DataProtectionPolicy

Document Version Control			
Document Version	**Date**	**Policy Reviewed by**	**Review Date**
Version 2.0	03/03/2025	Shahin Reza	01/03/2026

School of Commerce & Technology (SCT)

March 2025

1. Introduction

In order to operate effectively and fulfill its legal obligations, the School of Commerce and Technology (SCT) must collect, maintain, and use certain personal information about current, past, and prospective employees, students, customers, suppliers, and other individuals with whom it has dealings.

All such personal information, whether held on computer, paper, or other media, will be obtained, handled, processed, transported, and stored lawfully and correctly in accordance with the safeguards contained in the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) 2018.

2. Data Protection Principles

SCT is committed to adhering to the eight principles of data protection. These principles require that personal information must:

- Be fairly and lawfully processed, and not processed unless specific conditions are met.
- Be obtained for one or more specified, lawful purposes, and not processed in any manner incompatible with those purposes.
- Be adequate, relevant, and not excessive for the intended purposes.
- Be accurate and, where necessary, kept up to date.
- Not be kept for longer than necessary.
- Be processed in accordance with the data subject's rights.
- Be kept secure from unauthorised or unlawful processing, and protected against accidental loss, destruction, or damage.
- Not be transferred to countries outside the European Economic Area (EEA) unless the country or territory ensures adequate protection for the rights and freedoms of data subjects.

3. Compliance

To ensure compliance with these principles, SCT will:

- Fully observe all conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or comply with legal obligations.
- Ensure the quality of the personal information used.
- Apply strict checks to determine the duration personal information is retained.
- Ensure individuals about whom information is held are able to exercise their rights under the DPA and GDPR, including:
    - The right to be informed that processing is taking place;
    - The right of access to their personal information;
    - The right to prevent processing in certain circumstances;
    - The right to correct, rectify, block, or erase incorrect information.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred outside the EEA without suitable safeguards.

4. Responsibilities

- **Chief Executive Officer**: Overall responsibility for ensuring that SCT complies with its data protection obligations rests with the Chief Executive Officer.

- **Employees**: All employees are responsible for ensuring that the personal information they provide to SCT (e.g. current address) is accurate and up to date. Employees must notify SCT immediately of any changes.
- Employees involved in the collection, maintenance, and processing of personal information are required to follow SCT's data protection guidelines and best practices, as communicated by management from time to time.

5. Employee Information

SCT holds the following personal information about its employees for payroll and administrative purposes:

- Name
- Address
- Salary
- Partner's Name
- Telephone Numbers
- National Insurance Number
- Previous Employment Details
- References

Sensitive personal information held may include:

- Racial or ethnic origin
- Physical or mental health conditions
- DBS check (formerly CRB)
- Passport copies
- Immigration/visa documentation

This sensitive data is used for purposes such as Equal Opportunities and Health and Safety monitoring.

6. Access to Information

Any individual whose personal information is held by SCT has the right to make a **Subject Access Request**. Employees wishing to exercise this right should write to the Chief Executive Officer.

SCT reserves the right to charge a £25 fee for processing such requests. If any personal information is found to be incorrect, it will be amended promptly. SCT aims to respond to all subject access requests within 40 days. In cases of delay, the individual will be informed accordingly.

7. IT Communications and Monitoring

SCT provides employees with access to computer facilities for work and communication purposes. To ensure compliance with data protection, information security, and relevant laws, SCT has adopted an **IT Communications and Monitoring Policy**, which should be read in conjunction with this Data Protection Policy.

8. Breach of Policy

Any breach of this policy will be regarded as a **disciplinary offence** and will be dealt with in accordance with SCT's formal **Disciplinary Procedure**.

Employees who believe there has been a breach of this policy in relation to their personal data should raise the matter through SCT's formal **Grievance Procedure**.