and communication-accessible form.

4

Legal Framework

This policy has been developed in accordance with:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.
- Human Rights Act 1998.
- Education Act 2002.
- Children Act 1989.
- Children Act 2004.
- Keeping Children Safe in Education.
- Working Together to Safeguard Children.
- Independent School Standards.
- Information Commissioner's Office (ICO) guidance.
- Department for Education guidance relating to data protection in schools.

Where there is any conflict between confidentiality and safeguarding responsibilities, the Academy will always act in accordance with safeguarding legislation and statutory guidance.

5

Data Protection Principles

LCE Academy processes personal information in accordance with the seven principles of UK GDPR.

Personal information will be:

Lawful, Fair and Transparent

Individuals will understand why information is collected and how it will be used.

Collected for Specified Purposes

Information will only be collected for legitimate educational, safeguarding, employment or operational purposes.

Adequate, Relevant and Limited

Only information that is necessary for the identified purpose will be collected.

Accurate

Reasonable steps will be taken to ensure information remains accurate and up to date.

Where inaccuracies are identified they will be corrected promptly.

Kept Only as Long as Necessary

Information will only be retained in accordance with statutory requirements and the Academy's retention schedule.

Secure

Appropriate technical and organisational measures will protect information from unauthorised access, loss, damage or disclosure.

Accountable

The Academy will be able to demonstrate compliance with data protection legislation through policies, procedures, training and governance arrangements.

6 Definitions

For the purposes of this policy:

Personal Data

Any information relating to an identified or identifiable living individual.

Examples include:

- Name.
- Date of birth.
- Address.
- Email address.
- Telephone number.
- Photographs.
- Attendance records.
- Assessment information.

Special Category Data

Information requiring enhanced protection, including:

- Health information.
- Mental health.

- SEND information.
- Ethnicity.
- Biometric information where applicable.
- Religious beliefs where collected.
- Information relating to safeguarding concerns.

The Academy processes special category data only where there is a lawful basis and an additional condition for processing.

Processing

Processing includes collecting, recording, storing, using, sharing, updating, deleting or destroying personal information.

Data Subject

The individual whose personal information is being processed.

Personal Data Breach

A security incident leading to the accidental or unlawful:

- Destruction.
- Loss.
- Alteration.
- Unauthorised disclosure.
- Unauthorised access.

7 Roles and Responsibilities

Proprietor body and advisory governance

Krystian Liptrot, as Chair of the proprietor board and company acting on behalf of Life Changing Education Ltd, is accountable for ensuring that the following controls are effective. The governing body provides recorded advice and challenge without displacing that accountability:

- Appropriate data protection arrangements are in place.
- Sufficient resources are available.
- Compliance is monitored.
- Risks are reviewed.
- Appropriate policies are maintained.

Headteacher

The Headteacher has operational responsibility for ensuring compliance across the Academy.

Responsibilities include:

- Implementing this policy.
- Promoting good information governance.
- Ensuring staff understand their responsibilities.
- Reporting serious data breaches.
- Working alongside the Data Protection Lead.
- Ensuring appropriate training is delivered.
- Maintaining secure information systems.

Data Protection Lead

Kathryn McAuley is the Academy's Data Protection Lead and will, with independent specialist advice where necessary:

- Monitor compliance.
- Provide professional advice.
- Support investigations.
- Advise on Data Protection Impact Assessments.
- Monitor data breaches.
- Liaise with the Information Commissioner's Office where appropriate.
- Support policy development.

The Data Protection Lead has direct access to the Headteacher and proprietor. Any formally appointed statutory DPO will operate independently and will not be instructed on the exercise of that role.

All Staff

Every member of staff is responsible for protecting personal information.

Staff must:

- Follow this policy.
- Complete mandatory training.
- Maintain confidentiality.
- Keep passwords secure.
- Challenge inappropriate information sharing.
- Report suspected breaches immediately.
- Use Academy systems appropriately.
- Ensure paper records remain secure.
- Lock devices when unattended.
- Dispose of confidential information securely.

Failure to comply with this policy may result in disciplinary action.

