FUTURE CONNECT
TRAINING INSTITUTE

Produced by Abhishek Sharma, Director IT

Approved by Palwi Sood , Managing Director

Version date: 25/05/25 Version Number: FCT/DPP/15

Review schedule: 25/05/26 or in line with operating procedure requirements

Person/s responsible: SLT, all management and delivery staff

DPO : Umar Tariq

Signed Abhishek Sharma

Signed Palwi Sood

Policy owner: Abhishek Sharma

Future Connect Training & Recruitment Data Protection Policy

Table of Contents

Data Protection Statement of Intent

1. This policy applies to all employees (permanent and temporary), students, board members, contractors, and other users of Future Connect Training & Recruitment's personal data.
2. The Organisation processes personal and confidential data about its employees, students, employment applicants, board members, and clients. All individuals have a right to privacy under the Data Protection Laws. This policy sets out how Future Connect Training & Recruitment protects and promotes the rights of individuals and groups. It identifies the information that is to be treated as confidential and the procedures for collecting, storing, handling, and disclosing such information.
3. This policy will ensure that Future Connect Training & Recruitment complies with the fair processing code regarding the collection and use of the data collected.
4. This policy will ensure that all persons processing personal data on behalf of the Organisation receive adequate and periodical awareness training to ensure that they understand their contractual and legal responsibility towards the personal information they process in their daily work.
5. Where students are required to process the personal data of individuals as part of their course of study, specific awareness training will be provided as part of their course induction.
6. To ensure the effective application of the Principles of the Act, Future Connect Training & Recruitment will ensure that there is a nominated Data Protection Officer within the management structure with the specific responsibility for data protection.
7. The Organisation will ensure that management controls are in place to:
    - Maintain an accurate and up-to-date Notification of Processing Purposes.
    - Comply with the fair processing code regarding the collection and use of the data collected and ensure the methods for handling and managing personal information collected and processed by the Organisation are periodically reviewed.
    - Maintain the quality and accuracy of data held and processed.
    - Review the retention periods for which data is reasonably retained.
    - Fully meet the rights of the data subject regarding data held and processed by the Organisation.
    - Take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and accidental loss, destruction, or damage.
    - Protect personal data from transfer outside of the EEA or, where such transfer is necessary, provide adequate security of the information.

1. Introduction

Future Connect Training & Recruitment, as a Data Controller, needs to process certain information, including personal information, about its employees, students, and other persons to operate effectively and efficiently. This includes:

- Monitoring performance, achievements, and health and safety.
- Recruitment and payroll processing.
- Organising courses and training sessions.
- Complying with legal obligations to funding bodies and government

regulations. To comply with the Data Protection Laws, personal information must be:

- Processed fairly, lawfully, and transparently.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary for the purposes for which it is being processed.
- Accurate and kept up to date, ensuring that inaccurate personal data is erased or rectified as soon as possible.
- Retained for no longer than necessary.
- Processed securely, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, using appropriate technical or organisational measures.

These principles are further expanded upon throughout this policy.

All staff and users of personal information must adhere to these principles. This Data Protection Policy ensures compliance with relevant legislation.

2. Status of the Policy

2.1 Employment Condition

This policy is a condition of employment. Staff must adhere to the rules and policies set forth by Future Connect Training & Recruitment. Failure to comply may lead to disciplinary action.

2.2 Reporting Policy Violations

If a member of staff believes that the Data Protection Policy has not been followed regarding their personal data or that of others, they should report it to the Director of Risk, Control, and Compliance or Legal Counsel. If the issue is unresolved, the matter may be escalated through the grievance procedure, which can be accessed via internal HR documentation.

2.3 Student Data Concerns

Students who believe their personal data has been mishandled should first raise the matter with their Course Tutor. If the issue remains unresolved, they may escalate their concerns to the Director of Risk, Control, and Compliance or the Legal Counsel for further review.

3. The Data Controller, the Data Protection Officer, and Assistant Data Protection Officers

3.1 Organisational Responsibility

Future Connect Training & Recruitment, as a body corporate, is the Data Controller under the Act and is ultimately responsible for its implementation. However, the designated Data Protection Officer (DPO) and Deputy Data Protection Officers manage daily data protection operations.

