

GDPR and Learner Privacy Policy

Document control	Current position
Policy owner	Director of Contracts & Operations
Operational owner	Quality & Compliance Lead
Applies to	Adult learners (19+), applicants, staff, employers, funders, awarding bodies, referral partners, subcontractors, suppliers and other stakeholders involved in funded training provision
Primary purpose	To explain how Quack Recruitment & Training Ltd collects, uses, shares, stores and protects personal data for funded training programmes and associated recruitment/progression activity
Safeguarding leads	DSL: Jessica Roughton Deputy DSL: Aaron Jones
Data protection contact	compliance@quackrecruitmentandtraining.co.uk 0333 577 0036
Next review	October 2026, or sooner if legislation, funder requirements, systems, delivery model or organisational responsibilities change

Funder feedback addressed

This version has been revised so the policy is no longer focused mainly on recruitment candidates and workers. It now explicitly covers funded programme learners, enrolment, eligibility, learner support, ILR/funding evidence, safeguarding, learner files, awarding body activity, progression evidence and data sharing with funders and public bodies. The next review date has also been corrected to October 2026.

Contents

1. Purpose and Policy Statement.....	3
2. Scope of this Policy	3
3. Data Protection Principles	4
4. Roles and Responsibilities	4
5. What Personal Data we Collect for Funded Programmes	4
6. How, When and Why We Collect Learner Data	5
7. Lawful Basis for Processing	5
8. Special Category and Criminal Offence Data	6
9. How Learner Data is used Across Funded Programmes.....	6
10. Data Sharing: Funders, Awarding Bodies, Employers and Partners	6
11. Learner Files, PICS, ILR, FESIT and Audit Evidence.....	7
12. Safeguarding, Prevent and Welfare Information Sharing	7
13. Online Learning, Digital Platforms and Systems.....	7
14. Learner Voice, Case Studies, Photography and Marketing	8
15. Data Security, Confidentiality and Access Controls	8
16. Data Accuracy, Minimisation and Quality Assurance	8
17. Retention and Disposal	9
18. Learner and Data Subject Rights	9
19. Subject Access Requests and Complaints	9
20. Personal Data Breaches	10
21. Staff Training, Monitoring and Review	10
Annex A: Funded Programme Data Map.....	11
Annex B: Retention Schedule	11
Annex C: Third-party Systems and Data Sharing	11
Annex D: Version Control.....	12

1. Purpose and Policy Statement

Quack Recruitment & Training Ltd is committed to protecting personal data and handling information lawfully, fairly, securely and transparently. This policy explains how the organisation collects, uses, shares, stores and protects personal data in relation to funded training programmes, including Skills Bootcamps and associated learner recruitment, enrolment, delivery, support, assessment, quality assurance, progression and funding compliance activity.

This policy has been revised to reflect the training and learner side of the business, not only recruitment activity. It applies to funded learners, applicants, employers, staff, funders, awarding bodies, referral partners and other stakeholders involved in the learner journey. It should be read alongside the Safeguarding Policy, Prevent Risk Assessment, Online and E-Learning Policy, Information Security Policy, Learner Support Policy, Document Retention Policy, Complaints Policy and relevant funder contract requirements.

The policy supports compliance with UK data protection law, including the UK GDPR and the Data Protection Act 2018, and sets out how learner data is managed in a way that supports eligibility checking, learner support, safeguarding, attendance monitoring, achievement, progression, audit readiness and continuous improvement.

Policy Standard

Personal data must only be collected where there is a clear purpose, used only for lawful and transparent reasons, kept accurate, shared only where appropriate, stored securely and retained only for as long as required by law, funding rules, audit requirements or legitimate organisational need.

2. Scope of this Policy

This policy applies to all personal data processed by Quack Recruitment & Training Ltd in connection with funded training and learner activity. This includes data processed before, during and after a programme.

