

DATA PROTECTION POLICY

Date to be implemented from:	September 2026
Date to be reviewed by:	August 2027
Version No:	v10
Lead responsibility:	Data Processor Officer

Distribution to:	
All Staff	✓
SLT only	☐
Teaching Staff/Tutors	☐
Administration Staff	☐
Other (please specify)	✓ Learners

Key Contacts:	
Data Processor Officer	
Information Commissioners Office	www.ico.org.uk

This Policy supersedes any previous Policy of this name or instructions that pre-date this edition.

DATA PROTECTION POLICY

1 Policy Statement

Barrett-Bell Ltd does all it can to ensure that Staff and Learners information is safe and secure. The Company is committed not only to the letter of the Law, but also to the spirit of the Law and places high importance on the correct, Lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

Barrett-Bell Ltd has an accessible, documented system for data subjects to submit complaints. Barrett-Bell Ltd acknowledges data breaches and deals with them immediately investigates them without undue delay, keeping the complainant informed and notifying them of the outcome.

Barrett-Bell Ltd is registered as a Data Controller with the Information Commissioner's Office (ICO), in line with Data Protection/UK GDPR. The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Full details of data held by Barrett-Bell Ltd, is outlined in our Staff Privacy Notice and our Learner Privacy Notice.

2 Regulations

Following the UK's departure from the EU, the GDPR was incorporated into the domestic Law that applies in the UK, under Section 3 of the European Union (Withdrawal) Act 2018 (the "Withdrawal Act"). UK Data Protection Law is primarily governed by the UK GDPR and the Data Protection Act 2018 (DPA), amended by the Data (Use and Access) Act 2025 (DUAA).

The Privacy and Electronic Communications Regulations (PECR) relates to specific exemptions for analytics and security (e.g. website cookie consent)

The most significant recent operational shift took effect on 19-6-26 requires all organisations to handle Data Protection complaints formally before individuals can escalate them to the Information Commissioner's Office.

2.1 The Policy applies to:

- The offices and associated premises for Barrett-Bell Ltd delivery
- All methods of delivery – classroom based and on-line
- All Staff, including work experience students, apprentices of Barrett-Bell Ltd and its partners

- All contractors, suppliers and other people working on behalf of Barrett-Bell Ltd
- All data held by Barrett-Bell Ltd and its partners relating to identifiable individuals, electronic and hard copy

2.2 Barrett-Bell Ltd will ensure that its service providers (Data Processors) that

- Provider
- HR Provider
- IT / Cloud Provider
- Certification Awarding Bodies
- Funding Authorities
- Educational Platform/App Providers
- Work Placement Organisations/Accredited Engineers

2.3 All personal data will be Processed lawfully, fairly and in a transparent manner in relation to data subjects.

2.4 Processing of personal data is Lawful only if, and to the extent that, it is permitted under UK Data Protection Law. The UK GDPR provides a list of legal bases on which personal data may be processed:

- **Consent** - prior, freely given, specific, informed and unambiguous consent of the data subject
- **Contractual** necessity
- Compliance with **legal obligations** legitimate interests necessary for the purposes of legitimate interests pursued by the Data Controller
- **Vital interests** – as a company dealing with possible at risk and vulnerable adults
- **Public task** - processing necessary to perform a task for your official functions
- **Recognised legitimate interest** – Safeguarding, investigating crime, emergencies
- **Legitimate interests** - for the legitimate interests or the legitimate interests of a third party

3 Definitions

3.1 This Policy uses the following definitions:

- **Personal Data** - any information relating to an identified or identifiable

natural person directly or indirectly, by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

- Data Subject - an individual who is the subject of the relevant personal data
- Special Categories of Personal Data - includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health, sex life or sexual orientation, genetic data or biometric data
- Sensitive Personal Data - special categories of personal data together with personal data relating to criminal convictions and offences
- Profiling - any form of automated processing of personal data consisting of the use of personal data to evaluate, analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- Processing - any operation(s) performed on personal data (whether or not by automated means) such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- Data Controller - the person, public authority, agency, company or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- Data Processor - a natural or legal person, public authority, agency, company or other body which processes personal data on behalf of the Data Controller
- Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

personal data transmitted, stored or otherwise processed

4 Process

- 4.1 Data is only collected for appropriate, specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes – ie purpose limitations. Barrett-Bell Ltd will only hold data required for the successful delivery of courses, compliance with Safeguarding requirements, Funding Bodies, MATRIX and the Examination Boards / External Verifiers.
- 4.2 Personal data will be processed lawfully, fairly and in a transparent manner. Data Controllers will provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- 4.3 Personal data will be processed in a manner 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.
- 4.4 Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be considered compatible with the initial purposes.
- 4.5 Barrett-Bell Ltd shares Learner data with relevant awarding bodies, funding bodies and companies we deal with regarding qualifications and training.
- 4.6 Barrett-Bell Ltd shares Staff information with companies for the effective day to day running of the business and future training/progression for individuals. Barrett-Bell Ltd does not export personal information to countries outside of the UK.
- 4.7 Data will be processed to meet the requirements of being:
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
 - Accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate, have regard to the purposes for which it is processed is erased or rectified without delay
 - Retained only for as long as necessary - Barrett-Bell Ltd retention timescales are outlined in the Learner Privacy Notice and the Staff Privacy Notice

