EMPOWERING FUTURES ALTERNATIVE PROVISION

CYBER SECURITY POLICY

Issue Date: December 2025
Next Review: December 2026
Approved by: Director, Empowering Futures Alternative Provision

1. POLICY STATEMENT

Empowering Futures Alternative Provision (EFAP) is committed to maintaining the highest standards of cyber security to protect:

- Learners (children, young people and adults)
- Staff and contractors
- Sensitive and personal data
- Educational resources and systems
- Online learning platforms
- Operational continuity

This policy ensures compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- KCSIE 2024/25
- Cyber Essentials and government cyber security principles
- National Cyber Security Centre (NCSC) guidance
- Prevent Duty 2015
- LA commissioning requirements
- Awarding body requirements for online assessment and digital evidence

Cyber security is integral to safeguarding, data protection, online safety, and business continuity.

2. SCOPE

This policy applies to:

- All staff, tutors, assessors, managers, directors
- Volunteers, contractors, external tutors, agency staff
- Learners (children, young people, adult learners)
- Visitors using EFAP systems
- Any person accessing EFAP digital systems, platforms or data

It covers:

- Computers, laptops, tablets, mobile devices
- Cloud platforms
- Virtual Learning Environments (VLE)
- Remote learning platforms (Teams, Zoom, Google Classroom, etc.)
- Email and messaging systems
- Social media accounts
- Wi-Fi networks
- Assessment systems and e-portfolios

---

3. OBJECTIVES

EFAP aims to:

1. Protect all digital information from unauthorised access, alteration, or destruction.

2. Ensure secure delivery of online education and remote learning.

3. Prevent cyber attacks, malicious activity, and data breaches.

4. Ensure all staff understand cyber security responsibilities.

5. Comply with LA and awarding body digital safety standards.

6. Maintain learner and staff safety in online environments.

7. Protect systems essential to EFAP’s operation.

---

4. ROLES & RESPONSIBILITIES

Director (Lead DSL)

- Holds overall accountability for cyber security.
- Ensures policy compliance and incident response oversight.

Data Protection Lead / IT Lead

- Ensures cyber security measures are implemented.
- Oversees system access controls.
- Maintains secure data storage solutions.
- Liaises with external IT/security suppliers.

DSL / Safeguarding Team

- Ensures cyber security links to online safety and safeguarding.
- Leads on incidents involving learner harm or malicious online behaviour.

Staff, Tutors and Assessors

Must:

- Follow cyber security protocols without exception.
- Report suspicious activity immediately.
- Use only approved devices and systems.
- Protect logins and sensitive data.

Learners (Children, Young People and Adults)

Must:

- Use EFAP digital platforms responsibly.
- Follow online behaviour guidance.
- Report cyber bullying, hacking attempts or suspicious activity.

---

5. SYSTEM & DEVICE SECURITY

5.1 Authorised Devices

Only EFAP-approved devices may access EFAP systems.
Personal devices may be used only where explicitly authorised.

5.2 Password Management

Staff must:

- Use strong passwords (minimum 12 characters)
- Never share passwords
- Change passwords annually
- Use multi-factor authentication where available

5.3 Software & Updates

- Automatic updates must be enabled
- Unapproved software installation is prohibited
- Antivirus software must be active on all devices

5.4 Wi-Fi Security

- EFAP Wi-Fi uses strong encryption
- Guest access, if provided, is restricted and monitored
- Learners may only use approved networks

---

6. DATA SECURITY, STORAGE & ACCESS

EFAP follows UK GDPR and Data Protection Policy requirements.

6.1 Access Levels

Access is granted by role, not convenience.
Sensitive data is restricted and logged.