- adult learners aged 19+ and applicants applying for funded programmes;
- funded programme participants, including Skills Bootcamp learners;
- learners receiving IAG, enrolment, assessment, employability or progression support;
- staff, tutors, assessors, IQA staff, progression staff, learner engagement staff, managers and directors;
- employers involved in interviews, job matching, progression, vacancy discussions or feedback;
- funders, mayoral combined authorities, local authorities, DfE/DWP/Ofsted where applicable, awarding bodies, auditors and external quality assurance bodies;
- third-party systems and processors used to deliver, record, quality assure or report funded provision, including PICS, BKSB, Highfield systems, Microsoft Teams, SharePoint, Power BI and other approved platforms.

Where Quack processes personal data on behalf of a funder or awarding organisation, the applicable contract, data sharing agreement, data processing agreement or funding rules will be followed. Where Quack determines how and why personal data is processed for its own learner support, quality assurance, safeguarding, progression or operational purposes, Quack will act as data controller for that processing.

3. Data Protection Principles

All staff must apply the following principles when handling personal data.

Principle	What this means in funded programme delivery
Lawfulness, fairness and transparency	Learners must be told what data is collected, why it is needed, how it is used, who it may be shared with and how long it may be kept.
Purpose limitation	Learner data must only be used for clear and legitimate purposes such as enrolment, eligibility, learning, support, safeguarding, assessment, funding, audit, quality assurance and progression.
Data minimisation	Staff must collect only the data needed for the purpose. Unnecessary evidence, excessive copies of ID or unrelated personal information must not be retained.
Accuracy	Learner records, ILRs, attendance records, support needs, progression records and contact details must be kept accurate and corrected promptly where errors are found.
Storage limitation	Data must not be kept indefinitely. Retention must follow funder, awarding body, statutory and organisational retention requirements.
Integrity and confidentiality	Personal data must be stored securely, accessed only by those with a legitimate need and protected from unauthorised access, loss or disclosure.
Accountability	Leaders must be able to evidence compliance through policies, training, records, data checks, audit trails, data sharing arrangements and review activity.

4. Roles and Responsibilities

Role	Responsibilities
Director of Contracts & Operations	Has senior accountability for ensuring data protection is embedded within funded programme delivery, contract management, compliance oversight, audit readiness and organisational governance.
Quality & Compliance Lead	Maintains operational oversight of policy implementation, learner file quality, staff guidance, compliance checks, data protection actions and links with safeguarding, SEND and quality assurance.
DSL and Deputy DSL	Ensure safeguarding, Prevent and welfare information is handled securely, proportionately and in line with safeguarding procedures. Escalate concerns where appropriate and maintain confidential records.
MIS / Data staff	Maintain accurate learner records, ILR/funding data, PICS records, FESIT/Power BI reporting, PDSAT/FIS checks and data quality processes.
Tutors, assessors and IQA staff	Use learner data only for legitimate teaching, assessment, support, progress review, quality assurance and learner welfare purposes. Keep learner files accurate and secure.
Learner engagement and progression staff	Use learner data to support enrolment, attendance, communication, IAG, job matching, employer engagement, progression tracking and outcome evidence.
All staff	Complete relevant training, maintain confidentiality, use approved systems, report breaches promptly and follow this policy at all times.
Learners	Provide accurate information, update the provider if key details change, use systems responsibly and report data, safeguarding or privacy concerns promptly.

5. What Personal Data we Collect for Funded Programmes

The information collected will depend on the programme, funder, awarding body and learner circumstances. The provider will only collect information that is necessary and proportionate for the relevant purpose.