- 4.8 Barrett-Bell Ltd holds electronic and hard copies of personal information of Staff and Learners which are kept securely for the duration of the time needed for retention.
- 4.9 When any personal data is to be erased or otherwise disposed of for any reason, (including where copies have been made and are no longer needed), it shall be securely deleted and disposed of.
- 4.10 Data breaches will be dealt with immediately and reported as required:
- All data breaches must be reported immediately to the Company's Data Processor by Staff and/or Learners
 - If a personal data breach occurs, and that breach is likely to result in a risk to the rights and freedoms of an individual (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) then the Data Processor must ensure that the Information Commissioner's Office is informed within 72 hours after becoming aware of it
 - If a data breach is likely to result in high risk to the rights and freedoms of individuals, the Data Processor Officer must ensure that all affected individuals are informed directly and without undue delay
 - The individual has the right to report a data breach to the Information Commissioner's Office. www.ico.org.uk after the internal process has been followed

5 Data Security

- 5.1 **Storage** - Barrett-Bell Ltd holds electronic and hard copies of personal information of Staff and Learners, the full details are outlined in the Staff Privacy Notice and the Learner Privacy Notice
- Electronic data is held on a secure cloud server, which has a Multifactor Identification System in place
 - Working hard copies are held at all our sites, in secure filing cabinets and lockable cupboards at all times
 - Archived hard copies are held at our storage units, which have security coded access and is only accessible by Senior Management. Records of the data kept in the storage unit are held on our secure cloud server
- 5.2 **ICT security** - Barrett-Bell Ltd works in conjunction with our ICT contractor,

OfficeTechHub Ltd. Barrett-Bell Ltd electronic data is held on a UK cloud server, which has a multifactor identification system.

- No software can be installed onto the Barrett-Bell Ltd cloud account without permission of SLT and the assistance of our ICT contractor
- There are no data files held on laptops static drives, data is held on the secure cloud, password protected and only accessible by Barrett-Bell Ltd Staff
- Staff are not permitted to use personal electronic equipment i.e. laptops and mobile phones for Barrett-Bell Ltd commercial purposes

5.3 **Use** – in conjunction with the ESFA Privacy Notice and in accordance with Data Protection regulations, personal data is used by Barrett-Bell Ltd to exercise its functions to meet its statutory responsibilities:

- Information collected on individuals is used in Learner Files is only shared as required by third parties in relation to the courses we run only (eg. City & Guilds, ESFA, sector external verifiers, sector standards, Register of Exercise Professionals (REPS), Chartered Institute for the Management of Sport and Physical Activity (CIMSPA) and OfQUAL)
- Staff Files - information is shared as required by third parties in relation to employment (third parties include: Company Accountant, Company HR Consultants, governing bodies and legal or criminal investigations)
- Artificial Intelligence Transparency ensures all parties are clear where AI is being used and how it is being used

5.4 **Transfer** – Barrett-Bell Ltd takes data security and protection extremely seriously and ensures that the following measures are taken with respect to all communications and other transfer involving personal data:

- All emails containing personal data must be encrypted and marked 'Confidential'
- Personal data may be transmitted over secure networks only - transmission over unsecured networks is not permitted in any circumstances.
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked 'confidential'

5.5 **Disposal** – all copies (hard or electronic) will be deleted as required:

- electronic copies of data are deleted by the Administrator on instruction from Senior Management
- Hard copies of data are shredded by the Administrator on instruction from Senior Management
- Barrett-Bell Ltd will either use on-site shredders and record disposal or an external shredding company who will certify the destruction of documentation in accordance with BS EN 15713:2009

6 The Rights of Data Subjects (Individuals)

6.1 The Data Protection/UK GDPR sets out the following rights applicable to data subjects as a key transparency requirement under the Data Protection/UK GDPR:

- **The right to be informed** - individuals have the right to be informed about the collection and use of their personal data
- The right to be informed about the collection and use of their personal data.
- Barrett-Bell Ltd will ensure individuals have information including: the purpose for processing their personal data, the retention periods for that personal data and who it will be shared with. This is called 'privacy information'

6.2 Individuals have the right to access their personal data:

- **The right of access** - commonly referred to as subject access
- Individuals can make a subject access request verbally or in writing. The Company then has one calendar month to respond to the request and in most circumstances, will not charge a fee to deal with the request
- A SAR is not guaranteed where it is unfounded, excessive or professional privilege

6.3 The regulations allow for an individual to have inaccurate personal data corrected

- **The right to rectification** - this right has close links to the accuracy principle of the Data Protection/UK GDPR
- An individual may be able to have incomplete personal data completed, although this will depend on the purposes for the processing
- Requests for rectification can be made verbally or in writing. Barrett-Bell Ltd

has a specific obligation to reconsider the accuracy upon request and one calendar month to respond

