

LNK:



DATA PROTECTION POLICY

**LIVES
NOT
KNIVES**

ABOUT: LIVES NOT KNIVES

Document Name	Data Protection Policy
Version	2.0
Produced By	Callum Clements
Contributors	Board of Trustees
Last Review Date	May 2024
Next Review Date	May 2025
Signed Off By	Board of Trustees

Contents

PAGE	CONTENTS
4	Introduction Policy Benefits
5	ICO Policy Statement
6	Purpose Policy Objectives
7	Principles Policy Scope
8	Procedures Internal Data Records
9	Accuracy Storage Use Of Photographs External Data Records
10	Consent Personal Data Access Accuracy
11	Disclosure and Barring service Responsibilities of Staff, Volunteers and Board Members Compliance
12	Security Retention Of Data Policy Communication
13	Policy Revisions

1. INTRODUCTION

At Lives Not Knives, we are dedicated to protecting the privacy and security of personal data entrusted to us by our beneficiaries, volunteers, employees, and partners. This Data Protection Policy outlines our approach to collecting, using, storing, and safeguarding personal information following applicable data protection laws and regulations.

We understand that privacy is a fundamental right, and responsible handling of personal data is crucial to maintaining the trust and confidence of those we work with. This policy establishes the principles and practices we follow to ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes related to our mission
- Adequate, relevant, and limited to what is necessary for our charitable activities
- Accurate and kept up to date
- Kept in a form that permits identification for no longer than necessary
- Processed in a manner that ensures appropriate security and confidentiality

This policy applies to all staff members, volunteers, trustees, and third parties who handle personal data on behalf of Lives Not Knives. It is designed to provide a framework for compliance with data protection regulations, including but not limited to the General Data Protection Regulation (GDPR) and other applicable local laws.

We recognise that as a charity, we have a special responsibility to handle personal data with the utmost care, as it often relates to vulnerable individuals or sensitive situations. This policy reflects our commitment to upholding the highest data protection standards while fulfilling our charitable objectives.

POLICY BENEFITS

This policy will benefit LNK by:

1. Enabling excellent standards of management and processing of personal data through the provision of a consistent and stable culture towards data protection.
2. Ensuring continued compliance with the DPA principles.
3. Providing an appropriately supportive environment and culture towards best practice processing and protection of personal data.
4. Ensuring staff confidence and compliance in their processing of personal data, being fully informed and aware of their responsibilities and obligations.
5. Reducing the potential risk of legal or reputational damage through poor personal data management.
6. Providing confidence to the LNK community that their personal data is being handled correctly and ensuring individuals and members know how to access it.

2. ICO

The ICO (Information Commissioner's Office) is the UK's independent authority responsible for upholding the information rights in public interests and the data privacy of individuals. To elaborate, the major aim of the ICO is to ensure that the rights of individuals over their own data are duly respected and protected.

How are we compliant with the ICO

1. **Know why we have the data** – LNK should know why we have data and be able to explain to others why we use it in ways that are fair and lawful.
2. **Protect the data** - LNK needs to keep the data safe and destroy it securely when it's no longer needed. If the data is sensitive; this includes health information, LNK must take extra steps to protect it. This could be storing it in password-protected files or only certain members of staff have access to files.
3. **Be Transparent** – communication about data should be in simple language and not in jargon. This means no specific terms to the organisation should be used.
4. **Get consent** – A signature or confirmation that they are happy to share data is sufficient. This for example is done by giving consent on our forms to take photography or videography.
5. **Keep up to date** – LNK should regularly review our privacy information to ensure its accurate.

3. POLICY STATEMENT

1. Lives Not Knives CIO collects and uses information about people, with whom it communicates and fully understands its obligations to ensure that personal information is treated fairly, lawfully, and correctly.
2. LNK is committed to achieving compliance to the laws of the Data Protection Act (DPA) 1998. To this end, LNK fully endorses and adheres to the Principles of Data Protection, as set out in the Data Protection Act 1998.
3. Sensitive personal data collected by LNK must be dealt with properly and securely however it is collected, recorded, and used – whether on paper copies, electronically, and/or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998.
4. Individuals working for/ or who are members of LNK have the right to view and amend any of their personal data held by LNK (both electronically and/or within a manual filing system).
5. LNK prioritises and is committed to ensuring that all staff members and volunteers are aware of the Data protection policy and (where required) are appropriately trained and supported to achieve compliance with the DPA.