3.2 Data Protection Officer (DPO)

The Director of Corporate Governance, Risk, and Compliance serves as the Data Protection Officer (DPO) and is responsible for:

- Informing and advising the Data Controller, processors, and employees about their legal obligations under data protection laws.
- Monitoring compliance with UK GDPR, Data Protection Act 2018, and internal policies, including responsibility assignments, staff training, and internal audits.
- Providing guidance on Data Protection Impact Assessments (DPIAs) and ensuring compliance with Article 35 of UK GDPR.
- Cooperating with the Information Commissioner's Office (ICO) and acting as the main contact for supervisory authorities.
- Handling and advising on data processing risks, ensuring accountability, and implementing privacy-by-design principles.

3.3 Deputy Data Protection Officers

The **Deputy Data Protection Officers** ensure compliance within their specific operational areas. These officers include:

- Managing Director
- Compliance & Risk Manager
- Head of IT Security
- HR Manager
- Finance Director
- Head of Training & Recruitment Operations
- Head of Marketing & Communications

Each **Deputy Data Protection Officer** is responsible for ensuring that data protection regulations and security measures are followed within their areas of responsibility.

4. Basis for Processing Personal Data

4.1 Lawful Processing

Before processing personal data, Future Connect Training & Recruitment will:

1. Assess the processing purpose and determine the most appropriate lawful basis for processing.
2. Ensure compliance with at least one of the six lawful bases under UK GDPR:

- Consent: The data subject has given explicit consent for specific processing.
- Contractual Necessity: Processing is necessary for the performance of a contract.
- Legal Obligation: Processing is necessary to comply with legal obligations.
- Vital Interests: Processing is necessary to protect the life of an individual.
- Public Task: Processing is required to carry out a task in the public interest.
- Legitimate Interests: Processing is required for legitimate business operations, provided that it does not override individuals' fundamental rights and freedoms.

4.2 Documentation & Transparency

- Maintain records documenting the lawful basis for processing activities.
- Ensure all privacy notices clearly explain why and how data is being processed.
- For sensitive personal data, establish a specific lawful condition under UK GDPR Article 9 (e.g., explicit consent, employment law obligations, or public interest requirements).

5. Sensitive Personal Data

5.1 Definition

Sensitive personal data includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Data concerning health or sex life and sexual orientation
- Genetic data or biometric data

5.2 Processing Conditions

Future Connect Training & Recruitment may process sensitive personal data only when:

1. A lawful basis exists (as outlined in Section 4.1.5 above); and
2. One of the following special conditions applies:

- The data subject has given explicit consent.
- Processing is necessary to exercise employment law rights or obligations.
- Processing is required to protect the data subject’s vital interests, and the individual is incapable of giving consent.

- The data has been manifestly made public by the data subject.
- Processing is necessary for legal claims or defence.
- Processing is necessary for substantial public interest reasons.

5.3 Access to Sensitive Data

- Sensitive personal data will be restricted to personnel on a need-to-know basis.
- Measures will be taken to ensure secure handling, storage, and access controls for sensitive data.
- Any breaches or concerns regarding sensitive data processing must be reported to the Data Protection Officer (DPO) immediately.

6. Data Privacy Impact Assessments ('DPIAs')

6.1 Assessment Process

When processing is likely to result in a high risk to an individual's data protection rights (e.g., introducing a new technology or system), Future Connect Training & Recruitment will conduct a DPIA (Data Privacy Impact Assessment) before processing begins. The assessment will evaluate:

- Whether the processing is **necessary and proportionate** to its intended purpose.
- The **potential risks** to individuals.
- **Mitigation measures** to address risks and protect personal data.

6.2 Approval & Oversight

- All DPIAs must be reviewed and approved by the Data Protection Officer (DPO).
- DPIAs will be conducted in collaboration with relevant stakeholders to ensure compliance.

