EMPOWERING FUTURES ALTERNATIVE PROVISION

DATA PROTECTION POLICY

Policy Name	**Data Protection**
Site	**Birmingham**
Version	**1.0**
Approved By	**Director / DSL**
Date Reviewed & Confirmed	**18 January 2026**
Next Review Due	**January 2027**

1. POLICY STATEMENT

Empowering Futures Alternative Provision (EFAP) is committed to protecting the personal data of all learners (children, young people and adults), parents/carers, staff, contractors, partner agencies, visitors and external stakeholders.
We recognise our responsibilities as a **Data Controller** under:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Information Commissioner's Office (ICO) guidance

This policy ensures that personal data is:

- Collected lawfully
- Processed fairly and transparently
- Stored securely
- Used only for legitimate purposes
- Protected from unauthorised access, loss or damage
- Retained for the correct length of time
- Deleted or anonymised securely

Data protection at EFAP directly supports safeguarding, online safety, cyber security, health and safety, quality assurance and compliance with Local Authorities and awarding bodies.

2. SCOPE

This policy applies to:
• All EFAP staff, tutors, assessors, DSLs, managers, volunteers, contractors, freelance tutors and agency staff
• All learners aged 11–18 in Alternative Provision
• All adult learners (18+) in evening/weekend and online programmes
• All online, remote, on-site and off-site delivery
• All vocational training environments (beauty, nails, hair, sports, fitness, customer service)

Personal data includes any information relating to an identified or identifiable individual, including:

• Names
• Contact details
• Date of birth
• Assessment results
• Behavioural records
• Safeguarding information
• Medical information
• Attendance
• Online learning logs
• Portfolio evidence
• Photographs and CCTV (where applicable)

3. DATA CONTROLLER & DATA PROTECTION LEAD

Data Controller:
Empowering Futures Alternative Provision
Director: **Rhean White**

Data Protection Lead (DPL):
Appointed internally to oversee GDPR compliance, reporting and training.

The DPL:

- Oversees data management
- Responds to subject access requests (SARs)
- Ensures secure processing
- Supports incident response
- Works with DSL for safeguarding-linked data

EFAP does **not** use Data Protection Education Ltd or any external DPO service.

4. LAWFUL BASES FOR PROCESSING

EFAP processes data under the following lawful bases:

4.1 Contract

For delivering AP or adult learning services to learners commissioned by LAs, schools, or individuals.

4.2 Legitimate Interests

For:
- Monitoring attendance
- Ensuring safety and security
- Quality assurance
- Behaviour management
- Online learning access
- Awarding body processes

4.3 Legal Obligation

Including:
- Safeguarding (Children Act, KCSIE, Working Together)
- Health and safety reporting (RIDDOR)
- Prevent Duty
- HMRC payroll legislation
- LA reporting duties

4.4 Consent

Used **only** where no other lawful basis applies, such as:
- Use of photographs for marketing
- Optional surveys
- Certain aspects of online platform usage

Consent is:
- Freely given
- Informed
- Revocable at any time

4.5 Vital Interests

For emergencies where a person's life or safety is at risk.

5. HOW EFAP COLLECTS AND USES PERSONAL DATA

Data is collected to:

• Provide Alternative Provision education
• Deliver adult learning qualifications
• Monitor safeguarding and wellbeing
• Support SEND needs
• Assess learner progress
• Comply with LA commissioning requirements
• Meet awarding body standards
• Ensure online safety
• Maintain vocational and physical safety

EFAP uses personal data for:

• Registration and enrolment
• Internal assessment and reporting
• Attendance monitoring and alerts
• Safeguarding referrals
• Risk assessments
• Behaviour and incident logs
• Vocational portfolio creation
• Online platform access
• Communication with parents/carers, professionals and adult learners
• Submitting evidence to awarding bodies
• Internal quality assurance (IQA) and external quality assurance (EQA) • Funding or commissioning audits

EFAP does **not** sell or transfer data for marketing purposes.

6. CHILDREN, YOUNG PEOPLE & ADULT LEARNERS: SPECIFIC DATA HANDLED

6.1 Children & Young People (11–18)

We may process:
- Safeguarding records
- Risk assessments
- EHCP information
- Multi-agency reports
- Behaviour incident data
- Body maps
- Online activity logs

6.2 Adult Learners (18+)

We may process:
- Identification and eligibility documents
- Assessment portfolios
- CPD records
- Contact information
- Payment or funding evidence
- Awarding body information

Adult learners have full GDPR rights to access, rectify or delete personal data (subject to lawful exemptions).