6.4 The Data Protection/UK GDPR introduces a right for individuals to have personal data deleted ('the right to be forgotten') under certain circumstances:

- **The right to erasure** - is not absolute as Examination Board and legal time scales for the retention of personal data must be adhered to
- Individuals can make a request for erasure verbally or in writing, Barrett-Bell Ltd has one calendar month to respond to a request

6.5 Individuals have the **right to restrict** the processing of their personal data in certain circumstances:

- The right to restrict processing - an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data
- When processing is restricted, organisations are permitted to store the personal data, but not use it
- An individual can make a request for restriction verbally or in writing, Barrett-Bell Ltd has one calendar month to respond to a request

6.6 The Data Protection/UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances:

- **The right to object** - individuals have an absolute right to stop their data being used for direct marketing
- In other cases where the right to object applies, organisations may be able to continue processing if they can show they have a compelling reason for doing so
- Individuals have the right to make an objection verbally or in writing, Barrett-Bell Ltd has one calendar month to respond to an objection

6.7 **Consent** - Barrett-Bell Ltd abide by strict rules for gaining consent from individuals:

- Consent shall be freely given, fully informed and evidenced on appropriate documentation
- Requests for consent shall be easily understood, in plain English and unambiguous

- Consent for visibility when hosting an online session or webinar may be required for attendance or evidence of live interactions (this should be made clear at Induction and Tutors must consider digital privacy and seek permission for recording sessions)
- Consent can be withdrawn at any time for data, which is not statutory and lawfully required for the course delivery
- Silence, inactivity, lack of response and pre-ticked boxes are not to be taken as indicating consent

7 Timescales

Records are required to be kept by a variety of bodies related to the delivery of courses and for the Quality Assurance of courses. Barrett-Bell Ltd adheres to the following requirements:

- Barrett-Bell Ltd and partners hold Staff details, ID, qualifications, appraisals, reviews HR files for a minimum period of 5 years after the end of employment. Financial information must be held for a period of 3 years after the end of employment
- Barrett-Bell Ltd holds course work, Portfolios, certification information for 6 years in accordance with awarding bodies
- Barrett-Bell Ltd hold individuals contact information and qualification dates for 5 years for those who have consented (Barrett-Bell Ltd will contact Learners to remind them of their renewal dates)
- Barrett-Bell Ltd hold ID for Learners until the end of the course, at which time it is either returned to the Learner or shredded
- ESFA hold information for a period of 6 years
- City & Guilds hold individual's registration and certification information for 6 years
- Blueflame holds individuals' registration, ACS elements course work, certification information for 6 years

- Tracpipe hold copies of certificates without timescale to ensure those working with their product are qualified

8 CCTV

Barrett-Bell Ltd operates a number of CCTV cameras in order to assist with the security of the Company and protect property and individuals. If any individual has any queries regarding the operation of the CCTV system, they should contact the Data Protection Officer.

- 8.1 The images are held in secure conditions for 30 days, and previous data is automatically erased.
- 8.2 If anyone wishes to access any personal data about themselves from the CCTV system within 21 days of an incident/occurrence, they will be required to complete and return a Subject Access Request form, with as much information as possible to enable the data to be located.

9 Enforcement

- 9.1 All Staff must follow the Staff guidelines, which are outlined in our Staff Privacy Policy, without exception.
- 9.2 Staff found to be in violation of this Policy and the guidelines by either unintentionally or maliciously stealing, using or otherwise compromising corporate or personal data may be subject to disciplinary action up to and including termination and may be financially liable for a breach of Data Protection/UK GDPR.

10 Penalties for data breaches

- 10.1 Fines based on serious breaches of the Data Protection/UK GDPR are potentially substantial - fines of up to £17.5 million or 4% of the annual worldwide turnover, whichever is higher.
- 10.2 Fines for infringements will be considered on a case-by-case basis and take a number of circumstances into consideration, including any intentional nature of the infringement, how many people were affected or any previous infringements by the controller/company.

- 10.3 Separate to these fines and penalties, individuals will have the right to claim compensation for any damage suffered as a result of violating the GDPR.

11 Accountability

Barrett-Bell Ltd are accountable for security and confidentiality of all data the company collects, this is overseen by the Data Protection Officer.

- 11.1 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, other Data Protection related Policies with the Data Protection/UK GDPR and other applicable Data Protection regulations, in relation to Barrett-Bell Ltd and its partners.
- 11.2 A number of measures are in place to ensure Barrett-Bell Ltd are accountable:
- Updating, adopting and implementing Data Protection Policies
 - Putting written contracts in place with organisations that process personal data on Barrett-Bell Ltd's behalf
 - Maintaining documentation of processing activities
 - Implementing appropriate security measure.
 - Recording and, where necessary, reporting personal data breaches
 - Adhering to relevant Codes of Conduct
 - Implementing a privacy framework to create a culture of privacy
 - Keeping individuals informed of data collected, secure storage, retention, disposal and updates
 - Annual audits of personal data accuracy take place
 - Audits of electronic equipment to take place every six months
- 11.3 Accountability obligations are ongoing - Barrett-Bell Ltd reviews and where necessary updates the measures in place.