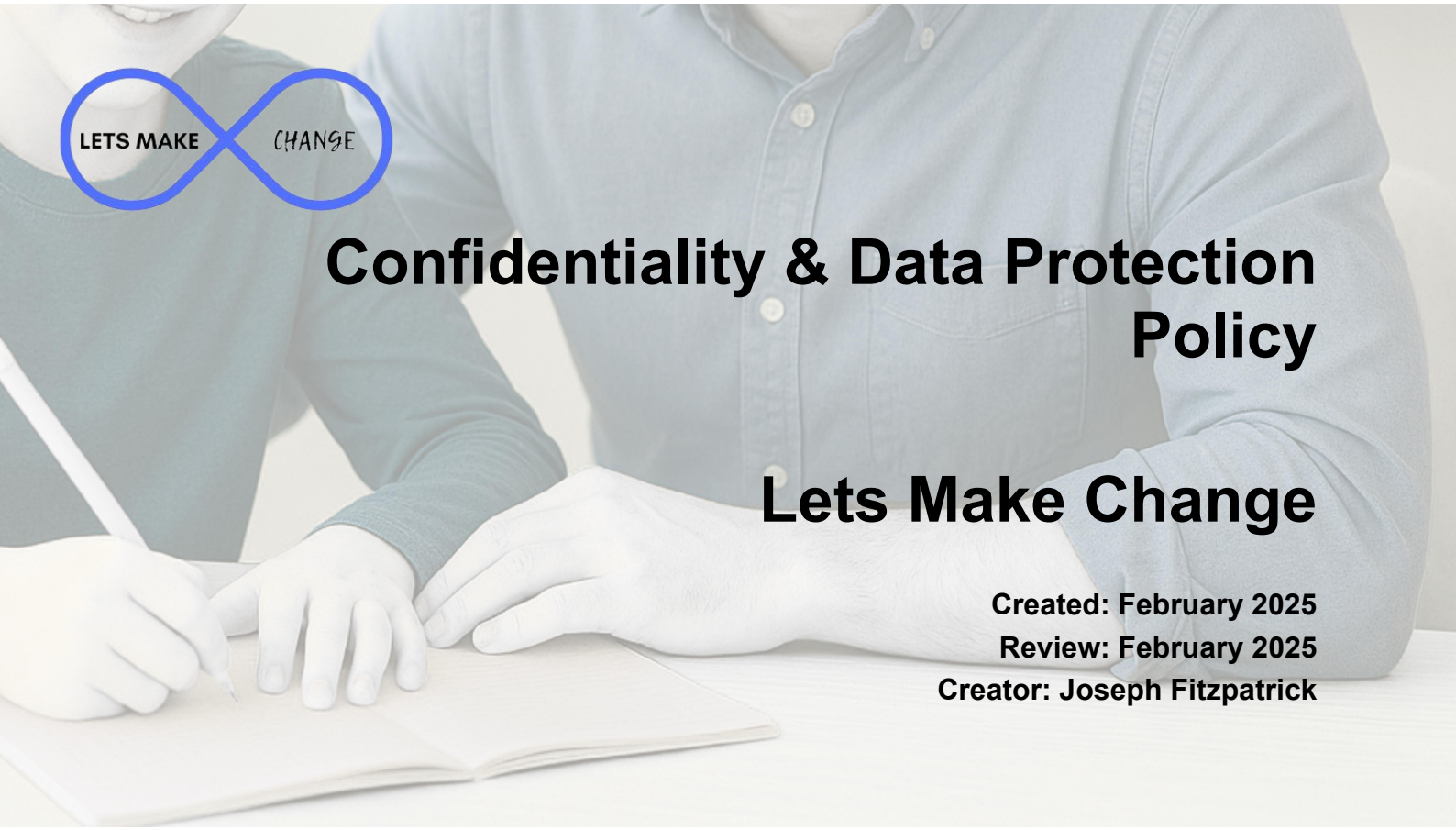

Confidentiality & Data Protection Policy

Lets Make Change

Created: February 2025
Review: February 2025
Creator: Joseph Fitzpatrick

1. Introduction

Let's Make Change is committed to maintaining the highest standards of confidentiality and data protection. As a community-based tutoring organisation, we recognise our responsibility to protect the personal information of children, parents, staff, and volunteers in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Lets Make Change is committed to data protection an is registered with ICO an independent body that regulates data protection and privacy laws, provides guidance to organizations and the public on information rights, and takes action against those who do not comply with the law.

