



Reviewer: Morné Du Toit
Version: 2
Review date: 11/02/2026
Next reviewed: 11/02/2027
Document Number: IT-016-R2

Public

Twin Protection of Personal Information (PPI) Policy

Applicability

This policy/procedure/process applies to all divisions, subsidiaries, departments, and associated organisations within Twin. It is binding on all employees, contractors, and stakeholders engaged in activities on behalf of Twin, regardless of business unit or location. All members of Twin are expected to adhere to the principles, standards, and requirements set out herein.

Archbury Holdings Limited has adopted the Protection of Personal Information Policy of Twin Training International Limited at acquisition of some of its subsidiaries. These policies remain in place until December 2026. Over this time Archbury Holdings Limited will review these arrangements and implement its own policy.

1. Purpose

Twin is committed to protecting personal information in accordance with the **UK General Data Protection Regulation (UK GDPR)**, the **EU General Data Protection Regulation (EU GDPR)** where applicable, the **UK and Irish Data Protection Acts 2018**, and **ISO 27001 standards**.

The policy provides a framework to manage and secure personal data across its lifecycle, from collection to disposal, thereby protecting the rights and privacy of individuals whose data we handle.

Twin has appointed a Data Protection Officer (DPO), responsible for overseeing compliance with data protection legislation, managing data protection risks, and acting as the primary contact point for data protection queries or complaints.

Data protection queries can be directed to:

Email: dataprotection@twingroup.org

2. Scope

This policy applies to all Twin employees, contractors, third-party vendors, and any other individuals who access, handle, or manage personal information collected, stored, processed, or transmitted by Twin. This includes both physical and electronic personal data assets.

This includes personal data relating to **learners, applicants, staff, contractors, partners, and other stakeholders involved in Twin's education, training, and employment services**.

3. Definitions

- **Personal Information:** Any information that can be used to identify an individual, such as name, address, identification number, email, or phone number.
- **Data Subject:** The individual whose personal information is being processed.



- **Data Processing:** Any operation or set of operations performed on personal data, including collection, storage, alteration, retrieval, or deletion.

4. Policy Objectives

- To ensure compliance with applicable data protection laws and ISO 27001 standards.
- To define roles and responsibilities for managing personal information.
- To protect personal data from unauthorized access, use, disclosure, alteration, or destruction.
- To establish a framework for responding to data breaches involving personal information.

5. Data Protection Principles

These seven data protection principles underpin the Twin execution of its data protection obligations:

5.1 Lawfulness, fairness and transparency

Twin will make all reasonable efforts to ensure that natural persons who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

5.2 Limitation of purpose.

Twin will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of and consents to any additional processing before it takes place.

5.3 Minimization of data

Twin will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

5.4 Data accuracy

Twin will review and update all data as required. It is the responsibility of the natural persons giving their personal data to ensure that this is accurate, and each individual should notify

Twin if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of Twin to ensure that any notification regarding the change is noted and acted on.

5.5 Limitations of storage

Twin undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Twin will operate defined data retention policies according to the types of information held and the purposes for which it is held.

Twin will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g., secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

5.6 Confidentiality and integrity of data

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. In most cases where no “hard” copy is required, personal data will be kept on Twin-specified systems with appropriate access rights implemented.

Twin will ensure that all personal data is accessible only to those who have a valid reason for using it.

5.7 Accountability

Twin is committed to putting in place the following appropriate technical and organisational measures that are fully compliant with UK GDPR:

- adopting and implementing a data protection policy
- taking a ‘data protection by design and default’ approach
- putting written contracts in place with organisations that process personal data on our behalf
- implementing appropriate security measures
- recording and, where necessary, reporting personal data breaches
- undertaking all necessary data subject protections and notifications relating to personal data breaches
- appointing a Data Protection Officer
- adhering to relevant codes of conduct

Twin will have in place appropriate security measures for personal data:



- Electronic security: where data is held electronically, it will be in systems compliant with contemporary electronic security standard with controlled access rights, hence capabilities
- Electronically held Data will be stored on Twin-provided or -approved cloud systems, not on Twin-owned personal terminals or non-Twin-owned devices like laptops and smartphones
- Where data is held physically or processed in open office, adherence is required to relevant codes of conduct, e.g., but not limited to
 - keeping all personal data in a lockable cabinet with key-controlled access.
 - password protecting personal data held electronically.
 - archiving personal data which are then kept securely (lockable cabinet).
 - placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
 - ensuring that PC screens are not left unattended without a password protected screen saver being used.

6. Data Collection and Consent

6.1 Data Minimization

Twin will only collect personal information that is necessary for legitimate business purposes and as required by applicable laws.

6.2 Legal Basis for Data Collection

Personal information will only be collected and processed where there is a lawful basis, such as consent, contractual necessity, legal obligation, or legitimate interest.