7. Individual Rights

7.1 Data Subject Rights

All staff, students, and other users (collectively referred to as data subjects) are entitled to:

- Know what information is held about them and how it is processed.
- Request access to their data (see Section 8).
- Update or correct inaccurate personal data.
- Request erasure of data when it is no longer necessary for its original purpose or where no overriding legitimate grounds exist (also known as the right to be forgotten).
- Restrict processing under certain conditions, such as if the accuracy of data is contested or if processing is unlawful but the data subject does not want the data erased.
- Object to processing when data is used for direct marketing or other legitimate interest-based processing.
- Understand what measures Future Connect Training & Recruitment is taking to comply with UK GDPR and data protection laws.

7.2 Privacy Policies

Future Connect Training & Recruitment maintains the following privacy policies:

- **General Privacy Policy**
- **Privacy Policy – Students**
- **Privacy Policy – Staff**
- **Privacy Policy – Clients**

These policies provide details on how individuals can exercise their rights. In most cases, individuals are advised to contact the **Data Protection Officer (DPO)** for further assistance.

8. Individual Obligations

8.1 Staff Responsibilities

All staff members must:

- Regularly check and update the personal information held by Future Connect Training & Recruitment.
- Inform the Organisation of any changes in their personal data (e.g., change of address or banking details).
- Notify the Organisation of any inaccuracies in the data provided to ensure compliance.

8.2 Handling Personal Data

Staff members who have **access to personal data** of other staff, students, or clients must:

- Only access personal data for authorised purposes.
- Ensure data is shared only with those who have proper authorisation.
- Follow all data protection procedures to prevent unauthorised access or leaks.

8.3 Data Collection & Approval

- Any data collection forms (e.g., staff applications, student enrolment forms) must be approved by the Data Protection Officer (DPO).
- Data collected must be relevant to its intended purpose and not excessive.

8.4 Local Data Processing Restrictions

- Data collected centrally must **not be used** to create local reporting systems unless approved by the **DPO**.
- Any **new data reporting systems** must be developed in collaboration with **IT and the Data Protection Officer** to ensure compliance with data security policies.

8.5 Reporting Data Protection Concerns

Staff should **immediately report** any concerns or suspected violations, including:

- Processing of personal data without a lawful basis.

- Unauthorised access to personal data.
- Data loss, deletion, or inadequate security measures.
- Improper removal of personal data or devices containing personal data.
- Any breach of data protection laws or this policy.

Concerns should be reported to the **Data Protection Officer (DPO)** for further investigation and corrective action.

9. Data Security

Future Connect Training & Recruitment takes information security very seriously and has security measures in place to prevent unauthorised processing, accidental loss, destruction, or damage to personal data. The Organisation follows strict security protocols and technological safeguards to protect data from collection to destruction.

9.1 Staff Responsibilities

All staff members are responsible for ensuring that:

- Any personal data they hold is stored securely.
- Personal data is not disclosed to unauthorised parties either orally, in writing, or by accident.
- Unauthorised disclosure of personal data will be treated as a disciplinary offence, which in severe cases, may be considered gross misconduct.

9.2 Secure Storage of Hard Copy Data

Future Connect Training & Recruitment enforces a Clear Desk Policy, meaning all manual/hard copy personal information must be:

- Stored in a locked filing cabinet when not in use.
- Kept in a locked drawer when unattended.
- Offices should be locked when unoccupied to prevent unauthorised access.

9.3 Protection of Computerised Data

All computerised personal data must be:

- Password protected within the Organisation's secure file storage network.
- Not stored on unauthorised cloud services without prior approval.
- Encrypted if stored on portable devices (e.g., USB drives, external hard drives, laptops).

Future Connect Training & Recruitment provides access to a **secure virtual desktop system**, making external cloud storage unnecessary. Where justified, only **encrypted** USB storage may be used, and encrypted USB devices can be requested from IT Services.

Additionally, all staff members must follow:

- The IT Security Policy
- The Mobile Devices & Remote Access Policy
- The Acceptable Use Policy

9.4 Restriction on Removing Data

- Staff must not take electronic personal data off-site unless specifically authorised and adequately protected.
- Physical documents containing personal data must not be removed from the Organisation's premises without approval.