4. PURPOSE

1. LNK needs to collect and process personal data about members, including staff and individuals with whom it engages, to operate its daily activities and for the organisation to operate effectively.
2. The purpose of this policy is to ensure that the staff, volunteers, advisory board, and other individuals LNK is in contact with, are clear about the purpose and principles of Data Protection. In addition, it ensures that the organisation has guidelines and procedures in place which are consistently followed.
3. Failure to adhere to the Data Protection Act 1998 is unlawful and could result in legal action being taken against LNK, including its staff, volunteers, and /or board members.

5. POLICY OBJECTIVES

The objectives of this policy are to ensure that:

- Proper procedures are in place for the processing and management of personal data
- There is someone within the organisation who has specific responsibility and knowledge about data protection compliance.
- A better and more supportive environment and culture of best practice processing of personal data is provided for staff (including contract staff).
- All LNK staff (including contract staff) understand their responsibilities when processing personal data and the methods of handling information.
- Individuals wishing to submit a request for information held by LNK about them are fully aware of the procedure, whom to contact, and that requests will be dealt with promptly and courteously.
- Individuals are assured that their personal data is processed in accordance with the data protection principles and that their data is always secure and safe from unauthorised access, alteration, use, or loss.
- External organisations with whom LNK needs to share or transfer data comply with the requirements.
- Any new systems being adopted are assessed on whether they will hold personal data, whether the system presents any risks, damage, or impact to individuals' data, and whether meets this policy.

6. PRINCIPLES

The principles as outlined below, apply to “personal information” held electronically or in manual filing systems, from which individuals are identifiable. The Data Protection Act 1998 regulates the processing of personal information relating to individuals including the obtaining, holding, using, or disclosing of such information. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

LNK fully endorses and adheres to the Data Protection Principles given below. LNK’s staff members, volunteers, and board members who process or use any personal information in the course of their duties must always comply with the Data Protection Principles of good practice.

These Data Protection Principles in the Data Protection Act 1998 are outlined below:

1. Personal data will be processed fairly and lawfully: Data shall be obtained and used for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or purposes
2. Personal data will only be collected and used for specified purposes: Data must be fairly and lawfully processed and shall not be processed unless specific conditions 1 under Schedule 2 (personal data) and Schedule 3 (sensitive personal data) of the Act are met.
3. Data will be adequate, relevant, and not excessive: Data shall be adequate, relevant, and not excessive to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and kept up to date.
5. Data will not be held any longer than necessary: Personal data shall not be kept for longer than is necessary for the purpose or purposes it was collected for.
6. Personal data shall be processed in line with the rights of data subjects under this act.
7. Personal data will be kept safe from unauthorised access, accidental loss, or damage: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.
8. Personal Data will not be transferred to a country outside the European Economic Area: unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals about the processing of their personal data.

7. POLICY SCOPE

1. This policy applies to all personal data and sensitive personal data collected which is processed by LNK in the conduct of its activities/ business, using data in electronic format from any medium or paper filing systems.
2. This policy applies to all LNK staff, volunteers, and employees, whether permanent, temporary, contractors, or consultants.
3. Disciplinary action may be taken against staff failing to comply with this policy.

8. PROCEDURES

The following procedures have been developed to ensure that LNK meets its responsibilities in terms of the Data Protection Act. For these procedures data collected, stored, and used by LNK falls into two broad categories:

- LNK's internal data records for Staff, contract workers, volunteers, and board members.
- LNK's external data records for service users.

LNK is the Data Controller under the Act, and LNK's trustee board is ultimately responsible for the policy's implementation

Collection of personal data may include data for:

- individuals who have engaged with LNK via events, seminars, workshops and services provided by LNK.
- Members of trustee's board.Past, current and prospective employees.
- Suppliers, consultants, external business partners and other third parties with whom LNK communicates.
- Other persons as required by law.

