your future your choice

POLICY

DATA PROTECTION, ICT SECURITY & ACCEPTABLE USAGE

REFERENCE	PPDPV2026AB 26
ISSUE DATE	30.04.26
REVIEW DATE	30.04.27

1. POLICY STATEMENT

Crosby Training is committed to protecting the personal data of learners, staff, contractors, partners, and other stakeholders. We will process personal data lawfully, fairly, transparently, and securely in accordance with UK GDPR, the Data Protection Act 2018, relevant ESFA requirements, and current Ofsted expectations.

This policy sets out the standards Crosby Training applies to data protection, ICT security, acceptable use, breach management, retention, and third-party processing. It should be read alongside the Safeguarding and Welfare Policy, AI Policy, and any staff code of conduct or disciplinary procedures.

2. SCOPE

This policy applies to all Crosby Training staff, volunteers, governors, contractors, agency workers, and any third party who processes personal data on behalf of Crosby Training. It applies to all information processed in paper, electronic, cloud-based, and verbal form, and to all devices, systems, and media used for work purposes.

3. LEGAL FRAMEWORK

This policy is informed by the following:

- UK GDPR and the Data Protection Act 2018.
- ICO guidance on data protection practice, including privacy notices, records of processing, DPIAs, and breach management.
- ESFA funding, audit, and record-keeping requirements.
- Ofsted privacy notice and data-handling expectations.
- Relevant cybersecurity good practice from the NCSC and other recognised standards.

4. DATA PROTECTION PRINCIPLES

Crosby Training will 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 kept up to date.
- Kept only for as long as necessary.
- Processed securely using appropriate technical and organisational measures.

Crosby Training will also ensure that individuals' rights are respected, including the rights of access, rectification, erasure, restriction, objection, and portability where applicable.

5. ROLES & RESPONSIBILITIES

The Governance & Leadership Team will provide oversight of compliance, approve this policy, and ensure appropriate resources are available. Senior leaders will implement the policy and monitor compliance across the organisation.

The DPO, or an appropriately designated data protection lead where a formal DPO is not legally required, will advise on compliance, monitor practice, support breach management, advise on DPIAs, and act as the point of contact for the ICO where required.

All staff are responsible for handling personal data safely, completing required training, using systems appropriately, and reporting concerns, breaches, or near misses immediately.

6. LAWFUL BASIS & SPECIAL CATEGORY DATA

Crosby Training will identify and document a lawful basis before processing personal data. The lawful basis will normally be based on contract, legal obligation, legitimate interests, vital interests, consent, or public task depending on the activity.

Special category data, such as health information, ethnicity, disability, or religion, will only be processed where a valid Article 9 condition applies and only where the processing is necessary and proportionate. Consent will not usually be relied upon as the default basis for special category processing, especially where there is a power imbalance or where another lawful basis is more appropriate.

7. PRIVACY NOTES & TRANSPARENCY

Crosby Training will provide clear privacy notices to learners, applicants, staff, contractors, and other relevant individuals at or before the point of collection, or within a reasonable period where this is not possible. Privacy notices will explain what data is collected, why it is collected, the lawful basis relied on, who it may be shared with, retention periods, rights, complaint routes, and contact details for the DPO or data protection lead.

Privacy notices will be reviewed whenever data use changes, systems change, or legal requirements are updated.

8. DATA COLLECTION & SHARING

Only data that is necessary for legitimate educational, contractual, regulatory, safeguarding, operational, or legal purposes will be collected. Personal data must not be reused for incompatible purposes without checking the lawful basis and transparency requirements first.

Information will only be shared with staff, partners, contractors, regulators, or service providers where there is a lawful basis, a legitimate need to know, and appropriate safeguards in place. Where external sharing is routine or high risk, it must be documented and approved through the relevant process.

9. RECORDS OF PROCESSING AND DPIAs

Crosby Training will maintain a Record of Processing Activities for the main categories of processing carried out by the organisation, including purpose, lawful basis, categories of data, recipients, transfers, retention, and security measures.

A Data Protection Impact Assessment must be completed before introducing any processing activity that is likely to result in high risk to individuals, including but not limited to new monitoring systems, CCTV changes, AI tools processing personal data, biometric systems, or new platforms involving sensitive data. The DPO or data protection lead will advise on whether a DPIA is required and how risks should be reduced.

