

Best Foot Forward - Data Protection Policy

Author	Andrew Russell
Approved By	Bethany Russell
Date Approved	November 2025
Date of Last Update	August 2026
Assigned Review Period	1 Year
Next Review Due	August 2027

Purpose

To ensure that all personal data collected, processed, shared, retained and disposed of by Best Foot Forward is handled lawfully, fairly, transparently and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection legislation. This policy protects the rights, privacy and security of students, parents/carers, staff and other individuals whose information we hold.

This policy also establishes Best Foot Forward's approach to retention and secure disposal. The Data Retention & Disposal Schedule at Appendix A forms part of this policy and must be followed by all staff.

Key Contacts

Name / Role	Best Foot Forward Contact Information
Designated Safeguarding Lead (DSL) Bethany Russell	beth@bestfootforward.org.uk 07394 950803
Deputy Designated Safeguarding Lead(s) Andrew Russell	andrew@bestfootforward.org.uk 07538 719783

BEST FOOT FORWARD collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the service. This information is gathered to enable Best Foot Forward to provide education, mentorship and other associated functions. There may also be legal, safeguarding, contractual or regulatory requirements to collect and use information.

What is personal information?

Personal information (personal data) is information relating to an identified or identifiable living individual. This includes, for example:

Bethany Russell 07394 950803

beth@bestfootforward.org.uk

Andrew Russell 07538 719783

andrew@bestfootforward.org.uk

Website: www.bestfootforward.org.uk | Contact: admin@bestfootforward.org.uk

- Names (including initials)
- Location data (for example, a home address)
- Contact information
- Online identifiers and other information that can identify an individual when combined with information Best Foot Forward holds

Personal data may also include information relating to an individual's physical, physiological, genetic, mental, economic, cultural or social identity. Some information, including health information, racial or ethnic origin, religious or philosophical beliefs, biometric data used for identification and information about a person's sex life or sexual orientation, is special category data and requires additional protection.

Data Protection Principles

Under the UK GDPR, Best Foot Forward must ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in an identifiable form for no longer than is necessary;
- processed in a way that ensures appropriate security; and
- handled in a way that enables Best Foot Forward to demonstrate compliance with these principles.

This policy, together with Appendix A, sets out how Best Foot Forward will apply these principles in practice.

Collecting Personal Information

Best Foot Forward will identify and document an appropriate lawful basis before processing personal data. The six lawful bases under Article 6 of the UK GDPR are:

- contract - processing is necessary for a contract with the individual or to take requested steps before entering into a contract;
- legal obligation - processing is necessary to comply with the law;
- vital interests - processing is necessary to protect someone's life;
- public task - processing is necessary to perform a task in the public interest or exercise official authority, where applicable;
- legitimate interests - processing is necessary for the legitimate interests of Best Foot Forward or a third party, unless overridden by the individual's rights and freedoms;
- consent - the individual has freely given specific, informed and unambiguous consent.

Where special category data is processed, Best Foot Forward will also identify an appropriate condition under Article 9 of the UK GDPR and, where required, a condition under the Data Protection Act 2018.

Whenever we collect personal data directly from individuals, we will provide the privacy information required by data protection law. We will only collect information for specified, explicit and legitimate purposes. If we propose to use personal data for a materially different purpose, we will consider compatibility, provide further privacy information and obtain consent where consent is the appropriate lawful basis.

Staff must only access or process personal information where it is necessary for their role and must use approved Best Foot Forward systems and processes.

Data Retention, Review and Secure Disposal

Best Foot Forward will not retain personal data indefinitely or simply because it may be useful in the future. Standard retention periods are set out in Appendix A: Data Retention & Disposal Schedule.

- Records must be stored in the appropriate approved system and, where practicable, have a clear retention trigger and disposal date.
- When a retention period expires, the record must be securely destroyed, anonymised, transferred or formally reviewed as specified in Appendix A.
- Where a legal hold, safeguarding investigation, complaint, insurance claim, information-rights request, public inquiry or other formal investigation requires information to be preserved, routine destruction must be suspended. A revised review or disposal date must be set when the hold ends.
- Duplicate and temporary copies must be deleted when no longer required.
- Where records are held by a school, local authority or other commissioner as the statutory or authoritative record, Best Foot Forward will avoid retaining unnecessary duplicate copies.
- Disposal must be secure. Paper records containing personal data must be confidentially destroyed; electronic records must be permanently deleted from live systems where reasonably practicable.