9. INTERNAL DATA RECORDS

LNK obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from staff, volunteers and board members. This data is stored and processed for the following purposes:

- Recruitment.
- Volunteering opportunities.
- Equal opportunities monitoring.
- Anonymous surveys/ research.
- To distribute relevant organisational material e.g. meeting minutes etc.
- Payroll.

10. ACCURACY

- 1.LNK will take reasonable steps to keep personal data up to date and accurate.
- 2.Personal data will be stored for 6 years after a member, staff, volunteer or committee member has worked for the organisation and brief details for longer.
- 3.Unless the organisation is specifically asked by an individual to destroy their details, it will keep them on file for future reference. The Director is responsible for destroying personnel files.

11. STORAGE

1. Personal data is kept in paper-based systems and on a password-protected computer system.
2. Every effort is made to ensure that paper-based data are stored in organised and secure systems.
3. LNK is committed to GDPR compliance across our digital platforms. LNK utilises Microsoft 365, SharePoint, Upshot, Constant Contact, Brevo, Enthuse, Stripe and Just Giving. These are selected for their strong security measures, guaranteeing that all personal data is processed, stored, and transferred in compliance with GDPR regulations

Personal data for Children, Young People, Parents, and Carers will be retained as follows:

- Participant records (including personal information, consent forms, and attendance data) will be retained for 3 years after the last point of engagement with LNK's services
- Safeguarding records must be kept for 6 years after the last point of contact
- Medical information and accident reports will be retained for 3 years after the last point of engagement
- Photography and media consent forms will be retained for 3 years after the last use of the images
- Financial records relating to program payments or donations will be kept for 6 years in line with HMRC requirements

12. USE OF PHOTOGRAPHS

Where practicable, LNK will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website, other websites used by LNK in advertising or in the Newsletter.

13. EXTERNAL DATA RECORDS

1. LNK obtains personal data (such as names, addresses, and phone numbers) from service users. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of services.
2. Personal details supplied are only used to send potentially useful material. Most of this information is stored on the organisation's database.
3. LNK obtains personal data and information from service users in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by service user.

14. CONSENT

1. Personal data is collected over the phone and using other methods such as e-mail. During this initial contact, the data owner is informed as to how this information will be used.
2. Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

15. PERSONAL DATA

1. Personal data will not be passed on to anyone outside the organisation, without explicit consent from the data owner, unless there is a legal duty of disclosure under other legislation, in which case the member of staff will discuss and agree disclosure with the Chairperson.
2. Contact details held on the organisation's database may be made available to groups/ individuals outside of the organisation. Individuals are made aware of this when their details are being collected for the database and their verbal or written consent is requested.

16. ACCESS

1. Only the organisation's staff, volunteers and board members will normally have access to personal data.
2. All staff, volunteers and board members are made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.
3. Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service. Any paperwork that can be stored digitally will be cross cut shredded and uploaded onto our online systems. This includes Sharepoint, Outlook, Microsoft 365 and Upshot.
4. Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies and as required by law. All requests for personal data under GDPR must be submitted in writing, either by email or letter, to LNK's Office Manager. Verbal requests cannot be accepted to ensure proper documentation and verification of the request.
5. Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made. However, this shall be subject to verification of the requesting individual's identity. LNK aims to deal with all requests within 40 days.
6. All confidential post must be opened by the addressee only.
7. Members of staff and committee members will have access to personal data only where it is required as part of their functional remit.
8. A copy of staff, volunteer, advisory board emergency contact details will be kept for Health and Safety purposes to be used in emergency situations.

17. ACCURACY

1. LNK will take reasonable steps to keep personal data up to date and accurate.
2. Personal data will be stored for as long as the data owner/ client/ member/ customer use our services and normally longer. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed. However, unless we are specifically asked by an individual to destroy their details, we will normally keep them on file for future reference.
3. If a request is received from an organisation/ individual to destroy their records, we will remove their details from the database and request that all paper copies held or electronic details for the organisation/individual are destroyed. All requests for personal data under GDPR must be submitted in writing, either by email or letter, to LNK's Office Manager. Verbal requests cannot be accepted to ensure proper documentation and verification of the request.
4. This procedure applies if LNK is informed that an organisation ceases to exist.

