Data Protection, Information Governance & Records Management Policy

Policy Owner: Bridge 2 Education & Employment
Linked Policies: Health & Safety Policy, Safeguarding & Child Protection Policy, Staff Code of Conduct
Effective Date: June 2026
Review Date: June 2027

Policy statement

Bridge 2 Education & Employment (B2EE) recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated information governance legislation.

The organisation is committed to ensuring that all personal information is collected, processed, stored, shared and destroyed lawfully, fairly, securely and transparently.

B2EE processes personal information relating to pupils, families, staff, contractors, commissioners and partner agencies and recognises its responsibility to protect this information from unauthorised access, loss, disclosure or misuse.

The organisation is registered with the Information Commissioner's Office (ICO) and complies with all applicable data protection legislation.

Purpose

This policy aims to:

- Protect personal information.
- Promote good information governance.

- Ensure legal compliance.
- Safeguard confidential records.
- Define retention and disposal arrangements.
- Ensure secure information sharing.
- Protect children and vulnerable individuals.
- Support commissioning and regulatory requirements.

Information Commissioner's Office (ICO)

Bridge 2 Education & Employment is registered with the Information Commissioner's Office (ICO).

The organisation will:

- Maintain a valid ICO registration.
- Renew registration annually.
- Comply with UK GDPR.
- Comply with the Data Protection Act 2018.
- Cooperate with the ICO where required.

ICO registration details will be maintained within organisational compliance records.

Data Protection Lead

B2EE is not legally required to appoint a statutory Data Protection Officer (DPO).

The organisation has appointed a Data Protection Lead responsible for overseeing:

- Data protection compliance.
- Information governance.
- Information sharing.
- Subject Access Requests.
- Data breach management.
- Records management.

Contact

Email: info@bridge2ee.co.uk

Categories of Information Held

B2EE may process:

Pupil Information

- Names
- Addresses
- Dates of Birth
- Contact details
- EHCPs

- Attendance information
- Progress information
- Behaviour records
- Medical information
- Safeguarding records
- Risk assessments
- Examination information

Parent and Carer Information

- Contact details
- Emergency contacts
- Correspondence

Staff Information

- Recruitment records
- DBS information
- Employment records
- Payroll information
- Training records

Commissioner Information

- Referral documentation
- Placement information
- Funding documentation
- Contractual information

Where Information is Recorded and Stored

Information received from Local Authorities, schools and partner agencies is stored securely within approved electronic systems.

Safeguarding Information

Recorded and maintained on:

CPOMS

This includes:

- Child protection concerns
- Welfare concerns
- Attendance safeguarding concerns
- Missing child incidents
- Professional communications
- Multi-agency records

Educational and Operational Information

Stored securely within:

Microsoft 365

Including:

- EHCPs
- Referral documentation
- Risk assessments
- Attendance records
- Learner reports
- Provision maps
- Placement information

Quality Assurance and Monitoring Information

Maintained through:

- Secure Microsoft Excel spreadsheets
- Secure Microsoft 365 systems
- Internal monitoring systems

Access is restricted to authorised staff only.

Access Permissions

B2EE operates a strict need-to-know approach.

Access is granted according to role and responsibility.

Provision Manager / DSL

Access to:

- Safeguarding records
- CPOMS
- Attendance records
- EHCPs
- Risk assessments

SENCO

Access to:

- EHCPs
- SEND records
- Annual review documentation
- Educational information

Tutors

Access only to information necessary to support pupils safely and effectively.

Director of Operations

Access to strategic and operational information required for governance and safeguarding oversight.

Information Security

The organisation will ensure:

- Password-protected systems.
- Microsoft 365 security controls.
- Role-based access permissions.
- Secure cloud storage.
- Multi-factor authentication where available.
- Secure backup arrangements.
- Device security controls.

Personal information must not be stored on unauthorised devices or personal accounts.

Information Sharing

Information will only be shared where:

- Consent has been obtained; or
- A legal basis exists; or
- Safeguarding concerns require disclosure; or
- Statutory duties require disclosure.

The organisation follows the principle of sharing information:

Lawfully

Proportionately

Securely

On a Need-to-Know Basis

Secure Transfer of Information

B2EE recognises that personal and sensitive information must be transferred securely.

Approved methods include:

- Egress Secure Email
- Secure Local Authority portals
- Secure Microsoft 365 sharing arrangements
- Password-protected encrypted documents
- Secure government-approved systems

Sensitive information must never be transferred using unsecured methods.

Passwords must always be communicated separately.

Handling Guidance

All staff must:

- Maintain confidentiality.
- Follow information sharing procedures.
- Keep records accurate and factual.
- Lock screens when unattended.
- Store paper records securely.
- Report data breaches immediately.
- Follow CPOMS recording expectations.

Staff must only access information required for their role.

Subject Access Requests (SARs)

Individuals have the right to request access to their personal information.