The CEOs will oversee an annual retention and disposal review. Staff must not destroy records outside the schedule where they know or reasonably believe the record is required for safeguarding, legal, contractual or regulatory purposes.

Sharing Personal Information

We will only share personal information where there is a lawful and proportionate reason to do so. This may include where:

- there is a safeguarding or safety concern affecting a student, staff member or another person;
- we need to liaise with schools, local authorities, children's services, health services or other agencies;
- a supplier or contractor needs information to provide an authorised service;
- we are required or permitted by law to share information with law enforcement, courts, regulators or government bodies;
- sharing is necessary in connection with legal proceedings, the prevention or detection of crime, fraud or safeguarding responsibilities;
- information is used for research or statistical purposes in an appropriately anonymised form, or another lawful basis applies.

Consent is not always required for safeguarding information sharing. Data protection law does not prevent appropriate sharing where this is necessary to safeguard a child or another person. Staff should follow the Child Protection & Safeguarding Policy and consult the DSL where appropriate.

When appointing suppliers or contractors who process personal data on our behalf, Best Foot Forward will use providers that can provide sufficient guarantees of data protection compliance, put appropriate contractual terms in place and share only the information necessary for the service.

International Transfers

Where Best Foot Forward transfers personal data outside the UK, it will ensure the transfer is permitted by UK data protection law. This may include relying on UK adequacy regulations or putting appropriate safeguards in place. Staff must not use unapproved services that transfer Best Foot Forward personal data internationally.

Use of Personal Devices for Monitoring a Student's Diabetes Data

1. Purpose

This section outlines the data-protection requirements for Best Foot Forward staff who access or monitor a student's diabetes-related health data - including glucose readings transmitted from medical devices - on personal mobile phones or tablets. This information is special category personal data and requires enhanced protection under the UK GDPR and the Data Protection Act 2018.

2. Scope

This section applies to:

- all Best Foot Forward staff who support students with diabetes;
- any staff member who may receive glucose alerts or monitoring data through an approved application such as LibreLinkUp;
- any personal mobile device authorised to access or receive such data.

3. Lawful Basis for Processing

Before diabetes-related health data is accessed, Best Foot Forward must identify and document the applicable Article 6 lawful basis and Article 9 special-category condition for the particular arrangement. Depending on the circumstances, this may include vital interests and/or another lawful condition supported by the student's care arrangements. Explicit consent must not be relied upon where it is not freely given or where another lawful basis is more appropriate.

Any remote monitoring arrangement must be agreed with the parent/carer, the referring organisation where applicable, and the relevant health plan or care arrangements. Staff must not provide clinical interpretation beyond their role or training.

4. Conditions for Using Personal Devices

4.1 Staff Agreement and Authorisation

- Staff must receive written authorisation from Best Foot Forward management.
- Staff must sign a Best Foot Forward Personal Device Access Agreement confirming that they understand the responsibilities and security requirements.

4.2 Device Security Requirements

Personal devices used for accessing diabetes data must:

- have a secure PIN, password, fingerprint or facial-recognition lock;
- use automatic screen timeout;
- have up-to-date security patches and operating system;

- use device encryption;
- not be rooted or jailbroken;
- not be shared with family members or other individuals while the Best Foot Forward monitoring arrangement is active.

4.3 App Use Requirements

- Only an approved monitoring application may be used.
- No screenshots, forwarding, exporting or unauthorised sharing of health data is permitted.
- Staff may only use the app within the agreed scope of their role.
- Notifications containing health data must not be visible on a shared lock screen.

5. Data Minimisation and Access Control

- Only staff who require access to support the student safely may receive alerts or access data.
- Management must keep and regularly review a list of authorised users.
- Access must be revoked immediately when a staff member no longer supports the student or the monitoring arrangement ends.

6. Data Removal and Staff Leaving Best Foot Forward

- The monitoring app or Best Foot Forward account access must be removed or revoked immediately when no longer required.
- Any cached or stored Best Foot Forward health data must be securely deleted.
- Best Foot Forward must record completion of the removal/revocation process.
- Backups containing Best Foot Forward health data must not be deliberately restored to another personal device.