8 Lawful Bases for Processing

LCE Academy processes personal information only where there is an appropriate lawful basis under UK GDPR.

These include legal obligation; public task only where a specific statutory education or safeguarding function supports that basis; vital interests; legitimate interests where a balancing test shows it is appropriate; contract; and consent where consent is genuinely freely given and can be withdrawn. The record of processing activities and privacy notice identify the actual basis for each purpose rather than treating this list as blanket authority.

The Academy does not rely upon consent where another lawful basis is more appropriate, particularly where there is an imbalance of power or where processing is necessary to fulfil statutory educational or safeguarding responsibilities.

9 Special Category Data

Due to the nature of our provision, the Academy routinely processes special category data relating to pupils and staff.

This may include information concerning:

- Physical health.
- Mental health.
- Speech, language and communication needs.
- Special educational needs and disabilities.
- Social care involvement.
- Safeguarding concerns.
- Behaviour support.
- Educational Psychology advice.
- Occupational Therapy reports.
- Attendance and welfare.
- Medical treatment.
- Risk assessments.

Such information is processed only where necessary and in accordance with UK GDPR, the Data Protection Act 2018 and relevant safeguarding legislation.

Enhanced security measures are applied to all records containing special category data.

The Academy maintains a controlled Appropriate Policy Document for each Schedule 1 condition that requires one. It records the condition relied upon, necessity, data-protection principles, retention/erasure arrangements, security, accountability, review and responsible owner. The record of processing activities and retention schedule cross-reference the relevant condition.

10 Processing Personal Information

LCE Academy processes personal information only where it is necessary to fulfil its educational, safeguarding, employment and legal responsibilities.

Information is collected directly from individuals wherever possible and, where appropriate, from partner organisations including:

- Local Authorities.
- Previous schools.
- Family Help services, including services locally described as Early Help.
- Children's Social Care.
- NHS services.
- CAMHS.
- Speech and Language Therapy services.
- Occupational Therapy services.
- Educational Psychologists.
- Alternative Provision providers.
- Examination awarding organisations.
- The Department for Education.

Personal information is processed only for legitimate purposes and access is restricted to staff who require the information to fulfil their professional responsibilities.

11 Pupil Records

The Academy maintains individual pupil records to ensure that education, safeguarding and support are effectively coordinated.

Records may include:

- Admission documentation.
- Attendance records.
- Assessment information.
- EHCP documentation.
- Individual Provision Plans.

- Reading and assessment data.
- Behaviour records.
- Positive behaviour support plans.
- Risk assessments.
- Medical information.
- Safeguarding records.
- Speech and Language Therapy reports.
- Occupational Therapy reports.
- Educational Psychology reports.
- Alternative Provision reports.
- Careers information.
- Examination entries and results.

Information held within pupil files should always support the education, welfare and safeguarding of the child.

Records will be maintained accurately, reviewed regularly and transferred securely where required.

12

Staff Records

The Academy maintains confidential personnel records to support employment, safeguarding and statutory compliance.

These may include:

- Recruitment documentation.
- References.
- Identity checks.
- DBS information.
- Qualifications.
- Employment contracts.
- Payroll information.
- Training records.
- Appraisal documentation.
- Occupational health information.
- Disciplinary records where appropriate.
- Attendance records.

Access to staff records is restricted to authorised personnel.

Safeguarding Records

Safeguarding information is among the most sensitive information processed by the Academy.

Safeguarding records are maintained separately from the main pupil file where appropriate and are stored securely using the Academy's safeguarding management system.

LCE Academy uses CPOMS as its electronic safeguarding recording system.

Safeguarding records may include:

- Child protection concerns.
- Welfare concerns.
- Low-level concerns.
- Contextual safeguarding information.
- Child in Need information.
- Child Protection Plans.
- Family Help records, including records locally labelled as Early Help.
- Multi-agency communications.
- Social Care correspondence.
- Police information.
- Chronologies.
- Body maps.
- Meeting records.

All staff with a reporting role may submit concerns through their authorised CPOMS account. Access to full pupil safeguarding records, chronologies, DSL decisions and exports is restricted by role and least privilege to authorised safeguarding personnel, with access reviewed and audited.

