



LIVING ON BEREAVEMENT SERVICE

GDPR and Data Protection Policy

Created by: CEO October 2026

To be reviewed: every 2 years (2028)



Content

1. Purpose and scope
2. Data protection responsibilities
3. Definitions
4. Data protection principles
5. Lawful basis for processing
6. Special category data
7. Children's personal data
8. Individual rights
9. Data storage and security
10. Personal data breaches
11. Personal data relating to families
12. Subject Access Requests
13. Personal data relating to staff, volunteers and trustees
14. Personal data relating to supporters and donors
15. Staff and volunteer responsibilities
16. Confidentiality and supervision
17. Website and online information
18. Data sharing and third parties
19. Data retention and disposal
20. Related policies and procedures
21. Use of Artificial Intelligence (AI)
22. Glossary



OUR COMMITMENT

Living On Bereavement Service is committed to protecting the personal information entrusted to us by children, young people, families, employees, volunteers, trustees, supporters and other people who work with or contact the charity.

We recognise that Living On handles particularly sensitive information because of the nature of our work with bereaved children, young people and families.

We will collect, use, store and share personal information lawfully, fairly and transparently, and will take appropriate steps to keep information secure.

Living On will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data-protection requirements.

1. PURPOSE AND SCOPE

Living On Bereavement Service is a registered charity supporting children and young people who are bereaved.

This policy explains how Living On manages personal data and the responsibilities of everyone working on behalf of the organisation.

It applies to:

- employees;
- sessional workers;
- Family Support Workers;
- therapists and practitioners;
- volunteers;
- trustees;
- students and placement workers;
- contractors and other people processing information on behalf of Living On.

The policy covers personal information relating to:

- children and young people;
- parents and carers;
- families;
- employees;
- volunteers;
- trustees;



- applicants;
- supporters and donors;
- professionals and organisations who work with Living On.

Everyone working for or on behalf of Living On is responsible for following this policy.

Failure to comply with this policy may result in appropriate action under Living On's employment, volunteer or disciplinary procedures.

2. DATA PROTECTION RESPONSIBILITIES

Board of Trustees

The Board of Trustees has overall responsibility for ensuring that Living On has appropriate arrangements for data protection and information security.

The Board will:

- approve and review this policy;
- ensure appropriate resources and arrangements are in place;
- oversee significant data-protection risks;
- ensure serious breaches or concerns are appropriately addressed.

CEO / Data Protection Lead

Living On will designate an appropriate person to oversee day-to-day data-protection matters.

The Data Protection Lead will:

- provide advice to staff and volunteers;
- oversee data-protection procedures;
- coordinate responses to data breaches;
- coordinate Subject Access Requests and other data-rights requests;
- maintain appropriate records;
- ensure relevant privacy information is kept under review;
- escalate significant concerns to the Board.

The named individual should be recorded separately in Living On's governance records so that the policy does not become out of date when roles change.



Employees and volunteers

All employees and volunteers must:

- understand and follow this policy;
- keep personal information secure;
- only access information they need for their role;
- only share information where there is a lawful and appropriate reason;
- report data breaches or concerns immediately;
- complete required data-protection and cyber-security training.

3. DEFINITIONS

Personal data

Personal data is information relating to an identified or identifiable living person.

This may include:

- names;
- addresses;
- telephone numbers;
- email addresses;
- dates of birth;
- photographs;
- emergency contact details;
- school information;
- clinical or session information;
- employment information;
- financial information;
- online identifiers.

Special category data

Special category data is particularly sensitive personal data which receives additional protection under the UK GDPR.

This includes information relating to:

- racial or ethnic origin;



- religious or philosophical beliefs;
- health;
- sex life;
- sexual orientation;
- political opinions;
- trade union membership;
- genetic data;
- biometric data used for identification.

Living On may process special category information where this is necessary for the delivery of our services, safeguarding, employment or another lawful purpose.

Data subject

A data subject is the individual whom the personal data relates to.

Processing

Processing means anything Living On does with personal data, including collecting, recording, storing, accessing, using, sharing, changing or deleting it.

Data controller

Living On Bereavement Service is the **data controller** for the personal data it determines how and why to process.

Data processor

A data processor is an organisation that processes personal data on behalf of Living On under the instructions of Living On.

Examples may include certain external IT, payroll, database or other service providers.

Where Living On uses a data processor, appropriate contractual and security arrangements must be in place.

4. DATA PROTECTION PRINCIPLES

Living On will comply with the seven UK GDPR data-protection principles:

1. Lawfulness, fairness and transparency

Personal data will be processed lawfully, fairly and transparently.