6.2 Data Storage

- Cloud data stored in secure, encrypted systems
- Personal data never saved on USB drives without encryption
- Portable devices must use password protection

6.3 Data Transmission

- Personal data only sent through secure channels
- Encryption used for sensitive documents
- No data shared through personal email or messaging apps

6.4 Third-Party Platforms

EFAP ensures all third-party systems are:

- GDPR-compliant
- Secure
- Approved by senior leadership

---

7. ONLINE TEACHING & REMOTE LEARNING SECURITY

EFAP uses safe, monitored online platforms for:

- Alternative Provision
- Adult learning programmes
- Assessments
- Tutorials and wellbeing check-ins

7.1 Secure Platform Use

- Only approved platforms may be used (Teams, Zoom, etc.)
- Meeting links must not be publicly shared
- Waiting rooms enabled for admission control

7.2 Learner Verification

- Learners must use their real names
- Cameras on when required (with adjustments for SEND)

7.3 Recording Controls

- Sessions recorded only with permission
- Recordings stored securely
- Learners must not record sessions

7.4 Tutor Controls

Tutors must:

- Lock sessions when all learners are present
- Remove disruptive participants
- Report safeguarding concerns immediately

---

8. CYBER BULLYING & ONLINE SAFEGUARDING

Cyber incidents include:

- Harassment
- Impersonation
- Hacking or password theft

- Sharing explicit or harmful content
- Online grooming
- Extremist messaging
- Fraud or phishing

These are handled under:

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Prevent Duty

DSL must be notified immediately.

---

9. PREVENT DUTY & CYBER EXTREMISM

EFAP monitors for:

- Radicalisation recruitment
- Extremist online content
- Hate-based online messaging

Staff must report:

- Concerning online behaviour
- Extremist materials
- Attempts to access harmful content

Prevent referrals are made by the DSL.

---

10. PHISHING, MALWARE & CYBER ATTACKS

All staff and learners must be aware of risks including:

- Phishing emails
- Ransomware
- Fake links

- Fake websites
- Malicious downloads

Security measures:

- Annual cyber awareness training
- Email filtering
- IT monitoring
- Secure backups
- Never opening unexpected attachments

---

11. REPORTING CYBER SECURITY INCIDENTS

Incidents must be reported immediately to:

1. IT / Data Protection Lead

and

2. DSL (if safeguarding is involved)

Incidents include:

- Data breaches
- Hacking attempts
- Lost or stolen devices
- Unauthorised system access
- Malware infection
- Compromised passwords
- Cyber bullying
- Online exploitation

A formal incident log will be completed, including:

- What happened
- Who was affected
- Systems involved
- Impact assessment
- Containment actions
- Notifications (ICO, LA, awarding body if required)

---

12. BUSINESS CONTINUITY & RECOVERY

EFAP ensures:

- Encrypted backups of critical data
- Routine system testing
- Clear incident response plans
- Secure restoration procedures

In major attacks, EFAP will:

- Follow cyber incident playbook
- Notify affected parties
- Work with LA Digital Teams if relevant
- Notify awarding bodies if assessments are affected
- Notify ICO if a breach meets legal thresholds

---

13. TRAINING & AWARENESS

Annual training is mandatory for:

- Staff
- Tutors
- Assessors
- Volunteers
- Contractors
- Leadership

Training includes:

- Cyber security basics
- GDPR
- Safe online teaching
- Phishing and fraud
- Safeguarding online behaviours
- Protecting assessment data

Learners receive:

- Online safety guidance
- Digital citizenship education
- Cyber bullying awareness

---

14. COMPLIANCE WITH AWARDING BODIES

Awarding bodies require secure handling of:

- Assessments
- Portfolios
- Examination materials
- Evidence submissions
- EQA communications

EFAP ensures:

- Secure digital storage of learner evidence
- Controlled assessor access
- Safe handling of online assessments
- Authentication of learner work
- Traceable version control

Non-compliance will trigger internal audit and reporting.

---

15. MONITORING & REVIEW

Cyber security is monitored through:

- Regular system checks
- Random compliance audits
- Incident logs
- Staff feedback
- External IT reviews
- LA and awarding body audits

Policy reviewed annually or after a serious incident.

---

16. POLICY REVIEW

This policy will be reviewed:

- Every 12 months
- Following NCSC or legal updates
- After a significant cyber incident
- After awarding-body audits
- After LA feedback

Approved by:
Rhean White – Director & Lead DSL
Empowering Futures Alternative Provision