6.3 Consent Management

Where required, Twin will obtain clear, informed consent from data subjects prior to collecting or processing their personal information. Consent records will be maintained, and data subjects will have the right to withdraw consent at any time., with the proviso that this right may not be absolute if there are legal or contractual reasons for holding some personal data.

7. Data Use and Processing

7.1 Purpose Limitation

Personal information will only be used for the purpose for which it was collected, as defined in Twin's privacy notice or as agreed upon with the data subject.

7.2 Access Control

Access to personal information is restricted to authorized personnel only, based on the principle of least privilege and role-based access. Access permissions will be regularly reviewed to ensure compliance.

7.3 Data Anonymization and Pseudonymization

Where feasible, Twin will anonymize or pseudonymize personal information to minimize the risk to individuals' privacy in case of unauthorized access.

7. Data Storage and Retention

7.1 Secure Storage

All personal data will be stored securely, with access restricted to authorized personnel. Physical data storage will be protected by appropriate physical controls, while electronic data will be safeguarded through encryption, firewalls, and other relevant security measures.

7.2 Data Retention and Disposal

Personal information will only be retained for as long as necessary to fulfil the purposes for which it was collected or as required by law or public sector contract. When personal information is no longer needed, it will be securely disposed of in a manner that prevents recovery.

Learner records and assessment documentation will be retained in accordance with **regulatory and awarding body requirements**, including QQI retention requirements where applicable.

8. Data Protection by Design and Default

8.1 Data Protection Principles

Twin will integrate data protection principles into all systems and processes that handle personal information, ensuring privacy considerations are addressed from the outset.

8.2 Privacy Impact Assessments (PIAs)

A PIA will be conducted for any new project, process, or system involving personal information to assess and mitigate potential privacy risks.

8.3 Protection of learner assessment data

Twin ensures the confidentiality and integrity of learner assessment data, examination materials, results, and certification records through appropriate technical and organisational security measures.

9. Data Subject Rights

Twin recognizes and will uphold the following rights of data subjects, as applicable under relevant data protection laws:

- **Right to Access:** Data subjects have the right to access their personal information held by Twin.
- **Right to Rectification:** Data subjects can request correction of inaccurate or incomplete personal information.

- **Right to Erasure:** Data subjects can request the deletion of their personal information under certain conditions.
- **Right to Restrict Processing:** Data subjects can request limitations on the processing of their personal information.
- **Right to Data Portability:** Data subjects have the right to receive their data in a commonly used format and transmit it to another controller.
- **Right to Object:** Data subjects may object to processing based on legitimate interests or for direct marketing purposes.

Data subjects will be informed of these rights either before or at the point of the commencement of a course or programme with Twin. An enrolment form, or consent form, signed by the data subject, may be an appropriate instrument of assurance of compliance with this duty.

10. Data Breach Management

10.1 Incident Reporting and Response

All data breaches involving personal information must be reported immediately hours to the Information Security team, the Director of IT and the Data Protection Officer. Twin will have an incident response plan in place to promptly contain, investigate, and remediate any data breach.

10.2 Notification Requirements

In the event of a data breach involving personal information, Twin will notify affected data subjects and relevant regulatory authorities within 72 hours becoming aware of the breach, as required by law, providing details on the nature of the breach, potential risks, and mitigation steps, unless the breach is highly unlikely to result in a risk to the rights and freedom of individuals.

11. Third-Party Vendors and Data Processors

11.1 Vendor Due Diligence

Twin will conduct thorough due diligence on third-party vendors who process personal information on its behalf, ensuring they have adequate data protection policies measures in place.

11.2 Data Processing Agreements (DPAs)

All third-party vendors processing personal data on behalf of Twin must sign a DPA that includes obligations to protect personal information in line with Twin's standards, the GDPR and any other applicable laws.

11.3 Ongoing Monitoring

Twin will monitor third-party vendors to ensure continued compliance with data protection requirements, including regular audits and performance reviews.

12. Employee Responsibilities



Reviewer: Morné Du Toit
Version: 2
Review date: 11/02/2026
Next reviewed: 11/02/2027
Document Number: IT-016-R2

All employees and contractors of Twin who handle personal information must comply with this policy and complete regular data protection training. Non-compliance may result in disciplinary action, up to and including termination.

13. Policy Review and Compliance

This policy will be reviewed annually or as needed to reflect changes in data protection regulations, ISO 27001 standards, or Twin's business processes. Internal audits will be conducted periodically to assess compliance with this policy and to identify areas for improvement.

14. Compliance with ISO 27001

This policy forms part of Twin's Information Security Management System (ISMS) and is aligned with ISO 27001 standards, demonstrating our commitment to safeguarding personal information and ensuring information security best practices are maintained across the organization.