2. Purpose limitation

Personal data will only be collected and used for specified, explicit and legitimate purposes.

3. Data minimisation

Living On will only collect and use information that is adequate, relevant and necessary for the purpose.



4. Accuracy

Personal information will be kept accurate and, where necessary, up to date.

5. Storage limitation

Personal information will not be retained for longer than necessary.

Living On's retention arrangements will set out how long different categories of information should be kept.

6. Integrity and confidentiality

Personal information must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7. Accountability

Living On is responsible for demonstrating compliance with data-protection requirements and will maintain appropriate policies, procedures and records.

5. LAWFUL BASIS FOR PROCESSING

Living On must have a lawful basis whenever it collects, uses or shares personal data.

The six lawful bases under the UK GDPR are:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

The appropriate lawful basis will depend on the purpose for which the information is being processed.

Living On will identify and document the appropriate lawful basis where required.

Consent

Where Living On relies on consent, consent must be:

- freely given;
- specific;
- informed;
- clearly indicated by a positive action;
- capable of being withdrawn.

Consent will not be used where another lawful basis is more appropriate.



Withdrawal of consent will not necessarily require Living On to delete information where another lawful basis permits continued processing.

6. SPECIAL CATEGORY DATA

Living On handles special category information, including health information, because of the nature of our bereavement support.

Special category data requires:

1. an appropriate lawful basis under Article 6 of the UK GDPR; and
2. an additional condition for processing under Article 9.

Living On will only collect and use special category data where it is necessary and appropriate and will take additional care to keep it secure.

Where required, Living On will consider whether a Data Protection Impact Assessment (DPIA) is necessary.

The ICO confirms that special category data requires both an Article 6 lawful basis and an Article 9 condition.

7. CHILDREN'S PERSONAL DATA

Living On recognises that children and young people require particular care and protection when their personal information is processed.

We will:

- collect only information that is necessary;
- explain, in an age-appropriate way where appropriate, how information is used;
- consider the child's age, understanding and circumstances;
- protect children's confidentiality while complying with safeguarding responsibilities;
- take additional care when processing sensitive information about children;
- consider the child's rights and best interests when making decisions about their information.

Where information is shared with parents, carers, schools or other professionals, Living On will consider confidentiality, consent, safeguarding and the legal basis for sharing.

8. INDIVIDUAL RIGHTS

People have rights regarding their personal information.

These include, subject to legal exemptions:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;



- the right to restrict processing;
- the right to object;
- rights relating to data portability in certain circumstances;
- rights relating to automated decision-making and profiling where applicable.

Living On will respond to requests within the timescales required by data-protection law.

9. DATA STORAGE AND SECURITY

Living On will take appropriate technical and organisational measures to protect personal data.

This includes:

- storing paper records securely;
- using password-protected systems;
- using strong passwords;
- using multi-factor authentication where available and appropriate;
- keeping software and security measures appropriately maintained;
- restricting access to people who need the information for their role;
- securing mobile phones and devices with screen locks;
- not leaving confidential information unattended;
- using secure methods of communication;
- securely disposing of confidential paper records;
- securely disposing of or wiping electronic equipment before disposal;
- taking additional care when working away from Living On premises or from home.

Staff and volunteers must not:

- share passwords;
- leave confidential records unattended;
- use personal devices or accounts to store Living On information unless authorised;
- send personal information to an incorrect recipient;
- access information they do not need for their role.



10. PERSONAL DATA BREACHES

A personal data breach may occur where personal information is:

- lost;
- stolen;
- accidentally destroyed;
- accidentally disclosed;
- accessed without authorisation;
- sent to the wrong person;
- altered without authorisation;
- otherwise compromised.

Examples could include:

- sending an email containing personal information to the wrong recipient;
- losing a work mobile phone;
- leaving a confidential file in a public place;
- someone accessing information they are not authorised to access;
- a cyber-attack.

Reporting a breach

Any suspected or actual data breach must be reported **immediately** to the Living On Trustees, or CEO.

Staff and volunteers should not attempt to conceal or resolve a suspected breach themselves.

Living On will:

1. contain the breach where possible;
2. establish what information has been affected;
3. assess the potential risk to individuals;
4. record the incident;
5. take steps to prevent further harm;
6. determine whether the breach must be reported to the ICO;
7. determine whether affected individuals need to be informed;
8. review whether any changes to procedures or training are required.



Where a breach is reportable to the ICO, it will normally need to be reported without undue delay and, where feasible, within 72 hours of becoming aware of it.

Not every personal data breach is required to be reported to the ICO. The reporting decision will be based on the level of risk to individuals.