9.5 Data Sharing & Transfers

When transferring personal data to external organisations (such as funding bodies or auditors):

- Data must be encrypted.
- Secure transfer protocols must be approved by the Data Protection Officer (DPO) and the IT Services Manager.
- Where necessary, a Data Sharing Agreement must be in place before sharing any personal data.

If there is any uncertainty, staff must contact the Data Protection Officer (DPO) or Legal Counsel before sharing data externally.

9.6 Use of Cloud Storage & Externally Hosted Systems

- Future Connect Training & Recruitment may use **externally hosted systems** (cloud-based platforms) to support staff and learners.
- Any new cloud-based systems must be approved by management after verifying data protection and security compliance with third-party providers.

All staff members should refer to the Guidance on Externally Hosted Services and the Externally Hosted Services Checklist before engaging in cloud-based data processing.

9.7 Prohibited Data Practices

- Staff must not use personal emails for storing or transferring high-risk data.
- Personal cloud storage services (e.g., Google Drive, Dropbox, iCloud) must not be used to store organisational data unless explicitly authorised.
- All personal data must be handled strictly within Future Connect Training & Recruitment's approved storage and transfer systems.

10. Data Breach & Incident Management

10.1 Types of Data Breaches

A data breach can take many forms, including:

- **Loss or theft** of data or equipment containing personal data.
- **Unauthorised access** to or misuse of personal data by staff or third parties.
- **System failures** leading to the loss of data.
- **Human errors**, such as accidental deletion or alteration of data.
- **Unforeseen incidents**, including fire, flood, or other disasters affecting data storage.
- **Cybersecurity threats**, such as hacking, phishing scams, and malware attacks.
- **Deception-based breaches**, where an entity is tricked into disclosing personal data.

10.2 Reporting a Data Breach

If personal data is lost, stolen, or compromised, the incident **must** be reported immediately to:

- The **Data Protection Officer (DPO)**
- The **Legal Counsel**
- The **Director of IT**

Future Connect Training & Recruitment has established Incident Management Procedures to address breaches effectively.

10.3 Organisational Response to Data Breaches

- Future Connect Training & Recruitment will:
- Investigate all actual or suspected data security breaches.
- Determine whether notification to the Information Commissioner's Office (ICO) is required.
- The ICO provides a self-assessment tool for determining breach notification requirements: ICO Reporting a Breach
- If a breach is likely to result in a risk to individual rights and freedoms, the ICO will be notified within 72 hours.
- Notify affected individuals where the breach poses a high risk to their rights and freedoms.
- Notify senior management in the event of a major breach.

10.4 Maintaining a Data Breach Log

A **central log** is maintained for:

- All reported data breaches
- Actions taken in response to each incident
- Data subject requests for information held by the Organisation

This log is regularly reviewed to identify trends and improve security measures.

11. Student Obligations

11.1 Accuracy of Personal Data

Students must ensure that all personal data provided to Future Connect Training & Recruitment is **accurate and up to date**. Any changes (e.g., address updates) must be **submitted in writing** using the appropriate forms.

11.2 Processing Personal Data for Learning Purposes

Students may process personal data as part of their coursework or practical learning experiences. When doing so, students must:

- Follow departmental protocols regarding data collection and processing.
- Use data solely for learning and educational purposes.

- Notify their course tutor if they have concerns about their data processing responsibilities.

11.3 Students Handling Client Data

Students on **practical courses** that require handling client personal data will be provided with training during their **course induction**. They must also adhere to:

- Future Connect Training & Recruitment's data protection policies.
- Guidelines for Students, available in Appendix 2 of this policy.

12. Rights to Gain Access to Information

12.1 Accessing Personal Data

All staff, students, and other data subjects have the right to access their personal data held by Future Connect Training & Recruitment, whether stored digitally or physically. The Organisation's **Privacy Policies** outline the types of data held, how they are processed, and the lawful reasons for processing.

Requests for access should be submitted to the **Data Protection Officer (DPO)** via [Insert Contact Email].

12.2 Response Timeline

Future Connect Training & Recruitment will respond to data access requests within one month, in accordance with statutory deadlines.