7. Alternative to Personal Devices

Use of a personal device must never be mandatory. Where a staff member does not wish to use a personal device, cannot meet the security requirements or does not have a compatible device, Best Foot Forward will make alternative arrangements, which may include providing a work-issued device where necessary.

8. Reporting Data Breaches

Any suspected or actual personal-data breach - including unauthorised access, device loss, accidental disclosure or inappropriate retention - must be reported immediately to Best Foot Forward management and handled under the organisation's data-breach arrangements. Breach records will be retained in accordance with Appendix A.

Staff Acknowledgement Statement

I confirm that I have received, read and understood the Best Foot Forward Data Protection Policy, including Appendix A: Data Retention & Disposal Schedule. I understand my responsibilities in handling personal data lawfully, fairly, securely and in accordance with applicable data protection law.

By signing this statement, I agree to:

- comply with the expectations and procedures in this policy and Appendix A;



- only collect, access, use, store, retain or share personal information where necessary for my role and permitted by Best Foot Forward;
- maintain the confidentiality and security of personal data;
- follow the applicable retention and disposal requirements and not retain personal information for personal convenience;
- report data breaches, concerns or risks immediately;
- seek guidance if I am unsure about data handling, retention or disposal responsibilities.

I understand that failure to follow data-protection requirements may result in disciplinary action.

Staff Member Name: _____

Job Title: _____

Signature: _____

Date: _____

Appendix A - Data Retention & Disposal Schedule

This appendix forms part of the Best Foot Forward Data Protection Policy. It sets the organisation's default retention periods. A longer period may apply where legislation, safeguarding requirements, a commissioner/funder contract, insurance, legal proceedings or another documented lawful reason requires it. A shorter period should be used where the information is no longer necessary.

DfE note: the Department for Education's own retention schedule applies directly to data processed by DfE and its arm's-length bodies where DfE is controller. Best Foot Forward uses relevant DfE periods and the DfE "Data protection in schools - record keeping and management" guidance as education-sector benchmarks, adapted to Best Foot Forward's role as an alternative provision provider.

A1. Student and learner records

Record / information	Default retention period	Retention trigger	End action	Basis / note
Referral forms, registration details and parent/carer contact details	6 years	End of Best Foot Forward provision	Destroy	BFF operational/contractual record; avoid unnecessary duplication of the statutory pupil record.
Provision agreements, individual plans, road maps and objectives	6 years	End of provision	Destroy	Supports commissioning, provision and limitation-period needs.
Baseline assessments, academic assessments and progress records	6 years	End of provision	Destroy	BFF operational record unless commissioner/funder requires longer.
Weekly reports, six-week reviews and end-of-placement reports	6 years	End of provision	Destroy	BFF operational record.
Attendance and routine session records	6 years	End of provision	Destroy	BFF operational record; statutory school attendance record remains with the responsible school where applicable.
Behaviour/engagement records not forming part of safeguarding record	6 years	End of provision	Destroy	If safeguarding thresholds are met, move/copy relevant material to safeguarding record.
Qualification/achievement evidence retained by BFF	6 years or funding requirement	Completion/end of provision or final payment	Review / Destroy	DfE benchmark: evidence of DfE-funded learning can be 6 years from last payment.
Copies of EHCPs and information supplied by referrer	Duration of provision + up to 6 years where needed to evidence provision	End of provision	Review / Destroy	Do not retain merely as a duplicate where no continuing need exists.

A2. Safeguarding and child protection

Record / information	Default retention period	Retention trigger	End action	Basis / note
Child protection files / safeguarding case records	Until child's 25th birthday	Child's date of birth	Securely destroy	DfE school record-keeping benchmark. Transfer separately and securely when responsibility transfers.
Child protection file relating to child sexual abuse	Until child's 75th birthday	Child's date of birth	Securely destroy	DfE school record-keeping guidance reflecting IICSA recommendation.
Records relating to protection of children/learners held for organisational safeguarding purposes	Age 25 or 10 years after case received, whichever is later, where this DfE benchmark is the more appropriate record category	Case received / date of birth	Review	DfE retention-schedule benchmark; use professional judgement to avoid duplicate retention where the statutory child protection file is held elsewhere.
Allegations of child protection against a member of staff, including unfounded allegations	Until normal retirement age or 10 years from allegation, whichever is later	Date of allegation	Securely destroy	DfE data-protection-in-schools/KCSIE benchmark.
Safeguarding transfer record / confirmation of secure transfer	6 years after transfer unless linked to an ongoing case	Date transferred	Destroy	Evidence that safeguarding information was transferred appropriately.