Requests should be submitted to:

info@bridge2ee.co.uk

Requests will be managed in accordance with UK GDPR timescales and requirements.

Data Breaches

Any actual or suspected breach must be reported immediately to the Data Protection Lead.

Examples include:

- Lost devices
- Incorrect email recipients
- Unauthorised access
- Lost paperwork
- Cyber incidents

The organisation will:

- Investigate promptly.
- Assess risk.
- Notify the ICO where required.
- Implement corrective actions.

Records Retention

B2EE follows recognised education sector retention guidance.

Pupil Records

Pupil records will be retained until:

Date of Birth + 25 years

unless legal proceedings, safeguarding requirements or statutory guidance require longer retention.

Safeguarding Records

Safeguarding records will be retained in accordance with safeguarding guidance and transferred securely when appropriate.

Staff Records

Retained in accordance with employment and statutory requirements.

Records Disposal and Destruction

When records reach the end of their retention period they will be securely destroyed.

Electronic Records

Destroyed through:

- Secure deletion processes.
- Permanent removal from systems.
- Destruction of backup copies where appropriate.

Paper Records

Destroyed through:

- Cross-cut shredding.
- Confidential waste disposal services.
- Secure destruction providers.

Certificates of destruction may be retained where appropriate.

Information must never be disposed of through general waste.

Auditing and Monitoring

The organisation will regularly monitor:

- Access permissions.
- Data protection compliance.
- Information sharing practices.
- Data breach incidents.
- Records retention compliance.

Audits may be undertaken annually or following significant incidents.

Training

All staff receive annual training covering:

- Data Protection.
- GDPR.
- Confidentiality.
- Information Sharing.
- Cyber Security.
- Record Keeping.

Training forms part of the B2EE Staff Training and Development meetings.

Monitoring and Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- ICO guidance changes.
- Significant incidents occur.
- Suffolk County Council requirements change.

Policy Approval

Policy Owner: Bridge 2 Education and Employment

Approved by: Director of Operations

Date Approved: June 2026

Next Review Date: June 2027

Appendix 1 – Records Retention Schedule

Record Type	Retention Period	Disposal Method
Pupil Educational Records	Date of Birth + 25 years	Secure electronic deletion / confidential shredding
EHCP Documentation	Date of Birth + 25 years	Secure destruction
Attendance Records	Date of Birth + 25 years	Secure destruction
Behaviour Records	Date of Birth + 25 years	Secure destruction
Safeguarding Records (CPOMS)	Date of Birth + 25 years minimum	Secure destruction in line with safeguarding guidance
Risk Assessments (Pupil Specific)	Date of Birth + 25 years	Secure destruction
Accident Records (Pupils)	DOB + 25 years	Secure destruction
Staff Personnel Files	6 years after employment ends	Secure destruction
DBS Information	6 months after recruitment decision	Secure destruction
Staff Training Records	6 years after employment ends	Secure destruction
Supervision Records	6 years after employment ends	Secure destruction
Complaints Files	6 years after closure	Secure destruction
Data Breach Records	6 years	Secure destruction
Health & Safety Records	3–40 years depending on record type	Secure destruction
Finance Records	6 years plus current financial year	Secure destruction
Contracts and Service Agreements	6 years after termination	Secure destruction

Disposal Procedures

Electronic records will be permanently deleted from systems and storage locations.

Paper records will be destroyed using:

- Cross-cut shredding
- Confidential waste services
- Approved destruction contractors

Records must never be disposed of through general waste.

Appendix 2 – Information Asset Register

Information Asset	Information Held	System Used	Access Permissions	Retention Period
Safeguarding Records	CP concerns, welfare concerns, attendance concerns, multi-agency information	CPOMS	DSL, DDSLs, Director of Operations	DOB + 25 years
Pupil Files	Referral information, EHCPs, reports, attendance, assessments	Microsoft 365	Provision Manager, SENCO, authorised staff	DOB + 25 years
Attendance Tracking	Attendance data and monitoring	Microsoft 365 / Excel	Provision Manager, Tutors	DOB + 25 years
QA Monitoring	Audit information and compliance records	Excel / Microsoft 365	Senior Leadership Team	6 years
Staff Personnel Files	Employment information, training records	Microsoft 365	Director of Operations, authorised managers	6 years after employment
Training Matrix	Workforce compliance information	Excel / Microsoft 365	Provision Manager, Directors	6 years
Financial Records	Invoices, contracts and payments	Secure finance systems	Directors	6 years
Complaints Records	Complaints and investigations	Microsoft 365	Directors	6 years

Security Controls

All information assets are protected through:

- Password-protected accounts
- Role-based permissions
- Microsoft 365 security controls
- Secure backups
- Multi-factor authentication where available
- Regular access reviews

Appendix 3 – Subject Access Request Form

Include:

- Applicant details
- Relationship to data subject
- Information requested
- Identity verification checklist
- Date received
- Response deadline (one month)
- Outcome section

APPENDIX 4 – Information Sharing Flowchart