

The Log Cabin Charity

Data Protection Policy

1. Introduction

The Log Cabin Charity ("the Charity") processes a considerable volume of personal and special category data about children and young people, families, staff, volunteers, contractors, and visitors. This policy delineates the Charity's compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, relevant Codes of Practice established by the Information Commissioner's Office (ICO), and the Age-Appropriate Design Code (Children's Code).

The Charity is committed to ensuring that all personal data is:

- Handled in a lawful, fair, and transparent manner
- Processed securely
- Protected from misuse, loss, or unauthorised access
- Retained only for the duration necessary
- Utilised solely for legitimate and explicitly stated purposes

Failure to comply with this policy may lead to disciplinary measures, underscoring the importance of everyone's role in maintaining data security and trust.

2. Definitions

Personal Data: Any information that relates to an identifiable living person.

Special Category Data: This includes information regarding health, special educational needs and disabilities (SEND), race/ethnicity, religion, sexual orientation, biometric data, safeguarding notes, and behavioural information.

Criminal Records Data: Information related to offences, allegations, or investigations.

Data Subject: Any individual whose personal data is processed.

Data Controller: The Log Cabin Charity

Data Protection Lead: The Head of Service is responsible for overseeing day-to-day compliance, supporting staff, responding to rights requests, and liaising with the Information Commissioner's Office (ICO) when necessary.

Processing: Any action involving data, such as collecting, storing, using, sharing, erasing, or destroying it.

The Log Cabin Charity

3. Data Protection Principles

Data Protection Principles The Charity actively adheres to all principles outlined in the UK GDPR, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security.

Additionally, the Charity's adherence to the accountability principle and the ICO Children's Code aims to foster trust and confidence among all involved in data governance.

4. Lawful Bases for Processing

The Charity processes personal data using the following lawful bases:

Personal Data

- Consent (where appropriate and clearly obtained)
- Contract
- Legal obligation (Ofsted, safeguarding, employment law)
- Vital interests
- Public interest / statutory duties
- Legitimate interests (where not overridden by individual rights)

Special Category Data

Must also meet *one* of these conditions:

- Explicit consent
- Employment/social protection obligations
- Vital interests
- Substantial public interest (e.g., safeguarding, SEND, health/safety)
- Health and social care
- Legal claims
- Archiving/statistics/research

5. Children's Data & the ICO Children's Code

The Log Cabin Charity must meet enhanced obligations:

- Act in the **best interests of the child**
- Apply **high privacy settings by default**
- Conduct **Data Protection Impact Assessments (DPIAs)** for any digital tools involving children
- Limit profiling or tracking
- Avoid unnecessary data collection
- Provide age-appropriate explanations where children can understand what is happening with their data
- Ensure staff are trained in handling children's personal and sensitive data safely

All systems used with or for children must comply with the Children's Code principles.

6. Data Minimisation & Digital Use

Staff must:

- Only collect the minimum data necessary
- Use the Log Cabin Charity **devices** where possible
- Never store personal data on personal phones or personal email accounts
- Use encrypted platforms for communication
- Avoid WhatsApp for safeguarding or sensitive information
- Use the Charity's cloud storage systems correctly
- Ensure photos/videos follow parental consent rules and safeguarding expectations

The Log Cabin Charity

7. Accuracy

Data must be kept accurate and up to date.

Families and staff are responsible for informing the Charity of changes.

- The Charity will correct inaccuracies without delay.

Data is retained in accordance with the LCC Retention Schedule. The methods for secure disposal include:

- Secure deletion
- Shredding
- Certified deletion by the IT provider
- Restricted access before destruction

Records that require safeguarding adhere to statutory retention periods and may not be subject to standard deletion rules, including those that allow deletion at a subject's request.

9. Data Security & Cybersecurity

Security measures include MFA, strong passwords, encryption, managed devices, firewalls, role-based access, cyber monitoring, and regular updates. Staff must lock screens, keep devices secure, avoid unencrypted USBs, report suspicious emails, and handle portable devices safely.

10. Sharing Personal Data

Data sharing with local authorities, the Local Authority Designated Officer (LADO), schools, health professionals, the police, Ofsted, and approved third-party processors must comply fully with the UK GDPR and relevant safeguarding legislation. Sharing is permitted only when it is legally required, necessary to protect a child or vulnerable person, or in the wider public interest.