2. Scope

This policy applies to all staff, tutors, volunteers, and third-party service providers who handle personal data as part of their role within Let's Make Change. It covers all personal and sensitive information collected, stored, and processed in connection with our tutoring services.

3. Principles of Data Protection

3.1 Lawfulness, fairness, and transparency – Personal data will be processed fairly and lawfully, with transparency about how it is used.

- For learners/parents: Parents will always be told why their child's data (e.g. attendance, learning needs, safeguarding notes) is being collected. Nothing is hidden.
- For staff/tutors: Their personal data (DBS checks, payroll details) is handled fairly, only for employment reasons.
- For commissioners/local authority: They will be told clearly what learner data is shared with them and why.

3.2 Purpose limitation – Data will only be collected for specific, explicit, and legitimate purposes.

- For learners/parents: A learner's information is collected for education, safeguarding, and wellbeing purposes — not for marketing or unrelated use.
- For staff: Staff information is collected for employment, safeguarding checks, and training — not for other uses.
- For commissioners: Data shared with them is only for fulfilling contracts and monitoring learner progress.

3.3 Data minimisation – Only the necessary amount of data will be collected and processed.

- For learners/parents: You won't ask for unnecessary details
- For staff: Only job-related data will be collected (e.g. qualifications, DBS) — not irrelevant personal details.
- For commissioners: Only essential learner data will be shared, not whole files.

3.4 Accuracy – Data will be kept accurate and up to date where necessary.

- For learners/parents: Parents can update emergency contacts, medical needs, or address changes at any time to keep records correct.
- For staff: Staff can request corrections to their employment or payroll records.
- For commissioners: Reports sent will use the most accurate, updated information.

3.5 Storage limitation – Data will not be kept longer than necessary for its intended purpose.

- For learners/parents: Learner records are only kept as long as required (e.g. safeguarding records until age 25, attendance/progress for contract duration).
- For staff: Payroll and HR records are kept for the legally required time, then deleted securely.
- For commissioners: Data is only stored for as long as necessary to meet funding/reporting requirements.

Integrity and confidentiality – Personal data will be handled securely to protect against unauthorised or unlawful processing.

4. Collection and Use of Personal Data

Types of Personal Data We Collect:

- Learners: name, date of birth, home address, contact details, emergency contacts, medical needs (e.g. allergies, health conditions), education history, attendance, behaviour notes, learning progress, and safeguarding information where required.
- Parents/Carers: contact details, consent forms (e.g. photo/video use, trip permissions, medical treatment), records of communication with LMC.
- Staff/Tutors: recruitment information (applications, references, DBS details, qualifications), payroll and bank details, emergency contacts, training records, safeguarding records where relevant.

Why We Collect This Data:

- To safeguard learners by ensuring we have up-to-date emergency and medical details.
- To deliver educational services, track progress, and share reports with parents/carers and commissioners.
- To comply with legal and contractual obligations, e.g. safeguarding duties, local authority monitoring, HMRC requirements.
- To communicate effectively with parents/carers about learner progress, attendance, trips, or concerns.
- To recruit, support, and manage staff/tutors safely and in line with safer recruitment practices.

How We Use Personal Data:

- Learner data is used to plan, deliver, and evaluate educational sessions, support wellbeing, and keep children safe.
- Parent/carer data is used to maintain clear communication and respond in case of emergencies.
- Staff/tutor data is used to ensure safer recruitment, process salaries, and monitor training and safeguarding responsibilities.
- Information may be shared with commissioners/local authorities only on a need-to-know basis, for example, reporting attendance and progress.
- Safeguarding data will be shared with relevant agencies if a child is at risk of harm, in line with statutory duties.

Consent:

We obtain parental consent for matters such as:

- Use of photographs/videos for learning or promotional purposes.
- Participation in trips, activities, or medical treatment if required
- Where consent is required, it will be clearly explained and parents/learners have the right to withdraw consent at any time.

Your Rights:

Right of Access (Subject Access Request)

- You can request a copy of the personal data we hold about you or your child.
- Requests can be made verbally or in writing to the LMC Data Protection Officer/Management.
- We will respond within one month of receiving the request.

