Wild Embers CIC

Cyber and IT Security Policy

1. Purpose

This policy sets out how Wild Embers CIC protects the information we hold and the technology we use. It ensures compliance with UK GDPR, safeguarding requirements, and Devon County Council's expectations for alternative education providers.

The aims of this policy are to:

- Protect sensitive data relating to children, young people, families, and staff.
- Reduce the risk of cyber threats such as phishing, ransomware, or data loss.
- Provide clear rules for staff and volunteers using IT systems.
- Demonstrate Wild Embers' commitment to safe, secure, and responsible practice.

2. Scope

This policy applies to all Wild Embers staff, volunteers, contractors, and partners who access or use organisational devices, data, or systems.

3. Governance & Responsibilities

- **Information Security Lead (ISL):** Donald Young – responsible for cyber security, IT asset management, and incident reporting.
- **Designated Safeguarding Lead (DSL):** ensures cyber security links with safeguarding responsibilities.
- **All Staff & Volunteers:** must comply with this policy, complete training, and report incidents promptly.

4. IT Asset & Access Control

- An **IT Asset Register** is maintained listing all laptops, phones, and storage devices.
- All devices must be:

    - **Password/Pin protected** with strong passwords (12+ characters, "3 random words" recommended).

        - Set to **lock after 5 minutes** of inactivity.
        -
        - Enabled for **remote wipe** (Find My iPhone/Google Find My Device).
- Access to sensitive data is **restricted by role** and reviewed regularly.
- Shared logins are not permitted.
- Staff leaving the organisation will have all access removed immediately.

5. Acceptable Use of IT & Data

- Devices must only be used for authorised Wild Embers work.
- Personal use of devices is limited and must not compromise security.
- Staff must:
    - Keep passwords secure and never share them.
    - Use work accounts (not personal email) for handling CYP data.
    - Avoid storing sensitive files on local drives or USBs (use secure cloud storage).
    - Only use encrypted and approved USB drives if necessary.
- Staff must not:
    - Download unauthorised software.
    - Use public Wi-Fi for work unless connected via VPN.
    - Access inappropriate or harmful material on work devices.

6. Cyber Security Practices

- **Antivirus:** All laptops must run up-to-date antivirus (Microsoft Defender).
- **Software Updates:** Automatic updates must be enabled on all devices.
- **Phishing Awareness:** Staff must be vigilant for suspicious emails and links.

- **Two-Factor Authentication (2FA):** Enabled on email, cloud storage, and banking accounts.

7. Data Security & Backups

- CYP records and other sensitive data must be stored on **secure, UK/EU-based cloud storage**.
- Weekly **encrypted backups** are taken and stored separately.
- Data retention follows Wild Embers' Data Protection Policy.

8. Incident Management & Data Breaches

- **All incidents** (lost/stolen devices, suspicious emails, data errors) must be reported immediately to the ISL/DSL.
- The ISL will:
    1. Contain and assess the breach.
    2. Record it in the Incident Log.
    3. Notify the ICO within 72 hours if required.
    4. Inform affected families/commissioners using a clear notification template.
- Lessons learned will be reviewed and procedures updated.

9. Training & Awareness

- All staff receive induction training in cyber security, device security, and GDPR.
- Annual refresher training is mandatory.
- Updates from NCSC and Devon County Council are cascaded to staff.

10. Monitoring & Review

- Compliance checks (encryption, updates, access reviews) are carried out **termly** by the ISL.
- This policy will be reviewed annually or sooner if there are changes in law, guidance, or organisational needs.

11. Policy Approval

Approved by: Richard Scofield Director, Wild Embers CIC
Date: 16.09.25