Data category	Examples of information collected
Identity and contact details	Name, date of birth, address, postcode, telephone, email, emergency contact, learner reference numbers and unique learner identifiers where required.
Eligibility and funding evidence	Age, residency, right to live/work/study where relevant, employment status, benefit status where required, prior learning, funding eligibility declarations, ID evidence, enrolment forms and signed declarations.
Learner profile and equality data	Sex/gender, ethnicity, disability/LLDD, health declarations, postcode/IMD profile, prior attainment and other equality monitoring information required for funded programme reporting.
Learning and assessment data	IAG records, BKSB, initial and endpoint skills scans, ILPs, SMART targets, attendance, registers, workbooks, assessment evidence, qualification outcomes, feedback and achievement records.
Support, SEND and welfare data	Declared support needs, reasonable adjustments, SEND support plans, mental health support discussions, barriers to participation, tutor handover information and support interventions.
Safeguarding and Prevent data	Safeguarding concerns, Prevent concerns, welfare notes, referrals, DSL review notes, attendance concerns and information needed to keep learners safe.
Progression and destination data	CV support, job applications, employer interviews, job matching, employer feedback, job offers,

Data category	Examples of information collected
	employment starts, MS3 evidence, payslips/contracts where required by funders, and post-completion follow-up records.
Digital and systems data	Username, system access records, Teams attendance, email communications, PICS records, online learning engagement, Highfield Vault/system evidence and audit trails.

6. How, When and Why We Collect Learner Data

Learner data may be collected at several points in the learner journey. This includes application, referral, IAG, eligibility checking, enrolment, induction, teaching, assessment, learner review, safeguarding/support activity, employer engagement, progression follow-up and audit review.

Stage	Why data is collected
Application and referral	To understand interest, suitability, initial eligibility, preferred pathway, contact details and possible barriers.
IAG and suitability	To check the programme is appropriate, understand career goals, identify support needs, confirm expectations and direct learners to alternatives where required.
Enrolment and eligibility	To meet funder requirements, confirm eligibility, create learner records, obtain declarations and support audit evidence.
Delivery and review	To record attendance, progress, assessment preparation, ILP reviews, learner support, skills scans, feedback and engagement.
Assessment and achievement	To support qualification delivery, awarding body requirements, IQA, EQA, achievement recording and certification.
Progression and MS3 evidence	To support job matching, employer contact, interview tracking, destination evidence and funding outcome claims.
Quality assurance and improvement	To evaluate teaching, learner support, safeguarding, inclusion, attendance, achievement, progression and QIP actions.

7. Lawful Basis for Processing

Quack will identify an appropriate lawful basis before processing personal data. The lawful basis may differ depending on the activity, the funding arrangement and whether the information is personal data, special category data or criminal offence data.

Processing activity	Likely lawful basis / rationale
Application, IAG and enrolment	Contract or pre-contract steps with the learner; legitimate interests in assessing suitability; funder requirements where applicable.
Eligibility, funding and audit evidence	Legal obligation, contractual obligation with funders, legitimate interests and/or public-task-related processing where required by public funded programme arrangements.
Teaching, learner support and assessment	Contract with learner, legitimate interests and delivery of funded programme obligations.
Safeguarding, Prevent and welfare	Legal obligation, vital interests where urgent, substantial public interest and safeguarding-related processing where appropriate.
Equality monitoring and LLDD/support reporting	Legal obligation, substantial public interest, equality of opportunity monitoring, funder reporting and explicit consent where appropriate.
Employer engagement and progression support	Contract, legitimate interests and funded programme requirements, with consent used where optional case studies or marketing are involved.
Marketing, photographs, testimonials and case studies	Consent unless another lawful basis is clearly documented. Learners must be able to refuse without detriment to learning or support.

Lawful basis note

Consent is not the default basis for core funded programme administration, eligibility, safeguarding, assessment, audit or funding activity. Where data is required to deliver or evidence a funded programme, learners should be told clearly why it is required and what may happen if required information is not provided.

8. Special Category and Criminal Offence Data

Some learner data is more sensitive and requires additional safeguards. Special category data may include health information, disability/LLDD information, ethnicity, biometric data where applicable, religious belief, sexual orientation or other protected information. Criminal offence data may include information about convictions, allegations or prison-leaver status where relevant to a funded programme, support requirement or safeguarding/progression matter.

Special category and criminal offence data must only be processed where there is a clear purpose, lawful basis, additional condition under UK data protection law, appropriate safeguards and restricted access. Staff must not collect sensitive information “just in case”.

