



Information Security and AI Governance Policy

Protecting confidentiality, integrity and trust while using secure digital systems and responsibly governed AI-assisted tools.

LILYANNE'S WELLBEING POLICY

PRIVACY • SECURITY • ACCOUNTABILITY • MEANINGFUL HUMAN OVERSIGHT

Live policy

Effective September 2026 • Review by September 2027

Document control

Document owner	Board of Trustees / Information Governance Lead
Applies to	Trustees, staff, counsellors, volunteers, students, contractors, suppliers and approved system users
Status	Live
Version	2.0 - effective September 2026
Effective date	September 2026
Next review	September 2027, or sooner if required

This is a live LilyAnne's Wellbeing policy. It applies from September 2026 and should be read alongside the related policies and procedures identified in this document.

Purpose and scope

This policy governs information security, personal data and AI-assisted tools used for LilyAnne's work. It applies to paper records, devices, email, cloud services, client systems, websites, messaging, backups and any AI feature that processes or generates organisational content.

Governance and responsibilities

Trustees remain accountable for risk and compliance. An appointed Information Governance Lead maintains the asset register, access model, incident process, supplier checks, retention schedule and training. Every user must protect information and report concerns immediately.

Data protection principles

Personal data must be processed lawfully, fairly and transparently; collected for specified purposes; limited to what is necessary; accurate; retained only as required; and protected by appropriate security. Accountability evidence must be maintained.

- Identify and document an Article 6 lawful basis before processing personal data.
- Identify an Article 9 condition before processing health or other special-category data.
- Provide clear privacy information and support data-subject rights.
- Complete a data protection impact assessment where processing is likely to create high risk.

Access control and identity

Access is granted by role and least privilege, approved by an authorised manager and removed promptly when roles end or change.

- Use unique accounts, strong passwords and multi-factor authentication where available.
- Never share passwords or authentication codes.
- Review privileged and client-record access at least quarterly.
- Lock screens and prevent unauthorised viewing in shared or public areas.

Devices, systems and communications

Only approved, supported and appropriately secured systems may hold charity information.

- Apply security updates promptly and use malware protection where appropriate.
- Encrypt portable devices and backups containing personal data.
- Verify recipients before sending information and use secure sharing for sensitive records.
- Do not forward charity information to personal email or store it in personal cloud accounts.
- Keep work and personal profiles separate where bring-your-own-device use is authorised.

Records, retention and disposal

Records are retained under an approved schedule that reflects legal, safeguarding, clinical, insurance and operational needs. Disposal must be secure and recorded for sensitive material. Legal holds, complaints or safeguarding needs may suspend ordinary deletion.

Security incidents and personal data breaches

Loss, misdirection, unauthorised access, phishing, malware, accidental disclosure and suspected compromise must be reported immediately. Staff must preserve evidence and must not conceal, investigate independently or contact affected people unless authorised.

- Contain the incident and protect people from further harm.
- Record facts, systems, data, people affected and actions taken.
- Assess confidentiality, integrity, availability and risk to rights and freedoms.
- Notify the ICO without undue delay and, where feasible, within 72 hours when legally required.
- Notify affected people where the legal threshold is met and provide practical protection advice.

Approved use of AI

AI may assist with low-risk drafting, structure, accessibility or administrative work only through approved tools and processes. Outputs are suggestions and must be checked by a competent human before use.

- Use the minimum necessary information and prefer anonymised or synthetic data.
- Check accuracy, bias, tone, confidentiality, copyright and safeguarding implications.
- Record material AI use where it affects a decision, published content or a person's rights.
- Tell people about AI-assisted processing where fairness and transparency require it.

Prohibited AI uses

The following are prohibited unless trustees have approved a documented lawful, ethical and secure exception.

- Entering identifiable client, safeguarding, health, HR or complaint information into public or unapproved AI services.
- Allowing AI to make final clinical, safeguarding, eligibility, disciplinary, recruitment or complaint decisions.
- Using AI to diagnose, assess suicide risk, replace professional judgement or provide unsupervised crisis responses.
- Creating false records, invented citations, misleading evidence or impersonation.
- Training or fine-tuning systems on charity records without explicit governance, lawful basis and risk assessment.

Supplier assurance and change control

Before adoption, systems must be assessed for security, data location, retention, processor terms, sub-processors, deletion, access, incident response, service continuity and exit arrangements. Material changes require reassessment and, where appropriate, a DPIA.

Training, monitoring and review

Users receive induction and refresher training appropriate to their access. Compliance is monitored proportionately, respecting worker privacy. Serious or repeated breaches may lead to access removal, disciplinary action, professional referral or regulatory reporting.

Related documents and references

- Equality Act 2010 - legislation.gov.uk/ukpga/2010/15/contents
- Data Protection Act 2018 and UK GDPR - ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- LilyAnne's Wellbeing Safeguarding Policy and Privacy Notice.
- ICO AI and data protection guidance - ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/
- ICO data protection by design and default - ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/
- NCSC guidance for small charities - ncsc.gov.uk/charity