A3. Photography, video and consent

Record / information	Default retention period	Retention trigger	End action	Basis / note
Photographs/videos documenting learning or outcomes	Normally aligned to associated student record, up to 6 years where genuinely required	End of provision / purpose	Destroy	Prefer outcome-only/non-identifiable images where possible.
Unused or duplicate images	Delete promptly when no longer required	Decision not to use / duplicate identified	Destroy	UK GDPR storage limitation and data minimisation.
Case-study material and associated identifiable images	Up to 5 years	Case study sign-off	Destroy / Review	DfE corporate-communications benchmark: internal case studies 5 years.
Promotional campaign images/material	Up to 5 years, with annual appropriateness review	Campaign/publication date	Destroy / Remove	DfE corporate-communications benchmark: promotional campaigns 5 years.

Record / information	Default retention period	Retention trigger	End action	Basis / note
Website/social-media images	Review at least annually; remove when no longer current or appropriate	Publication date	Remove / Destroy	Publication can persist outside BFF control; do not retain merely because copies may exist elsewhere.
Photography/video consent and withdrawal records	Duration of use plus 6 years where needed to evidence the decision	Final use / withdrawal	Destroy	BFF evidential period; consent withdrawal applies to future use where reasonably practicable.

A4. Complaints, information rights and data breaches

Record / information	Default retention period	Retention trigger	End action	Basis / note
Formal complaints about Best Foot Forward provision	10 years	Date last modified / case closure	Destroy	DfE retention-schedule benchmark for complaints about education providers.
Subject Access Request (non-HR) records	2 years	Date last modified / request closed	Destroy	DfE retention-schedule benchmark.
HR Subject Access Request records	7 years	Date last modified / request closed	Destroy	DfE retention-schedule benchmark.
Personal data breach records	6 years	Date last modified / incident closed	Destroy	DfE retention-schedule benchmark.
Information-rights complaints/correspondence not otherwise covered	5 years	Date last modified	Destroy	DfE correspondence benchmark.

A5. Recruitment and staff records

Record / information	Default retention period	Retention trigger	End action	Basis / note
Unsuccessful application forms and recruitment paperwork	12 months	Recruitment decision	Destroy	Matches BFF recruitment/application arrangements; review if legal claim or complaint pending.
Successful applicant recruitment documents relevant to employment	6 years	End of employment	Destroy	Retain as part of personnel file where necessary.
Personnel file	6 years	Termination of employment	Destroy	DfE school record-keeping benchmark / limitation period.
DBS certificate copy or certificate information beyond audit details	Normally no longer than 6 months	Recruitment/relevant decision	Securely destroy	DBS guidance. Keep only permitted audit details after destruction.

Record / information	Default retention period	Retention trigger	End action	Basis / note
DBS audit details (date, type, certificate number/reference and decision)	Employment + 6 years where required as safer-recruitment evidence	End of employment	Destroy	BFF safer-recruitment evidence; do not retain certificate image.
Right-to-work check evidence	Employment + 2 years	End of employment	Destroy	Home Office employer guidance.
Training/CPD and appraisal records	6 years	End of employment	Destroy	BFF employment/business need.
Disciplinary/grievance records	6 years after employment ends unless safeguarding rule is longer	End of employment / case closure	Destroy	Safeguarding allegation retention takes precedence.

A6. Finance, contracts and commissioning

Record / information	Default retention period	Retention trigger	End action	Basis / note
Invoices, sales/purchase records, VAT/accounting records	6 years	End of relevant financial year/accounting period	Destroy	Tax/accounting and DfE financial-record benchmarks.
PAYE/payroll records	At least 3 years	End of tax year to which they relate	Destroy	HMRC requirement; retain longer if part of another required accounting record.
Contracts, grants and agreements	6 years	Contract end	Destroy	DfE/TNA contractual-record benchmark.
Contracts executed as deeds	12 years	Deed/contract expiry	Destroy	Limitation Act benchmark.
Commissioning reports and schedules of work	5-6 years depending on contract terms	Contract end / last modified	Destroy	DfE contract-data benchmark; commissioner terms take precedence where lawful.
Funding evidence	At least 6 years or funder-specified period	Final payment / project end	Destroy / Review	DfE-funded learning benchmark may require 6 years from final payment.