13. Publication of Organisational Information

13.1 Publicly Available Information

Future Connect Training & Recruitment follows an approved **Publication Scheme**, ensuring that certain organisational information is available to the public, including:

- Names of key staff and management
- Organisational governance and leadership structures
- Official photographs of key staff (where applicable)
- Registers of interests for key personnel
- Information included in policy statements related to **access to information**

If any individual objects to their personal data being made public, they should contact the **Data Protection Officer (DPO).**

Internal phone and email address lists will not be made publicly available.

14. Data Subject Information Requests

14.1 Handling Requests for Personal Data

All requests for access to personal data by staff, students, or external individuals must be referred immediately to the Data Protection Officer (DPO) or Legal Counsel.

14.2 Third-Party Requests

Requests from external parties can only be approved if they meet UK GDPR legal requirements. If the request falls under non-disclosure exemptions, data may be shared only when legally required. In all cases, requests must be assessed by the DPO, Legal Counsel, or senior management.

15. Examination Marks

15.1 Student Access to Marks

Students have the right to access their examination and coursework marks. Requests for examination marks should be directed to the Data Protection Officer (DPO) and will be processed within one month from the request date or the date of official mark release.

Note: Students do not have the right to access their examination scripts, but examiner comments on the scripts are disclosable upon request.

16. Retention of Data

Future Connect Training & Recruitment follows a **Data Retention, Archiving, and Disposal Policy** that outlines specific retention periods for different types of personal data.

17. Transferring of Personal or Sensitive Data via Email

17.1 Secure Communication

Staff must **not** use external email services for transmitting personal or sensitive data. When sending such data to a third party, it must be:

- Sent via a secure portal
- Encrypted or password-protected

If unsure, staff must seek advice from the **ICT Services Manager** or **DPO.**

17.2 Accountability of Email Usage

All emails sent from Future Connect Training & Recruitment accounts **are the responsibility of the account holder**.

Further compliance guidance is available in the:

- IT Security Policy
- Acceptable Use Policy
- Mobile Devices & Remote Access Policy

18. Transferring of Personal or Sensitive Data Outside of the EEA

18.1 Restriction on International Transfers

Personal data must not be transferred outside the EEA unless the country is:

- Listed as adequate under UK GDPR regulations.
- Subject to specific safeguards (e.g., Standard Contractual Clauses or Binding Corporate Rules).

This includes:

- Email transmissions
- Cloud storage and backups
- Publishing personal data on the Organisation's website or social media

If international data transfer is necessary, prior approval from the **Data Protection Officer (DPO)** is required.

19. Automated Decision Making and Profiling

19.1 Understanding Automated Decision Making and Profiling

Under **UK GDPR**, there are strict controls on **profiling and automated decision-making** concerning individuals:

- Automated Decision Making: This occurs when an organisation makes a decision solely through automated processes (without human involvement), which has a legal or significant impact on an individual.
- Profiling: This involves automated processing of personal data to evaluate specific attributes about an individual (e.g., behaviour, interests, or preferences).

19.2 Future Connect Training & Recruitment's Approach

- Future Connect Training & Recruitment does not carry out Automated Decision Making that has a legal or significant impact on individuals.
- The Organisation may use profiling techniques to enhance student performance, attendance tracking, and engagement monitoring. This is done responsibly and does not impact an individual's legal rights.

If automated decision-making or profiling is introduced in the future, appropriate impact assessments and compliance measures will be undertaken.

20. Compliance with the Policy

20.1 Responsibilities of Staff and Students

Compliance with UK GDPR and Data Protection Laws is the responsibility of everyone who processes personal information on behalf of Future Connect Training & Recruitment, including:

- Staff (permanent, temporary, and contractors)
- Students (where applicable to their studies or training)

20.2 Consequences of Non-Compliance

A deliberate breach of this policy may result in:

- Disciplinary action, including termination of employment.
- Withdrawal of access to IT systems and organisational facilities.
- Legal consequences, including potential prosecution and fines.

20.3 Questions & Concerns

For any questions regarding the interpretation or implementation of this policy, staff and students should contact:

- Data Protection Officer (DPO)
- Legal Counsel

The Organisation remains committed to ensuring compliance with data protection laws and safeguarding personal information at all times.