Recognising shared responsibility is essential for maintaining trust and accountability. Any organisation or individual processing data on behalf of the charity must meet the same legal and safeguarding standards, and must sign an appropriate data protection agreement before processing begins. This ensures that all personal data is handled lawfully, securely, and transparently, reinforcing confidence among children, families, partners, and regulators.

11. International Transfers

Personal data will only be transferred outside the UK in the following circumstances:

- The destination has received an adequacy decision.
- The Charity uses the ICO International Data Transfer Addendum (IDTA) or another approved equivalent mechanism.

IT providers must confirm their compliance with data transfer requirements before any transfers occur, emphasising the need for accountability and adherence to policies.

The Log Cabin Charity

12. Data Subject Rights

Individuals have the following rights regarding their personal data:

- Access their data
- Request rectification of inaccuracies
- Request erasure, unless there are safeguarding or legal exemptions
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent
- Not be subject to automated decision-making

Requests should be sent to the Data Protection Lead immediately to ensure your concerns are addressed promptly and securely.

13. Subject Access Requests (SARs)

The Charity will respond to Subject Access Requests within the following timeframes:

- 1 calendar month for standard requests.
- Up to 2 additional months for complex cases (with prior notice).

Please note that safeguarding exemptions apply if disclosing information could place a child at risk. For example, if revealing specific details might compromise a child's safety, the exemption is invoked. Staff should refer to the comprehensive SAR procedure, which provides detailed criteria and examples, to ensure proper handling of such cases.

14. Intersections of Safeguarding and Data Protection

The Charity processes safeguarding data based on the following grounds:

- Legal obligations
- Substantial public interest
- Vital interests

Safeguarding data may be shared without consent in the following situations:

- When a child is at risk of significant harm
- When there is a legal requirement to disclose information
- When professionals require information to protect a child

Staff members are encouraged to document any concerns factually, securely, and immediately to promote a sense of responsibility and trust. Data should never be stored on personal devices.

The Log Cabin Charity

Any requests should be sent to the Data Protection Lead as soon as possible to ensure your concerns are addressed promptly and securely.

15. Breach Reporting

A personal data breach is the loss, destruction, unauthorised access to, or disclosure of personal data. Staff members must:

- Report breaches immediately to the Data Protection Lead.
- Refrain from investigating the breach themselves.
- Follow any emergency instructions provided.

The Charity will:

- Assess the severity of the breach within 24 hours.
- Report notifiable breaches to the Information Commissioner's Office (ICO) within 72 hours.
- Notify affected individuals when there is a high risk.
- Record all breaches, including minor ones.

16. Data Protection by Design and Data Protection Impact Assessments (DPIAs)

DPIAs are required in the following circumstances:

- When using new digital tools.
- When processing special category data at scale.
- When monitoring individuals.
- When sharing systems with external partners.
- When using automated processing tools.
- When online platforms involve children.

DPIAs must be approved by the Data Protection Lead.

17. Data Processors and Contracts

Contracted suppliers must:

- Provide evidence of their compliance.
- Meet ICO standards.
- Support breach investigations.
- Delete or return data at the end of the contract.
- Sign a Processor Agreement that includes Articles 28 and UK GDPR clauses.
- Comply with the International Data Transfer Agreement (IDTA) for data transfers.

An annual review of all data processors is required to ensure ongoing compliance with contractual obligations and data protection standards. This review should assess their adherence to ICO standards, support for breach investigations, and data deletion or return procedures.

The Log Cabin Charity

18. Training & Awareness

Mandatory training includes:

- Induction training for new staff
- Annual training sessions
- Refresher modules (briefings and supervision)
- Scenario-based training on safeguarding and data handling

Ensure that staff members record their training completion in the LCC training matrix to maintain accountability and support compliance efforts.

19. Monitoring & Audit

The Charity conducts:

- Annual data protection audits
- Quarterly spot checks
- Policy reviews
- System access reviews
- Monitoring of the breach log

The findings from these activities inform continuous improvement.

20. Automated Processing & Profiling

The Charity does not engage in automated decision-making that produces legal or significant effects. However, it does utilise low-risk computerised tools (such as incident logging and HR reminders) that:

- Support decision-making
- Do not replace human judgment
- Must be monitored for fairness and accuracy

21. Policy Review

This policy will be reviewed annually or sooner if significant changes occur to ensure ongoing relevance and compliance.

This policy was reviewed on:

Date: 04th December 2025

Signed:



Job/role title: Head of Service

Date: 04th December 2025