Information will only be shared where there is a lawful basis and where sharing is necessary to safeguard a child or fulfil statutory responsibilities.

Safeguarding information will always be handled in accordance with:

- Keeping Children Safe in Education.
- Working Together to Safeguard Children.
- UK GDPR.
- The Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

The Academy recognises that data protection legislation supports appropriate safeguarding information sharing and should never prevent staff from acting to protect a child from harm.

14 Special Educational Needs Information

As an SEMH school, the Academy routinely processes significant volumes of SEND information.

This may include:

- EHCPs.
- Annual Review documentation.
- Specialist reports.
- Communication assessments.
- Learning assessments.
- Behaviour support plans.
- Therapeutic recommendations.
- Reasonable adjustments.
- Examination access arrangements.

This information is processed only where necessary to support pupils' education, wellbeing and statutory provision.

Access is limited to staff with a legitimate educational need to know.

15 Speech and Language Therapy Information

Speech, language and communication information forms an important part of many pupils' educational records.

The Academy's Speech and Language Therapist may process information relating to:

- Communication assessments.
- Therapy recommendations.
- Language profiles.
- Classroom strategies.
- Intervention programmes.
- Review notes.

Information will be shared with teaching staff where necessary to enable effective classroom practice.

Only relevant information will be shared and confidentiality will be maintained at all times.

16 Information Sharing

The Academy recognises that effective information sharing is essential for safeguarding and improving outcomes.

Information will be shared only where:

- There is a lawful basis.
- It is necessary.
- It is proportionate.
- It is relevant.
- It is accurate.
- It is shared securely.

Information may be shared with:

- Local Authorities.
- Children's Social Care.
- Police.
- NHS professionals.
- CAMHS.
- Educational Psychologists.
- Speech and Language Therapists.
- Occupational Therapists.
- Alternative Provision providers.
- Examination boards.
- Further Education providers.
- Other schools where pupils transfer.

Where appropriate, the Academy will record:

- What information has been shared.
- Why it has been shared.
- Who authorised the sharing.
- The lawful basis for sharing.

17

Confidential Conversations

Staff must take reasonable steps to protect confidential information during day-to-day practice.

Confidential discussions should not take place:

- In corridors.
- Reception areas.
- Public spaces.
- Car parks.

- Social media.
- Public transport.

Where confidential conversations are necessary, they should take place in private locations whenever reasonably practicable.

18 Email and Electronic Communication

Academy email systems must be used for Academy business.

Staff should:

- Check recipients carefully before sending emails.
- Use secure methods where sensitive information is shared.
- Password-protect or encrypt documents where appropriate and send the password through a separate communication channel.
- Avoid sending excessive personal information.
- Report accidental disclosures immediately.

Personal email accounts must not be used to store or routinely transmit confidential Academy information.

19 Academy Devices

Academy-issued devices remain the property of LCE Academy.

Staff are expected to:

- Keep devices secure.
- Use strong passwords.
- Lock devices when unattended.
- Report loss immediately.
- Install updates when prompted.
- Store information only on approved systems.

Devices should not be left unattended in public places or visible within vehicles.

20 Personal Devices

The Academy permits personal devices for Academy business only where explicitly authorised and risk assessed under the Acceptable Use Policy. Pupil images, recordings and pupil data must not be created, stored or retained on a personal device unless that specific use is authorised, necessary and securely controlled.

Where personal devices are authorised:

- Appropriate security measures must be in place.
- Password protection must be enabled.
- Devices must be encrypted where possible.
- Information must not be permanently stored.
- Authorised data is transferred promptly to the approved Academy system and securely deleted from the personal device, including temporary and cloud copies, once transfer is verified.

Pupil safeguarding concerns must be alerted immediately to the DSL or deputy and recorded factually on CPOMS as soon as reasonably practicable; recording must never delay protective action. Adult allegations and low-level concerns are held in the separate controlled personnel process unless distinct child-protection information must also be recorded for a pupil.

Personal devices must never be used where their use presents an unacceptable safeguarding or information security risk.