- Sensitive learner information must be recorded only where it is relevant to eligibility, support, safeguarding, reasonable adjustment, equality monitoring, funding, progression or statutory/funder requirements.
- Access must be limited to staff who need the information for their role.
- Sensitive information must not be shared with employers unless there is a lawful reason, learner agreement where appropriate, or a safeguarding/legal obligation.
- Safeguarding and Prevent information must be handled separately and confidentially, with DSL oversight.
- Criminal offence information must be processed only where permitted and necessary, such as prison-leaver provision, safeguarding, suitability, employer progression support or funder requirements.

9. How Learner Data is used Across Funded Programmes

Learner data is used to support the full learner journey and to meet funding, quality, safeguarding and progression requirements. The following uses are permitted where lawful, necessary and proportionate:

- checking eligibility and suitability for funded programmes;
- creating and maintaining accurate learner records on approved systems such as PICS;
- recording IAG, attendance, learner progress, ILPs, skills scans, assessment, achievement and progression;
- identifying and supporting SEND, LLDD, health, welfare, digital, English and mathematics or confidence-related needs;
- sharing required information with funders, awarding bodies, auditors and regulators;
- supporting safeguarding, Prevent and learner welfare interventions;
- arranging interviews, job matching, employer engagement and progression support;
- evidencing MS3 outcomes and other funder milestone requirements;
- monitoring quality, learner experience, achievement, equality, inclusion and QIP actions;
- responding to complaints, appeals, audits, inspections, data requests and legal obligations.

10. Data Sharing: Funders, Awarding Bodies, Employers and Partners

Learner data may need to be shared with third parties where this is necessary, lawful and proportionate. Data sharing must be limited to the information required for the purpose and must follow contract, funding, safeguarding and data protection requirements.

Recipient / partner	Purpose of sharing
Funders and public bodies	Eligibility checks, ILR/funding returns, contract monitoring, audit, performance review, milestone evidence, safeguarding assurance and reporting requirements.
Awarding bodies and EQA/IQA processes	Registration, assessment, qualification achievement, certification, quality assurance, assessment review and compliance with awarding body rules.
Ofsted, auditors and external reviewers	Inspection, monitoring, audit, quality assurance, governance review and evidence testing where required.
Employers	Interview arrangements, job matching, progression support and employer feedback. Only relevant data should be shared. Sensitive data must not be shared unless lawful and appropriate.
Referral partners, Jobcentres or support agencies	Referral, learner support, progression, safeguarding or welfare support where appropriate.
Safeguarding, Prevent and emergency	Where needed to protect the learner or others, comply with safeguarding duties, or respond to

Recipient / partner	Purpose of sharing
services	serious concerns.
IT and system providers	Secure hosting, system access, maintenance, support and service provision under appropriate contractual arrangements.

11. Learner Files, PICS, ILR, FESIT and Audit Evidence

Funded programme data must be accurate, complete and audit-ready. Learner records may be held across approved systems and evidence folders. Staff must ensure that information entered into PICS, ILR-related records, learner files, skills scans, ILPs, registers and progression trackers is accurate and updated promptly.

- Learner files must evidence eligibility, IAG, enrolment, attendance, support, assessment, achievement and progression requirements.
- PICS must be used to record learner information, contact, attendance, support indicators, ILP information and learner journey evidence where required.
- ILR, FIS, PDSAT and occupancy/funding checks must be used to identify validation issues, data discrepancies and audit risks.
- FESIT, Power BI and internal reporting may be used to analyse learner profile, deprivation, employment status, LLDD/support declarations, participation and outcomes.
- Where data is used for management information or quality improvement, leaders should minimise, anonymise or aggregate it where individual identification is not necessary.

12. Safeguarding, Prevent and Welfare Information Sharing

Safeguarding and Prevent information is sensitive and must be handled carefully. Staff must not promise absolute confidentiality where a learner may be at risk or where information needs to be shared to protect the learner or others. Safeguarding concerns must be recorded and escalated in line with the Safeguarding Policy and Prevent Risk Assessment.