18. DISCLOSURE AND BARRING SERVICE

1. LNK will act in accordance with the DBS's code of practice.
2. Copies of disclosures are kept for no longer than is required. In most cases this is no longer than 12 months in accordance with the DBS Code of Practice. There may be circumstances where it is deemed appropriate to exceed this limit e.g. in the case of disputes.

19. RESPONSIBILITIES OF STAFF, VOLUNTEERS AND BOARD MEMBERS

1. During their duties with LNK, members, staff (including contract staff), volunteers and board members will be dealing with information such as names/addresses/phone numbers/e-mail addresses of members/clients/customers/volunteers.
2. They may be told or overhear sensitive information while working for LNK. The Data Protection Act (1988) gives specific guidance on how this information should be dealt with.
3. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.
4. Staff paid or unpaid voluntary must abide by this policy.
5. To help staff, volunteers, board members meet the terms of the Data Protection Act, a Data Protection/Confidentiality statement has been produced.
6. Staff, volunteers and participating board members are asked to read and sign this statement to say that they have understood their responsibilities as part of the induction programme.

20. COMPLIANCE

1. Compliance with the Act is the responsibility of all staff (including contract staff), paid or volunteers.
2. LNK will regard any unlawful breach of any provision of the Act by any staff, paid or voluntary, as a serious matter which will result in disciplinary action.
3. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure, which may result in dismissal or exclusion for gross misconduct.
4. Any such breach could also lead to criminal prosecution.
5. Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the Board Of Trustees

21. SECURITY

- 1.Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.
- 2.Staff will report any actual, near miss, or suspected data breaches to the LNK CEO or The Board Of Trustees for investigation. Lessons learned during the investigation of breaches will be relayed to those processing information to enable necessary improvements to be made.
- 3.Any unauthorised use of corporate email by staff, including sending of sensitive or personal data to unauthorised persons, or use that brings LNK into disrepute will be regarded as a breach of this policy.
- 4.Staff will use appropriate protective markings to protect and secure any document containing personal information. Thus, informing recipients of the document of the measures that need to be employed for its appropriate handling.
- 5.Regular security training and awareness programs will be conducted to ensure all staff understand and can implement best practices in data protection, confidentiality, and information security.

22. RETENTION OF DATA

- 1.No documents will be stored for longer than is necessary and as required for the specified project.
- 2.All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.
- 3.Participant records (including personal information, consent forms, and attendance data) will be retained for 3 years after the last point of engagement with LNK's services
- 4.Safeguarding records must be kept for 6 years after the last point of contact
- 5.Medical information and accident reports will be retained for 3 years after the last point of engagement
- 6.Photography and media consent forms will be retained for 3 years after the last use of the images

23. POLICY COMMUNICATION

- 1.This policy will be made available to all staff members employed by LNK as a record and stored within the LNK server.
- 2.The LNK Policy Coordinator can be contacted via the email address info@livesnotknives.org for additional information on this policy.

24. POLICY REVISIONS

This Data protection policy will be reviewed annually by our Data Protection Policy Trustees to ensure it remains up-to-date and effectively addresses safeguarding risks. This policy may also be reviewed in the interim period as required following a serious incident, to cover any amendments to operating practices or policies, and/or changes in legislation, etc.

LNK are committed to reviewing and updating our Data protection policy annually, which will be done by our Board of Trustees. Any recommended updates or revisions to the policy resulting from the annual review or post-incident review will be formally approved by our Board of Trustees before being implemented.

All staff, volunteers, and The Board of Trustees will be notified of any changes to this Data Protection policy within two weeks of its occurrence and will receive updated training as necessary on the revised policy and procedures.

Version	Revision date	Summary of changes	Actioned by
1.0	October 2024	Changed the structure of the policy. Added information with the ICO. Defined what ICO is. Added the policy revision. Added introduction to outline what this policy will be on. Section 21 – Security.	C. Clements
2.0	January 2025	Point 11 - Storage. Added and included what platforms LNK use to store, handle and manage data. Added how long data is store for Children and Young people. Point 16 -Requesting for access to Data needs to be in writing. Point 23 - Added how long data is store for children and young people.	C. Clements Charandeep Kaur Khaira