11. PERSONAL DATA RELATING TO FAMILIES

Living On holds personal information about children, young people and families so that we can provide safe, appropriate and professional bereavement support.

Information may include:

- names and addresses;
- telephone numbers and email addresses;
- emergency contact details;
- school information;
- GP or other professional contact details where relevant;
- relevant health information;
- referral information;
- clinical/session notes;
- supervision or consultation information where relevant;
- artwork or other materials created as part of support;
- relevant correspondence;
- photographs where appropriate consent or another lawful basis has been established.

Living On will only collect and retain information that is necessary for the purposes for which it is processed.

Information may be shared with relevant professionals or organisations where there is a lawful and appropriate reason to do so, including where necessary for safeguarding.

12. SUBJECT ACCESS REQUESTS

Individuals generally have the right to request access to personal information Living On holds about them.

A Subject Access Request (SAR) should be made in writing where possible.

Requests should be passed promptly to the Living On Data Protection Lead.

Living On will:

- verify the identity of the requester where necessary;
- identify relevant information;
- consider applicable exemptions;



- protect the confidentiality of other people;
- respond within the statutory timescale.

Where a request involves information relating to another person, Living On will consider whether that information can lawfully be disclosed.

13. PERSONAL DATA RELATING TO STAFF, VOLUNTEERS AND TRUSTEES

Living On holds personal information about employees, volunteers and trustees for legitimate organisational purposes.

This may include:

- recruitment information;
- application and interview information;
- references;
- right-to-work information;
- DBS information where relevant;
- contact details;
- emergency contact information;
- payroll and pension information;
- qualifications and professional experience;
- supervision and performance information;
- holiday and absence information;
- relevant health information;
- disciplinary or grievance information where applicable.

Access will be restricted to those who need the information for legitimate organisational purposes.

Living On will provide appropriate privacy information to staff, volunteers and trustees explaining how their information is used.

14. RECRUITMENT INFORMATION

Living On will only collect information from job applicants that is relevant to the recruitment process or required by law.

Recruitment information will:

- be accessed only by people involved in the recruitment process;
- be stored securely;



- not be retained for longer than necessary;
- be disposed of securely when no longer required.

Where recruitment information is retained for longer than the normal recruitment period, there should be a clear reason for doing so.

Special category information used for equality monitoring should be separated from recruitment decision-making wherever practicable.

15. PERSONAL DATA RELATING TO SUPPORTERS AND DONORS

Living On may process supporter and donor information for purposes including:

- processing donations;
- Gift Aid administration;
- maintaining financial and accounting records;
- fundraising;
- communicating with supporters;
- promoting Living On activities and events;
- administering fundraising events;
- meeting legal and regulatory obligations.

Marketing communications will be managed in accordance with applicable data-protection and electronic communications requirements.

16. STAFF AND VOLUNTEER RESPONSIBILITIES

Everyone working for or on behalf of Living On must:

- keep personal data confidential;
- only access information required for their role;
- ensure information they record is accurate and relevant;
- avoid unnecessary or excessive personal information;
- avoid recording speculation or inappropriate personal opinions;
- only share information where there is a lawful and appropriate reason;
- keep paper and electronic records secure;
- use appropriate passwords and security measures;
- report suspected breaches immediately;
- complete required data-protection and cyber-security training.



Personal information must not be shared outside Living On unless there is an appropriate lawful basis and the sharing is authorised.

Safeguarding responsibilities may require information to be shared without consent where there is a lawful basis to do so.

17. CONFIDENTIALITY AND SUPERVISION

Confidentiality is an important part of Living On's work.

Information discussed during clinical supervision, management supervision and team discussions should be treated confidentially.

However, confidentiality is not absolute.

Information may need to be shared where:

- there is a safeguarding concern;
- there is a serious risk of harm;
- there is a legal requirement;
- disclosure is otherwise necessary and lawful;
- information is required for appropriate clinical or organisational governance.

Where possible, the limits of confidentiality should be explained at the beginning of a professional relationship.

18. WEBSITE AND ONLINE INFORMATION

Living On will provide appropriate privacy information to people who submit information through its website or other online services.

Website forms and other online services will only collect information that is necessary for the stated purpose.

The current Living On Privacy Notice should be used alongside this policy and kept under review.

19. DATA SHARING AND THIRD PARTIES

Living On may need to share personal information with external organisations, including:

- schools;
- health professionals;
- social care or safeguarding services;
- professional supervisors;
- funders where appropriate and lawful;
- payroll providers;
- IT and software providers;
- insurers;



- auditors;
- statutory or regulatory bodies.

Information will only be shared where there is a lawful and appropriate reason.