- Safeguarding, Prevent and welfare concerns must be shared only with those who need to know, normally the DSL, Deputy DSL, relevant senior leader or external safeguarding body where required.
- Attendance, disengagement, changes in behaviour, online safety concerns or welfare indicators may be recorded and reviewed as part of safeguarding and learner support activity.
- Where urgent risk is identified, staff must follow emergency escalation procedures and must not delay action because of data protection concerns.
- Safeguarding records must be stored securely, separately where appropriate, and accessed only by authorised staff.

13. Online Learning, Digital Platforms and Systems

The provider uses approved digital systems to support online learning, blended delivery, learner records, assessment, communication, quality assurance and reporting. Personal data must only be processed through approved systems and must not be downloaded, copied or shared unnecessarily.

- Microsoft Teams, SharePoint and approved email must be used appropriately for remote learning, learner communication and staff collaboration.
- PICS must be used for learner management records where required.
- BKSB, Highfield Vault/systems and other approved learning platforms must be used in line with system access controls and learner privacy expectations.
- Staff must protect usernames and passwords, use secure devices, lock devices when unattended and avoid storing learner data on unapproved personal devices.
- Online session attendance, engagement and safeguarding concerns must be recorded accurately and escalated where needed.

14. Learner Voice, Case Studies, Photography and Marketing

Learner feedback and learner voice are used to evaluate quality, support, teaching, inclusion, safeguarding, progression and improvement activity. Learner voice data should normally be used in aggregated or anonymised form unless individual follow-up is required.

Photographs, video, testimonials, case studies and marketing stories must only be used where the learner has provided clear consent and understands how the material will be used. Learners must not be disadvantaged if they choose not to consent.

- Consent must be specific, recorded and capable of being withdrawn where appropriate.
- Sensitive personal information must not be included in case studies or marketing material unless explicit consent has been obtained and the risk has been considered.
- Learner employment outcomes may be used for internal reporting, audit and funder purposes where required, but public promotion requires appropriate consent.

15. Data Security, Confidentiality and Access Controls

All staff must protect personal data from unauthorised access, loss, misuse, alteration, disclosure or destruction. Learner data must be stored only in approved systems or approved evidence folders.

Control area	Required standard
Access control	Access to learner data must be role-based. Staff should only access records needed for their work.
Passwords and accounts	Passwords must not be shared. Accounts must be individual, secure and disabled when no longer required.
Email and sharing	Personal data must be sent only where necessary, to the correct recipient, using approved email or secure sharing methods.
Portable devices	Learner data must not be stored on unencrypted USB devices or unapproved personal devices.
Hard-copy records	Paper records must be kept secure, not left unattended, and disposed of confidentially when no longer required.
Remote working	Staff must ensure screens are not visible to unauthorised people and must avoid discussing confidential learner information in public places.
System monitoring	System access and records may be checked for security, compliance, audit and quality assurance purposes.

16. Data Accuracy, Minimisation and Quality Assurance

Data quality is essential for funded programme compliance and learner support. Inaccurate data can affect eligibility, funding, learner support, safeguarding, achievement and progression evidence. Staff must ensure that learner records are accurate, complete and updated in a timely way.

- Learner contact details, attendance, employment status, LLDD/support information, assessment results and progression data must be checked and updated where required.
- Duplicate records, outdated forms and superseded evidence should not be retained in live learner files unless required for audit trail purposes.
- Leaders use learner file review, PICS reports, ILR reports, PDSATs, FIS, Power BI, FESIT and quality assurance activity to identify data quality risks.
- Where errors are found, the correction, owner and date should be recorded where appropriate.

17. Retention and Disposal

Personal data must be retained only for as long as required by law, funder requirements, audit rules, awarding body requirements, safeguarding requirements or legitimate organisational need. Where different retention periods apply, the longest required period should be followed unless there is a lawful reason to delete earlier.

Retention Standard

Funded learner records must be retained in line with the relevant funder contract, funding rules and audit requirements. Where a funder specifies a retention period, that requirement takes precedence over the general schedule in this policy.

