IT, Data Protection & Cybersecurity Policy

1. Purpose

The purpose of this policy is to protect Lovemore Project's digital systems, data, and information assets from unauthorised access, misuse, loss, or damage, and to ensure all staff, volunteers, and partners handle information securely.

2. Scope

This policy applies to:

- All Lovemore Project staff, directors, volunteers, contractors, and partners who access or manage organisational information systems.
- All organisational data — whether stored electronically or physically.
- All IT equipment, software, and networks used for Lovemore Project activities.

3. Policy Statement

Lovemore Project will:

- Protect sensitive and personal data in line with the Privacy Policy and applicable laws.
- Ensure secure and reliable IT systems that support our operations.
- Prevent and respond to cyber threats through proactive security measures.
- Ensure data security across borders, including with overseas partners in Italy and Zimbabwe.

4. Data Protection Principles

All personnel must:

- Collect only the minimum personal data necessary for the purpose.
- Store data securely (password-protected, encrypted where appropriate).
- Share personal data only with authorised individuals.
- Dispose of personal data securely when no longer needed.

5. Cybersecurity Standards

- Access Control – User accounts must be unique and password-protected; access granted on a "need-to-know" basis.
- Passwords – Minimum 12 characters, with a mix of letters, numbers, and symbols; changed regularly.
- Encryption – Sensitive data transmitted via secure, encrypted channels (e.g., HTTPS, VPN).
- Device Security – Devices must have antivirus software and automatic updates enabled.
- Backups – Regular backups of critical data stored securely, including offsite/cloud backups.
- Incident Response – Cybersecurity incidents reported immediately to the Executive/Project Coordinator; action taken to contain and investigate.

6. Use of IT Systems

- IT resources provided for organisational purposes must not be used for unlawful or inappropriate activities.
- Email and online communications must follow the Code of Conduct and represent Lovemore Project professionally.
- Social media use on organisational accounts must comply with fundraising and communications standards.

7. Data Sharing with Partners

- Overseas partners must agree to equivalent data protection standards through partnership agreements.
- Data transfers to Zimbabwe or Italy must be encrypted and documented.
- Partners must store and use data only for the agreed project purposes.

8. Training & Awareness

- All staff, volunteers, and board members will receive data protection and cybersecurity awareness training during induction and periodically thereafter.

9. Breach Management

In case of a data breach:

- Contain the breach immediately.
- Assess the scope and impact.
- Notify affected individuals if there is a risk of serious harm.
- Notify the OAIC (and DFAT if donor data is involved) in line with the Notifiable Data Breach scheme.

10. Related Policies

- Privacy Policy
- Code of Conduct
- Risk Management Policy
- Partnership / Partner Due Diligence Policy

10. Review

This policy will be reviewed every three years or sooner if:

- Technology or threat landscapes change significantly.
- Legal or donor requirements change.
- A serious cybersecurity incident occurs.

- Approved by: Board of Directors – Lovemore Project
- Date: 12/09/25
- Next Review: 12/09/28