Where an external organisation processes personal data on behalf of Living On, appropriate arrangements should be in place to protect that information.

20. DATA RETENTION AND DISPOSAL

Living On will not retain personal information indefinitely.

Information will be retained in accordance with the Living On **Data Retention Schedule** and applicable legal, regulatory and professional requirements.

When information is no longer required, it will be securely deleted, destroyed or anonymised as appropriate.

Paper records containing personal information must be securely shredded or disposed of as confidential waste.

Electronic devices and storage media containing personal information must be securely wiped or otherwise disposed of in accordance with appropriate security arrangements.

21. Use of Artificial Intelligence (AI)

Living On recognises that artificial intelligence (AI) tools can support administrative, communication, research and other organisational tasks. However, the use of AI must comply with UK data protection legislation, confidentiality requirements, safeguarding responsibilities and Living On's professional and ethical standards.

Personal and Confidential Information

Staff, volunteers, trustees and other representatives of Living On must not enter personal, confidential or sensitive information about children, young people, families, staff, volunteers or other individuals into publicly available AI tools unless the use of that specific tool has been approved by Living On and appropriate data protection safeguards are in place.

This includes, but is not limited to:

- names and contact details;
- dates of birth;
- addresses;
- school information;
- identifying information about children or families;
- clinical or therapeutic information;
- safeguarding information;
- information about bereavement circumstances;
- medical or mental health information;
- case notes, assessments or referral information;



- photographs or recordings;
- information that could identify an individual when combined with other information.

Removing a person's name does not necessarily make information anonymous. Staff should consider whether an individual could still be identified from the information provided.

Approved Uses of AI

AI may be used for appropriate low-risk activities, such as:

- drafting general communications;
- generating ideas or outlines;
- creating generic resources;
- proofreading or improving wording;
- summarising non-confidential information;
- administrative or organisational tasks where no personal data is entered.

Where AI is used to assist with work involving children, young people or families, staff must ensure that identifiable personal or clinical information is not included unless the tool and use have been specifically approved by Living On.

Accuracy and Professional Responsibility

AI-generated information must be treated as a tool to assist staff and not as a substitute for professional judgement.

Staff remain responsible for checking information produced by AI before using or sharing it. Particular care must be taken where information relates to:

- safeguarding;
- clinical or therapeutic work;
- legal or regulatory requirements;
- health or wellbeing;
- advice given to children, young people or families.

AI can produce inaccurate, incomplete or inappropriate information and should therefore not be relied upon without appropriate human review.

Confidentiality and Security

Staff must not upload Living On documents, case records, clinical notes, referral information, safeguarding records or other confidential material to an AI service unless the service has been approved by Living On for that purpose.

Where an AI tool is approved, its use must be consistent with Living On's data protection, confidentiality, information security and retention requirements.

Passwords, access credentials and other security information must never be entered into an AI tool.



AI-Generated Content

Where AI has been used to assist in creating material for Living On, the person using the tool remains responsible for ensuring that the final material is:

- accurate;
- appropriate;
- inclusive and non-discriminatory;
- consistent with Living On's values and policies;
- suitable for the intended audience; and
- free from confidential or inappropriate personal information.

AI should not be used to make significant decisions about an individual, including decisions concerning safeguarding, employment, access to services or clinical care, without appropriate human assessment and oversight.

Reporting Concerns or Data Breaches

If personal or confidential information is accidentally entered into an AI tool, or if a member of staff or volunteer is unsure whether information can safely be used with an AI tool, they must report this to their manager or the person responsible for data protection as soon as possible.

The incident should be managed in accordance with Living On's Data Breach and Information Security procedures.

Review

As the use and regulation of AI develops, Living On will review its approach to AI regularly and update this policy and associated guidance where necessary.

GLOSSARY

UK GDPR

The UK General Data Protection Regulation is the main framework governing the processing of personal data in the UK.

Data Protection Act 2018

UK legislation that sits alongside and supplements the UK GDPR.

Personal data

Information relating to an identified or identifiable living individual.

Special category data

Particularly sensitive personal data which receives additional protection under data-protection law.

Data controller

The organisation that determines why and how personal data is processed. Living On is a data controller.



Data processor

An organisation that processes personal data on behalf of a data controller.

Personal data breach

A breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Subject Access Request

A request from an individual to access personal information held about them.

Data Protection Impact Assessment (DPIA)

A process used to identify and minimise data-protection risks associated with processing that is likely to result in a high risk to individuals.

TRUSTEE APPROVAL RECORD

- **Approved by:** Board of Trustees and CEO
- **Date approved:** __14.10.2026_____
- **Trustee initials :** __LC_____
- **Next review:** September 2028