Right to Rectification (Corrections)

- If any personal data we hold is inaccurate or incomplete, you have the right to ask us to correct it.
- This includes updating contact information, correcting learner records, or amending staff details.

Right to Erasure (Right to be Forgotten)

- In some cases, you may request that we delete personal data.
- This will be considered where data is no longer needed for its original purpose, where consent has been withdrawn, or where there is no overriding legal/safeguarding reason to keep it.

Right to Restrict Processing

- You may ask us to limit how we use your personal data.
- For example, while a concern or correction request is being investigated, data may be restricted from further use.

Right to Object

- You may object to your data being used in certain ways, such as for research or non-essential communication.
- We will stop processing unless there is a compelling legitimate reason or legal obligation to continue.

Right to Data Portability

- You can request that your data be transferred to another organisation (for example, if a learner moves to a different provider).
- We will provide the data in a structured, commonly used, and machine-readable format.

How to Exercise Your Rights:

- Requests can be made by email, letter, or verbally to LMC management.
- Proof of identity may be required to protect your data.
- We will not charge a fee unless a request is excessive or repeated.
- If we cannot comply with a request due to safeguarding or legal reasons, we will explain why.

Complaints:

If you are unhappy with how we handle your data, you can raise a concern with us directly.

You also have the right to complain to the Information Commissioner's Office (ICO) at www.ico.org.uk.

5. Confidentiality Obligations

Non-disclosure of Information:
All staff, tutors, and volunteers must ensure that personal or sensitive information about learners, parents/carers, or colleagues is **never disclosed to unauthorised individuals**. Unauthorised disclosure could cause harm, breach trust, or result in a violation of data protection law.

Sharing Learner Information:
Information regarding learners (such as progress reports, attendance, or wellbeing concerns) must only be shared with a learner's **parent, carer, or legal guardian**, unless there is a legal or safeguarding obligation that requires sharing with another professional or agency (e.g. local authority, social services, or emergency services). In such cases, only the **minimum information necessary** will be shared, and always in line with safeguarding duties and GDPR.

Confidentiality Agreement:
All staff, tutors, and volunteers must sign a **confidentiality agreement** when joining LMC. This confirms their understanding that they are handling sensitive information and their duty to keep it secure. Any breach of confidentiality may result in disciplinary action and, in some cases, legal consequences.

Secure Handling of Information:

- Personal data must be stored securely (e.g., password-protected systems, locked cabinets for paper records).
- Information must not be left unattended in public spaces, discussed in open areas, or shared via unsecured emails or messaging platforms.
- Tutors working in community venues must ensure that paper notes are kept safe during sessions and returned to management for secure storage.

Safeguarding Exception:
Where a safeguarding concern arises, confidentiality cannot be promised to learners. Staff have a duty to share relevant information with the Designated Safeguarding Lead (DSL) or with external safeguarding agencies, in line with statutory requirements.

6. Data Storage and Security

Secure Storage of Personal Data
Personal data will always be stored securely, whether in physical paper format or digitally. This ensures the privacy and protection of learners, parents/carers, staff, and volunteers at all times.

Physical Security (Paper Records)

- Any paper records, such as consent forms, attendance registers, or incident reports, will be stored in locked filing cabinets in secure LMC office space.
- Only authorised members of management will hold keys to these cabinets.
- Tutors who collect information during community sessions must return any paperwork to management promptly for secure storage, ensuring sensitive data is not left unattended in public spaces or vehicles.

Digital Security (Electronic Records)

- Digital data (such as learner records, medical information, or safeguarding notes) will be stored on a secure, cloud-based system that is GDPR-compliant.
- Access will be restricted to authorised personnel only, based on their role and responsibility within the organisation.
- Two-Factor Authentication (2FA) will be implemented wherever possible, requiring staff to use both a password and a secondary method (e.g. text code or authenticator app) to log in.
- All files will be password-protected and regularly updated to maintain security.
- Laptops, tablets, and mobile devices used for work purposes must be encrypted, locked with strong passwords or PINs, and not shared with unauthorised individuals.

Encryption and Backups

- Sensitive data will be encrypted both when stored and when transmitted (e.g. emailing personal details).
- Regular backups of digital records will be maintained securely to prevent data loss due to system failure or cyber incidents.