18. Learner and Data Subject Rights

Learners and other data subjects have rights under UK data protection law. These rights are not absolute and may depend on the lawful basis for processing, the purpose of processing and whether retention is required for legal, safeguarding, funding or audit reasons.

Right	What this means
Right to be informed	Individuals should receive clear information about how their data is used.
Right of access	Individuals may request a copy of personal data held about them.
Right to rectification	Individuals may ask for inaccurate or incomplete data to be corrected.
Right to erasure	Individuals may ask for data to be deleted where there is no lawful reason to keep it. This may not apply where data is required for funding, legal, safeguarding or audit purposes.
Right to restrict processing	Individuals may ask for processing to be restricted in certain circumstances.
Right to object	Individuals may object to certain processing, particularly where based on legitimate interests.
Right to data portability	This may apply to certain information provided directly by the individual and processed by automated means.
Rights relating to automated decisions	Individuals have rights where decisions are made solely by automated processing and have legal or similarly significant effects.

19. Subject Access Requests and Complaints

Requests to access personal data must be passed promptly to the Director of Contracts & Operations or Quality & Compliance Lead. Staff must not ignore, delay or respond informally to a subject access request without checking the correct process. The organisation will respond within the statutory timescale unless an extension is permitted.

- Requests may be made verbally or in writing and do not have to mention “subject access request”.
- Identity must be verified before personal data is released.
- Information relating to other people must be reviewed and redacted where necessary.
- Safeguarding, legal privilege, management information or third-party information may require careful review before disclosure.
- Complaints about data handling should be sent to compliance@quackrecruitmentandtraining.co.uk Individuals may also complain to the Information Commissioner’s Office if they are dissatisfied.

20. Personal Data Breaches

A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending learner data to the wrong recipient, losing a learner file, unauthorised access to PICS, sharing confidential data on Teams incorrectly, or a cyber incident affecting learner information.

Step	Action required
1. Report immediately	Any suspected breach must be reported immediately to the Director of Contracts & Operations and Quality & Compliance Lead. Safeguarding-related breaches must also be escalated to the DSL.
2. Contain the breach	Take urgent steps to recover data, stop further disclosure, revoke access, delete wrongly sent information or secure affected systems.
3. Assess risk	Assess what data is involved, who is affected, likelihood of harm, potential impact and whether the ICO, funder or affected individuals need to be notified.
4. Record decision	Record the breach, decision-making, actions taken, notification decisions and learning points.
5. Improve controls	Use the incident to update training, systems, file checks, access controls or QIP actions where required.

21. Staff Training, Monitoring and Review

Staff who process learner or funded programme data must understand their responsibilities. Data protection expectations are reinforced through induction, policy access, staff communication, CPD, quality assurance activity and management oversight.

- All staff must read and comply with this policy.
- Staff must complete relevant data protection, information security, safeguarding and Prevent training according to role.
- Leaders will monitor compliance through learner file review, PICS checks, audit activity, data quality reports, quality assurance, staff meetings and QIP review.
- The policy will be reviewed by October 2026 and at least annually thereafter, or sooner where legislation, funder requirements, systems, delivery models or organisational responsibilities change.

Annex A: Funded Programme Data Map

Learner journey point	Data collected / processed	Main purpose	Typical evidence location
Application / enquiry	Name, contact details, programme interest, location, employment status, basic suitability information	Contact, suitability and recruitment into appropriate provision	CRM, enquiry form, email, PICS where applicable
IAG / suitability	Career goals, barriers, prior experience, support needs, digital access, English and maths confidence	Check suitability, identify support and ensure learner understands expectations	IAG record, PICS, learner file
Eligibility / enrolment	DOB, address, postcode, ID, eligibility declarations, employment status, prior learning, funding evidence	Confirm eligibility and create audit-ready learner record	Learner file, PICS, ILR-related records
Learning and review	Attendance, registers, ILP, SMART targets, skills scans, BKSB, workbooks, assessment preparation, feedback	Monitor progress, support learning and evidence distance travelled	PICS, learner file, BKSB, Teams/SharePoint, Highfield systems
Support / SEND / safeguarding	Support plans, reasonable adjustments, welfare notes, safeguarding/Prevent concerns, interventions	Support learners and keep learners safe	Confidential safeguarding records, support plans, PICS notes where appropriate
Achievement / assessment	Assessment results, IQA/EQA evidence, qualification outcomes, certificates	Confirm achievement and meet awarding body/funder requirements	Learner file, awarding body systems, IQA records
Progression / MS3	Employer contacts, interviews, job offers, employment evidence, payslips/contracts where required, follow-up notes	Support progression and evidence outcomes	Progression tracker, PICS, learner file, employer evidence folder