21 Remote Working

Where staff work remotely, they remain responsible for maintaining confidentiality.

Staff should:

- Work in private locations where possible.
- Prevent unauthorised viewing of confidential information.
- Lock screens when away from devices.
- Avoid printing confidential documents unnecessarily.
- Dispose of confidential waste securely.
- Access Academy systems only through approved methods.

Remote working arrangements must never compromise safeguarding or data security.

22 Information Technology Security

The Academy uses technical measures to protect personal information from unauthorised access, alteration or loss.

These include:

- Secure network infrastructure.
- Password controls.
- Access permissions.
- Multi-factor authentication where appropriate.

- Antivirus protection.
- Firewall protection.
- Secure backups.
- Monitoring and logging.

The Academy's IT infrastructure is supported by BluRock IT, who provide technical support and systems management under appropriate contractual and confidentiality arrangements.

23 Internet Filtering and Monitoring

LCE Academy uses Smoothwall as its confirmed filtering and monitoring provider to promote online safety and meet statutory safeguarding requirements. BluRock IT provides technical IT support but is not the filtering and monitoring provider.

Filtering and monitoring systems support the Academy by:

- Reducing exposure to inappropriate content.
- Identifying safeguarding concerns.
- Supporting online safety.
- Monitoring potential risks.
- Assisting with statutory safeguarding responsibilities.

Monitoring information will only be accessed by authorised personnel and used for safeguarding, information security or operational purposes where appropriate.

24 Contractors and Third-Party Processors

Where third parties process information on behalf of the Academy, appropriate contractual arrangements will be in place.

The Academy will ensure that providers:

- Meet UK GDPR requirements.
- Process information only on documented instructions.
- Maintain appropriate security standards.
- Notify the Academy of data breaches.
- Delete or return information when contracts end.

Regular assurance will be sought where appropriate.

25 Confidential Waste and Secure Disposal

Confidential information must be disposed of securely.

Paper records containing personal information will be shredded using approved confidential waste arrangements.

Electronic information will be securely deleted in accordance with recognised data destruction procedures.

Staff must never dispose of confidential information within general waste or recycling facilities.

Maintaining secure disposal arrangements is recognised as an essential part of protecting the privacy and dignity of pupils, families and staff.

26 Individual Rights

LCE Academy recognises that individuals have rights under UK GDPR regarding their personal information.

The Academy will ensure these rights are respected whilst balancing safeguarding responsibilities, legal obligations and the rights of others.

Individuals have the right to:

- Be informed about how their information is used.
- Request access to their personal information.
- Request correction of inaccurate information.
- Request restriction of processing where appropriate.
- Object to certain processing activities where applicable.
- Request deletion where the legal conditions are met.
- Request transfer of information where applicable.

These rights are not absolute and may be restricted where legislation permits, particularly where disclosure may place a child or another individual at risk of harm.

27 Subject Access Requests

Individuals have the right to request access to personal information held by the Academy.

Requests may be made verbally or in writing.

The Academy will:

- Verify the identity of the applicant.
- Clarify the scope of the request where appropriate.
- Locate relevant information.
- Consider any applicable exemptions.
- Redact information relating to third parties where required.
- Respond within the statutory timescale.

Where requests involve safeguarding information, legal advice or advice from the Data Protection Lead may be sought before disclosure.

Where requests relate to children, the Academy will consider the child's age, maturity, understanding and legal rights before determining whether information should be disclosed to a parent or carer.

28 Access to non-personal information and transparency

An ordinary independent school is not normally a public authority for the purposes of the Freedom of Information Act 2000. The Academy nevertheless responds transparently to reasonable requests where lawful and proportionate and complies with any disclosure duty that applies to a particular record, contract, commissioner, court, regulator or inspection body. Personal-data requests follow the subject-access route.

Requests for non-personal information are logged and considered separately from subject access requests. The Academy protects personal data, safeguarding information, security-sensitive material, commercial confidentiality and legal privilege and records the reason for any refusal or redaction.