Access Control

- Access to personal data will be given only to those staff, tutors, or volunteers who need it for legitimate work purposes.
- Permissions will be regularly reviewed to ensure data is not accessed unnecessarily.
- When staff or tutors leave the organisation, their access to systems and files will be immediately revoked.

Prevention of Data Breaches
We will maintain strict measures to prevent data breaches, including:

- Staff training on data protection and cyber safety.
- Monitoring and reviewing access logs.
- Immediate reporting and investigation of any suspected breach.
- Following the correct procedure to inform affected individuals and the ICO (Information Commissioner's Office) if a breach occurs.

7. Data Sharing and Third Parties

- Limited Sharing: Personal data will only be shared with third parties (such as local authorities, schools, or partner agencies) where it is essential for delivering services, meeting safeguarding duties, or fulfilling legal obligations. In all cases, only the minimum necessary information will be shared.
- Safeguards in Place: Whenever data is shared, strict safeguards will be applied to ensure it is transmitted securely (e.g. encrypted email, secure portals). Parents, carers, and staff will be informed where appropriate.
- Third-Party Compliance: Any third-party organisations or data processors working with LMC must demonstrate full compliance with UK GDPR and sign a data processing agreement confirming they will protect personal data to the same high standard.

8. Rights of Data

- Access: Individuals can request a copy of the personal data LMC holds about them. We must respond within one month and provide the data in a clear and accessible format.
- Correction: If any personal data is inaccurate or incomplete (e.g. wrong contact details or medical information), individuals have the right to request it be corrected without delay.
- Deletion ("Right to be Forgotten"): In certain circumstances (such as when data is no longer needed for service delivery, or consent is withdrawn), individuals may request their data be deleted. However, this does not apply where we must retain data for safeguarding, legal, or contractual obligations.
- Objection to Processing: Individuals can object to their data being processed for specific purposes (e.g. marketing or non-essential processing). Where the objection is valid, LMC will stop processing unless there are overriding legitimate grounds.

9. Breach Reporting

Immediate Reporting:
Any suspected or actual breach of personal data must be reported immediately to the organisation's Data Protection Officer (DPO) or designated manager. This includes accidental loss, unauthorised access, disclosure, or destruction of personal data. Prompt reporting ensures that action can be taken quickly to minimise risk to learners, staff, or parents.

Assessment and Containment:
Once reported, the DPO will assess the nature and severity of the breach, contain it where possible, and identify which individuals or systems are affected. This may include securing compromised systems, retrieving lost information, or restricting access.

Notification to the ICO:
For serious breaches that could result in risk to individuals' rights and freedoms, the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours, as required by UK GDPR.

Communication to Affected Individuals:
Where the breach poses a high risk to affected individuals (e.g., exposure of sensitive learner information), LMC will notify those impacted without undue delay, explaining the nature of the breach and any steps they should take.

Review and Prevention:
Following any breach, the DPO and management will review procedures, update risk assessments, and implement additional safeguards to prevent recurrence. Staff will be reminded of best practices and, where necessary, receive further training on data protection and security

10. Policy Review

Annual Policy Review:
This Data Protection and Confidentiality Policy will be formally reviewed at least once a year to ensure it remains fully compliant with current UK data protection legislation, including the UK GDPR and Data Protection Act 2018. Reviews may also take place sooner if there are significant changes in legislation, guidance from the Information Commissioner's Office (ICO), or organisational practice. Updates from the review will be communicated to all staff, tutors, and relevant stakeholders.

Staff Training:
All staff, tutors, and volunteers will receive regular training on data protection, confidentiality, and security best practices. This training ensures that everyone understands their responsibilities, knows how to handle personal data safely, and is aware of procedures for reporting breaches or concerns. Refresher training will be provided periodically, and all new staff will complete a mandatory induction on data protection.

Commitment to Confidentiality and Security:
By adhering to this policy, Lets Make Change (LMC) demonstrates its commitment to maintaining the confidentiality, integrity, and security of all personal data processed within our tutoring services. This commitment underpins trust with learners, parents/carers, staff, and commissioners, ensuring that personal information is handled lawfully, securely, and transparently.

By adhering to this policy, Let's Make Change ensures the confidentiality and security of all personal data handled within our tutoring services.

Date of Implementation: 27/08/25
Next Review Date: 27/08/26
Approved by: Joseph Fitzpatrick (Director)