A7. Health, safety and operational records

Record / information	Default retention period	Retention trigger	End action	Basis / note
General risk assessments	6 years after superseded/activity ends	Replacement / end of activity	Destroy	BFF operational/limitation benchmark.
Individual student risk assessments	6 years unless safeguarding-related	End of provision	Destroy	Safeguarding record period takes

Bethany Russell 07394 950803

beth@bestfootforward.org.uk

Andrew Russell 07538 719783

andrew@bestfootforward.org.uk

Website: www.bestfootforward.org.uk | Contact: admin@bestfootforward.org.uk

Record / information	Default retention period	Retention trigger	End action	Basis / note
				precedence where relevant.
Accident/incident records involving adults	At least 3 years; normally up to 6 years where liability evidence is required	Date of incident	Review / Destroy	HSE/RIDDOR minimums plus limitation considerations.
Accident/incident records involving children	Until at least age 21 where potential civil claim evidence is relevant	Date of birth / incident	Review / Destroy	Limitation considerations; retain longer where safeguarding or legal hold applies.
Diabetes personal-device authorisation/access logs	6 years	End of monitoring arrangement	Destroy	Evidence of authorisation, access removal and security compliance.

A8. Policies, governance, systems and routine administration

Record / information	Default retention period	Retention trigger	End action	Basis / note
Current organisational policies	Current	Replacement	Archive superseded version	Maintain current controlled copy.
Superseded policies	10 years	Replacement date	Review / Destroy	Allows BFF to evidence which policy applied at an earlier date.
Management meeting records containing substantive decisions	5 years	Date last modified	Destroy	DfE business-operations benchmark.
Routine administrative emails with no continuing record value	Delete when no longer needed; normally within 12 months	Purpose completed	Destroy	Emails inherit retention from their content; important emails must be filed with the relevant record.
System access/user lists	Duration of access + 12 months unless needed for security investigation	Access revoked	Destroy	Review access promptly and remove inactive users.
Disposal logs	6 years	Date of disposal action	Destroy	Retain category-level evidence of disposal, not copies of destroyed personal data.

A9. Retention holds and exceptions

Routine deletion must be suspended where a record may be relevant to an ongoing or reasonably anticipated safeguarding investigation, police investigation, LADO process, complaint/appeal, legal proceeding, insurance claim, public inquiry, regulatory investigation or information-rights request. When the hold ends, a new review or disposal date must be

recorded. Records must not be retained indefinitely after a hold without a documented reason.

A10. Secure disposal requirements

- Paper records containing personal or confidential information must be cross-cut shredded or disposed of using an approved confidential-waste process.
- Electronic records must be permanently deleted from the relevant live system when due for disposal. Where backups cannot be selectively altered, the record must not be restored into active use after its scheduled deletion date.
- Personal data must not be left in ordinary waste, recycling bins, downloads folders, personal cloud storage or on personal devices.
- Where information has continuing statistical or service-development value but individual identification is unnecessary, anonymisation should be considered instead of continued retention of identifiable data.

A11. Annual review and responsibility

The Best Foot Forward CEOs will arrange a retention and disposal review at least annually. The review should cover student systems, safeguarding systems, Google Drive and other approved cloud storage, email, HR and finance systems, archived paper files and any authorised local-device storage. The DSL must be consulted before safeguarding material is destroyed.

A12. Sources and guidance used

- Department for Education, "Data protection in schools - Record keeping and management" (current GOV.UK guidance).
- Department for Education, "DfE retention schedule", updated 9 June 2026. This schedule applies directly to DfE/ALB processing and is used by Best Foot Forward as a benchmark where relevant.
- Department for Education, "Keeping children safe in education 2025" (in force until 31 August 2026) and "Keeping children safe in education 2026" (comes into force 1 September 2026).
- Information Commissioner's Office, UK GDPR storage limitation guidance: organisations should establish justified standard retention periods and regularly erase or anonymise data no longer required.
- Disclosure and Barring Service guidance on handling certificate information, including secure storage, retention and disposal.
- Relevant HMRC, Home Office, HSE and limitation-period requirements where applicable.

Control note: This schedule should be reviewed whenever DfE, ICO, DBS or other relevant statutory guidance changes, and whenever Best Foot Forward introduces a new system, category of personal data, funding stream or commissioning arrangement.