Brighton Forward
Data Protection Policy

Brighton Forward is committed to reviewing its policies and good practice annually.

Approved by: Laura Vallone
Policy review date: Revised April 2026
Next review date: April 2027

Introduction

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The college collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the College. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the College complies with its statutory obligations.

The College is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The College must be able to demonstrate compliance. Failure to comply with the Principles exposes the College and staff to civil and criminal claims and possible financial penalties.

Aim

This Policy will ensure:

The College processes person data fairly and lawfully and in compliance with the Data Protection Principles.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

That the data protection rights of those involved with the College community are safeguarded.

Confidence in the College's ability to process data fairly and securely.

Scope

This Policy applies to:

Personal data of all College employees, Directors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the College.

The processing of personal data, both in manual form and on computer.

All staff and Directors.

The Data Protection Principles

The College will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The College will be able to demonstrate compliance with these principles.

The College will have in place a process for dealing with the exercise of the following rights by Directors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

Roles and Responsibilities

The Director's of the College is responsible for implementing good data protection practices and procedures within the College and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Directors.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Colleges Complaints Policy.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff sign and will comply with the College Acceptable Use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable Use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Colleges'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

The College will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don’ts in relation to data security in **Appendix A**

Subject Access Requests

Requests for access to personal data (Subject Access Requests - SARs) will be processed by the Data Protection Officer. Records of all requests will be maintained.

The College will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request.

Sharing data with third parties and data processing undertaken on behalf of the College.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the College e.g. by providing cloud-based systems or shredding services, the College will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles.

For commissioned placements, we share necessary information with the home/commissioning school or local authority to fulfil education and safeguarding duties.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read and sign the Acceptable Use Policy as part of their New Starters paperwork.

The College advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the College website.

Photographs, Additional Personal Data and Consents

As part of the College admissions process, parents/carers will be asked for consent on the college application form for processing person data such as photographs. Where consent is not given all staff will be informed.

Notification of Data Breaches to Partner Schools

Brighton Forward recognises the importance of transparency and timely communication in the event of any data security incidents. In cases where personal data relating to students placed by partner schools or data belonging to those schools is involved in a data breach, Brighton Forward will promptly inform the relevant school(s). This notification will include details of the breach, the potential impact, and the steps taken to mitigate any harm. This process ensures that partner schools are fully aware of any risks to their data and can take appropriate action as necessary.
In the event of a personal data breach, Brighton Forward will notify the Information Commissioner's Office (ICO) without undue delay, and where feasible, not later than 72 hours after becoming aware of it.

Appendix A

Do's and Don’ts in relation to data security

What staff should do:

DO get the permission of your manager to take any confidential information home.
DO transport information from college on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
DO ensure that any information on USB memory sticks is securely deleted off the device or saved on a College shared drive.
DO ensure that all paper-based information that is taken off premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper-based information and laptops are kept safe and close to hand when taken off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper-based information to the College as soon as possible and file or dispose of it securely.
DO report any loss of paper-based information or portable computer devices to your line manager immediately.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state Private - Contents for Addressee only'.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to Bromcom (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic usernames such as 'Sysman' are disabled. **DO** ensure that when sending emails to groups of external parties that the Bcc(Blind Carbon Copy) field is used to protect their privacy.

What staff must NOT do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine.

DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT leave documentation in vehicles overnight.
DO NOT discuss case level issues at social events or in public places.
DO NOT put confidential documents in non-confidential recycling bins.
DO NOT print off reports with personal dat a (e.g. student data) unless absolutely necessary.
DO NOT use unencrypted memory sticks or unencrypted laptops.

Appendix B

Brighton Forward – Data Flow Map (SEND Post 16 / KS4 AP)

1. Overview

This data flow map outlines how personal data is collected, processed, stored, shared, and deleted across Brighton Forward provision, including Post-16 SEND and KS4 Alternative Provision.