Annex B: Retention Schedule

Record type	Indicative retention standard
Funded learner eligibility, enrolment, attendance, assessment and progression evidence	Retain in line with relevant funder contract, funding rules and audit requirements; normally no less than the period required for funding audit and contract assurance.
ILR, PICS, Power BI, FESIT, PDSAT/FIS and performance records	Retain in line with funder, audit, quality assurance and organisational reporting requirements. Aggregated/anonymised data may be retained for longer where individuals are not identifiable.
Awarding body registration, assessment and IQA/EQA evidence	Retain in line with awarding body requirements and internal quality assurance policy.
Safeguarding and Prevent records	Retain securely in line with safeguarding policy, statutory expectations and risk-based decision-making. Access must be restricted.
SEND support plans and reasonable adjustment records	Retain as part of learner record where needed to evidence support, assessment access and quality assurance.
Complaints, appeals and malpractice records	Retain in line with relevant policy, awarding body requirements and legal/audit requirements.
Staff training, safer recruitment and compliance records	Retain in line with HR, safeguarding, safer recruitment, SCR and legal requirements.
Marketing consent, photographs, case studies and testimonials	Retain only while consent remains valid and the material remains in use, unless withdrawn earlier.

Annex C: Third-party Systems and Data Sharing

System / recipient	Data involved	Control expectation
PICS Learner Management System	Learner records, IAG, attendance, ILP, support, progression, audit evidence	Access controlled by role; records reviewed for accuracy and compliance.
BKSB	English and mathematics assessment and learning activity	Learner access controlled; progress used for support and teaching.
Highfield systems / Vault	Assessment, registration, portfolio, qualification and certificate evidence	Used in line with awarding body requirements and internal quality assurance.
Microsoft Teams, SharePoint and email	Online delivery, communication, learner records and staff collaboration	Approved channels only; access controls, secure sharing and confidentiality required.
Funders and public bodies	Eligibility, ILR/funding data, milestone evidence, outcomes, audit data	Shared only as required by contract, funding rules, audit or legal obligation.
Employers	Relevant learner progression information,	Only relevant data shared; sensitive data

System / recipient	Data involved	Control expectation
External reviewers, FIN/governance support, auditors	interview arrangements and feedback SAR/QIP, QA evidence, anonymised/limited learner evidence where possible	restricted unless lawful and appropriate. Share proportionately and securely; restrict sensitive data.

Annex D: Version Control

Version	Date	Author / owner	Description of changes	Next review
1.0	9 October 2024	Dion Bishop	Initial GDPR and Privacy Policy focused primarily on recruitment business activity.	9 October 2025
2.0	9 October 2025	Dion Bishop	Annual review. Funder feedback later identified that funded learner programme coverage and next review date required strengthening.	Superseded
3.0	June 2026	Dion Bishop	Major revision to align policy with funded training and learner provision. Added learner data map, funding and audit evidence, funder and awarding body sharing, safeguarding/Prevent information sharing, online systems, learner rights, breach process and training-specific retention schedule. Next review date updated to October 2026.	October 2026

Reference Guidance used for Policy Review: UK GDPR and Data Protection Act 2018 guidance from the Information Commissioner's Office, Prevent Duty statutory guidance and relevant funded programme/funder requirements.