7. SPECIAL CATEGORY DATA

EFAP may process sensitive data including:

- Medical information
- Safeguarding disclosures
- SEND information
- Ethnicity and nationality (for monitoring)
- Criminal offence information (where safeguarding requires it)

This data is processed under:

- Legal obligation
- Vital interests
- Substantial public interest (safeguarding)

Strict access controls apply.

8. DATA SHARING

EFAP shares data only when lawful and necessary.

We may share data with:
• Local Authorities (Safeguarding, SEND, Virtual School, commissioning) • Schools
• Social workers
• CAMHS and NHS professionals
• Police (where required)
• Awarding bodies (NCFE, Focus Awards, ASDAN)
• External quality assurers
• Ofsted (on request)
• Emergency services
• External tutors/contractors (with data processing agreements)

EFAP **does not** share data with third parties for profit.

9. DATA STORAGE & SECURITY

EFAP ensures:

• Password-protected systems
• Encryption of sensitive files
• Restricted user access
• Cloud storage compliance
• No USB storage unless encrypted
• Secure transportation of physical records
• Paper files stored in locked cabinets
• CCTV use conforms to ICO rules (if applicable)

Alignment with EFAP **Cyber Security Policy** is mandatory.

10. ONLINE & REMOTE LEARNING DATA HANDLING

EFAP processes online learning data through approved platforms.

We collect:

• Attendance logs
• Chat logs (if needed for safeguarding)
• Recordings (where authorised)
• Learner submissions
• Engagement monitoring

Online safety, cyber security and privacy protocols are embedded.

Recordings are:

• Stored securely
• Accessed only by authorised staff
• Deleted in line with retention schedule

11. DATA PROCESSING IN VOCATIONAL SETTINGS

Beauty, nails, hair, sport and fitness environments may require:

• Accident logs
• Photos of practical work (for assessment)
• Physical observations
• Portfolio evidence
• Health screening forms (e.g., PAR-Q for fitness courses)

These are stored in secure assessment folders or digital e-portfolio systems.

12. SUBJECT ACCESS REQUESTS (SARs)

Individuals may request:

• Access to their data
• Correction of inaccurate data
• Deletion (where lawful)

• Restriction of processing
• Transfer of data (where applicable)

EFAP will:

• Respond within 30 days
• Verify identity before release
• Redact data relating to third parties
• Inform individuals of any exemptions

SARs involving safeguarding data follow additional checks.

13. DATA BREACHES

A data breach may include:

• Lost or stolen devices
• Unauthorised access
• Accidental disclosure
• Cyber attacks
• Hacking or phishing events
• Loss of physical files

EFAP must:

1. Notify the Data Protection Lead immediately
2. Contain the breach
3. Assess the risk
4. Notify ICO within 72 hours if legally required
5. Inform affected individuals
6. Record the incident
7. Review security procedures

Breaches with safeguarding implications will also be escalated to the **DSL**.

14. RETENTION & DELETION

EFAP uses its own Retention Schedule based on:

• Legal requirements
• LA commissioning standards
• Awarding body requirements
• Safeguarding obligations
• ESFA guidance (for adult provision)

Typical retention periods:
• Safeguarding files – up to 75 years or in line with statutory guidance
• Attendance and behaviour logs – 6 years
• Adult learner portfolios – awarding body requirement (usually 3–5 years)
• Assessment evidence – awarding body minimum retention
• Accident/incident forms – 3–7 years depending on seriousness
• Financial/contractual data – 6 years

All deletion is:

• Secure
• Logged
• Irreversible

15. TRAINING & AWARENESS

All staff receive mandatory GDPR and data protection training covering:

• Safe storage & handling
• Password & cyber security
• Safeguarding-linked data
• Online learning data management
• Portable device use
• Email security (phishing awareness)

Contractors and external tutors must comply with EFAP policies before accessing data.

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

DPIAs are required for:

• New digital systems

• High-risk data processing
• Online monitoring tools
• Changes in safeguarding systems
• New assessment platforms

DPIAs are overseen by the Data Protection Lead and Director.

17. COMPLAINTS ABOUT DATA PROCESSING

Complaints should follow the EFAP **Complaints**

Policy. If unresolved, individuals may escalate to the:

Information Commissioner's Office (ICO)
www.ico.org.uk

18. POLICY REVIEW

This policy will be reviewed:

• Annually
• After data breaches
• After regulatory changes
• When new systems are introduced
• After LA or awarding body audit feedback

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