2. Core Data Types

Data Type	Examples	Sensitivity Level
Personal Data	Name, DOB, address, contact details	Medium
Educational Data	Assessments, PLJs, progress reports	Medium
SEND Data	EHCPs, targets, specialist reports	High
Safeguarding Data	CP concerns, referrals, DSL notes	Very High
Medical Data	Medication, conditions, care plans	High
Behaviour & Attendance	Logs, incidents, travel risk	Medium–High

3. Data Flow Journey

Stage 1: Data Collection

Sources:

- Parents / carers
- Home / commissioning schools
- Local Authorities
- External professionals (CAMHS, social care)
- Internal assessments and observations

Collection Methods:

- Referral forms
- EHCP documentation
- Email / secure transfer
- Baseline assessments
- Daily session observations

Stage 2: Data Input & Processing

Systems Used:

- Earwig → PLJs targets, evidence
- BromCom → attendance, behaviour, contacts, safeguarding
- Secure email systems
- Paper records (limited use)

Processing Activities:

- Setting EHCP-aligned targets
- Recording progress and evidence
- Behaviour and safeguarding logging
- Reporting to stakeholders

Stage 3: Data Access

Who can access data:

- Facilitators (limited to relevant students)
- Leads / Programme Lead
- DSL / DDSL (full safeguarding access)
- Senior Leadership Team
- Data Protection Officer

Controls:

- Role-based access
- Password-protected systems
- Staff training and Acceptable Use agreements

Stage 4: Data Sharing

Internal Sharing:

- Staff team (need-to-know basis)
- DSL for safeguarding

External Sharing:

- Local Authorities
- Home / commissioning schools
- Social care / police (if required)
- Health professionals

Methods:

- Secure email
- System access (where applicable)
- Reports and review meetings

Stage 5: Data Storage & Security

- Encrypted digital systems
- Password-protected access
- Locked cabinets (paper records)

Stage 6: Retention & Disposal

- In line with statutory guidance (IRMS)
- Secure deletion of digital records
- Confidential shredding of paper records
- Regular data audits

4. High-Risk Data Flows (SEND/AP Specific)

- Safeguarding referrals → DSL → external agencies
- Travel training (location, independence, risk assessments)
- Behaviour incidents (including AP reporting to schools)
- EHCP data sharing with Local Authorities
- Off-site learning (community-based data handling)

5. Risks Identified

- Use of personal devices (BYOD)
- Data accessed off-site (community learning)
- Safeguarding information sharing delays
- Human error (emailing wrong recipient)

6. Controls in Place

- BYOD agreement
- Staff training (GDPR & safeguarding)
- DSL-led safeguarding processes
- Secure systems (Earwig, BromCom)
- Clear reporting procedures

DPIA Template (Brighton Forward) -Data Protection Impact Assessment (DPIA)

1. Project / Process Name

(e.g. Earwig implementation / Safeguarding Recording)

2. Description of Processing

- What data is being collected?
- Who is it about? (students, staff, families)
- What is the purpose?

3. Lawful Basis (UK GDPR)

Tick applicable:

☐ Public Task
☐ Legal Obligation
☐ Vital Interests (safeguarding)
☐ Consent (where applicable)

4. Data Types Involved

☐ Personal Data
☐ Special Category Data (SEND, medical)
☐ Safeguarding Data

5. Data Flow Summary

- Where does data come from?
- Where is it stored?
- Who accesses it?
- Who is it shared with?

6. Risk Assessment

Risk	Likelihood	Impact	Mitigation
Data breach (device loss)	Medium	High	Encryption + remote wipe
Unauthorised access	Low	High	Role-based access
Human error (email)	Medium	Medium	Staff training
Off-site data handling	Medium	High	Clear protocols

7. Safeguarding Considerations

- Does this involve vulnerable learners? → YES
- Is safeguarding data processed? → YES
- Are DSL processes in place? → YES

8. Security Measures

- Encryption
- Password protection
- Secure systems (Earwig / BromCom)
- Staff training

9. Data Minimisation

- Only necessary data collected? → YES / NO
- Retention period defined? → YES / NO

10. Residual Risk Level

☐ Low
☐ Medium
☐ High

11. Approval

- **Completed by:** _____
- **Role:** _____
- **Date:** _____
- **Reviewed by (SLT):** _____
- **Date:** _____