29 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment will be completed before new processing that is likely to result in a high risk to individuals. This includes intrusive monitoring, CCTV, biometrics, new safeguarding or pupil-tracking platforms, significant use of generative AI, automated profiling or decision support, and large-scale processing of special-category children's data. No solely automated decision with legal or similarly significant effect will be made about a pupil unless a lawful route, required safeguards and meaningful human review are in place.

Examples include:

- Introduction of new electronic systems.
- CCTV installations.
- Biometric systems if introduced.
- New safeguarding platforms.
- Large-scale processing of special category data.
- Significant changes to existing systems.

The Data Protection Lead will advise on the completion of DPIAs where appropriate.

30 Personal Data Breaches

A personal data breach is any incident that results in the accidental or unlawful:

- Loss of personal information.
- Destruction of information.
- Alteration of information.

- Unauthorised disclosure.
- Unauthorised access.

Examples include:

- Sending confidential information to the wrong recipient.
- Loss of paperwork.
- Lost or stolen devices.
- Unauthorised access to records.
- Cyber security incidents.
- Inappropriate disclosure during conversations.

All suspected breaches must be reported immediately to the Headteacher and Kathryn McAuley, Data Protection Lead.

Staff should never attempt to conceal a breach.

31 Managing Data Breaches

Where a breach occurs, the Academy will:

1. Contain the breach immediately.
2. Assess the level of risk.
3. Protect affected individuals where possible.
4. Record the incident.
5. Inform the Data Protection Lead.
6. Determine whether notification to the Information Commissioner's Office is required.
7. Notify affected individuals where legally required.
8. Review lessons learned.
9. Update procedures where necessary.

Where required by legislation, notifiable breaches will be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

32 Record Retention

The Academy retains information only for as long as necessary to fulfil its legal, safeguarding, educational and operational responsibilities. A controlled retention and disposal schedule names each record class, owner, trigger, retention period, legal or guidance basis, disposal method, litigation/safeguarding hold and review date.

Retention periods are determined by:

- Statutory requirements.
- Department for Education guidance.
- Information Records Management Society guidance.
- Safeguarding requirements.
- Employment legislation.
- Financial regulations.

At the end of the retention period information will be securely destroyed or permanently deleted.

33

Staff Training

Effective data protection relies upon knowledgeable staff.

All staff will receive:

- Data protection training during induction.
- Annual refresher training.
- Safeguarding information sharing guidance.
- Cyber security awareness.
- Password security guidance.
- Information handling expectations.

Additional training will be provided where staff have responsibilities involving large volumes of confidential or safeguarding information.

Training records will be maintained by the Academy.

34

Monitoring Compliance

Compliance with this policy will be monitored through:

- Internal audits.
- Data protection reviews.
- Information security checks.
- Staff supervision.
- Review of reported incidents.
- Monitoring by the Data Protection Lead.
- External advice where appropriate.

Findings will be used to strengthen practice and reduce future risk.

Complaints

The Academy provides an accessible route for complaints about its processing of personal data. A complaint may be sent to Kathryn McAuley, Data Protection Lead, through the published school contact details; assistance will be provided where disability, language or communication creates a barrier. Under section 164A of the Data Protection Act 2018, the Academy will acknowledge the complaint within 30 days, investigate without undue delay, keep the complainant appropriately informed and communicate the outcome promptly. The response will explain any action taken and the right to complain to the Information Commissioner's Office. Data complaints that also engage safeguarding, employment or the general Complaints Policy will be coordinated so that no statutory duty or protective action is delayed.

Monitoring and Review

The Headteacher has overall responsibility for monitoring implementation of this policy.

Krystian Liptrot, as Chair of the proprietor board and company acting on behalf of Life Changing Education Ltd, receives assurance on the following matters. The governing body may provide recorded advice and challenge without displacing the accountability of Life Changing Education Ltd:

- Appropriate information governance arrangements are in place.
- Statutory obligations are met.
- Data breaches are reviewed.
- Staff receive appropriate training.
- Risks are effectively managed.

This policy will be reviewed:

- Annually in July.
- Following significant legislative changes.
- Following advice from the Information Commissioner's Office.
- Following serious data breaches.
- Following changes to Academy systems or processing activities.