10. DATA SECURITY & ICT CONTROLS

Crosby Training will apply appropriate security controls to all personal data and systems that store or process it. These controls will include:

- Strong passwords and multi-factor authentication where available.
- Encryption of portable devices and other devices carrying personal data.
- Access controls based on role and business need.
- Regular patching, antivirus protection, and secure configuration.
- Secure Wi-Fi, firewalls, and VPN use where remote access is permitted.
- Secure cloud services with appropriate contractual and technical safeguards.

Staff must not bypass security controls, share accounts, or use unauthorised devices or storage services to store work-related personal data.

11. ACCEPTABLE USE OF ICT

Devices, email, internet access, cloud services, and other ICT systems must be used lawfully, responsibly, and for legitimate work purposes. Staff must not access, store, create, or distribute illegal, harmful, abusive, offensive, or discriminatory content through Crosby Training systems.

Staff must keep credentials secure, lock devices when unattended, and report any lost device, suspicious message, malware alert, or unauthorised access immediately.

12. AI & DIGITAL TOOLS

Any use of AI tools or automated digital tools that may process personal data must comply with the Crosby Training AI Policy. Staff must not input personal, special category, confidential, or learner-identifiable data into AI systems unless the use has been approved, risk assessed, and governed by an appropriate lawful basis and contract or supplier assurance.

13. DATA SUBJECT RIGHTS

Crosby Training will respond to data subject rights requests in line with UK GDPR time limits and legal requirements. Requests may include access, rectification, erasure, restriction, objection, and portability where applicable.

Requests must be logged and forwarded promptly to the DPO or nominated data protection lead. Staff must not answer rights requests informally or delay passing them on. Where exemptions apply, Crosby Training will document the basis for relying on them and will provide the requester with a clear explanation where appropriate.

14. DATA BREACHES & INTERNAL MANAGEMENT

A personal data breach includes loss, unauthorised disclosure, unauthorised access, destruction, alteration, or unavailability of personal data. All suspected or actual breaches must be reported immediately to the DPO or nominated lead.

Crosby Training will assess each incident promptly, contain the issue, preserve evidence, record the facts, and decide whether the breach must be reported to the ICO within 72 hours of becoming aware of it where required. Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay.

All breaches, including those not reported to the ICO, will be logged and reviewed to identify lessons learned and corrective actions.

15. RETENTION & DISPOSAL

Personal data will only be kept for as long as necessary for the purposes for which it was collected, subject to legal, regulatory, contractual, audit, and safeguarding requirements.

Crosby Training will maintain a separate retention schedule that sets out the retention periods, disposal method, and justification for each record type. As a baseline:

- Learner records will normally be retained for 6 years after the end of the course, subject to any longer legal or safeguarding requirement.
- Staff records will normally be retained for 7 years after employment ends, subject to statutory, contractual, tax, or safeguarding requirements.
- Financial, audit, and compliance records will normally be retained for 6 years unless a longer period is required.
- Safeguarding-related records will be retained in line with safeguarding legislation, funding rules, and organisational policy.

Records must be securely destroyed or permanently deleted at the end of their retention period, and deletion must be suspended where a legal hold, investigation, complaint, or safeguarding matter is ongoing.

16. THIRD PARTY PROCESSORS & SUPPLIERS

Any third-party processor that handles personal data for Crosby Training must be subject to a written data processing agreement or equivalent contract terms. Contracts must address confidentiality, security, sub-processing, retention, breach notification, assistance with rights requests, and deletion or return of data at the end of the contract.

Crosby Training will carry out due diligence on suppliers handling personal data and will only use suppliers who can demonstrate appropriate security and compliance controls.

17. TRAINING & AWARENESS

All staff will complete data protection and ICT security training at induction and at least annually thereafter. Additional refresher training will be required where there are changes in law, systems, emerging risks, incidents, or high-risk processing.

Training will cover GDPR principles, phishing awareness, password security, breach reporting, privacy notices, records handling, AI use, and the secure sharing of information.

18. MONITORING & REVIEW

The DPO or data protection lead, together with senior leadership, will monitor compliance through training records, audits, incident reviews, spot checks, and process reviews. This policy will be reviewed annually or sooner if there is a material change in law, guidance, systems, operations, or risk.

19. SAFEGUARDING RESPONSIBILITIES

Where information relates to safeguarding, PREVENT, welfare, or a child or adult at risk, staff must follow the Safeguarding & Welfare Policy and any associated reporting procedures immediately. Data protection does not prevent lawful safeguarding disclosures where there is a legal basis or a serious risk of harm.