School of Coding & AI

Student First Always

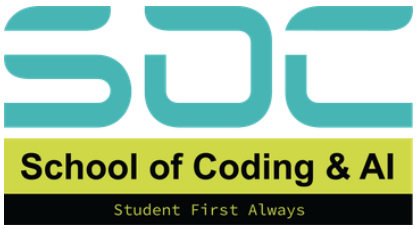
HIGHER EDUCATION

IT and Cybersecurity Policy

Policy Owner: Suki Gill

Full Name	Position	Signature	Date	Review Cycle
Suki Gill	Principal	SGill	01.09.2025	Annual

School of Coding Limited T/A School of Coding & AI
Company Number: **10808021 Registered in England & Wales**
Registered Address: **Unit 8-8b, Newton Court, Westrand, Pendeford Business Park, Wolverhampton, WV9 5HB**



1. Introduction

School of Coding & AI HE is committed to protecting the confidentiality, integrity, and availability of its IT systems and data. This policy sets forth guidelines on acceptable use, cybersecurity protocols, and data breach response to ensure compliance with relevant UK laws, legislations, and information security standards.

2. Relevant Laws and Legislations

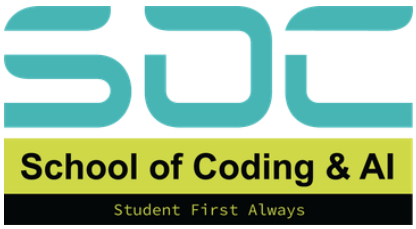
This policy adheres to the following UK laws and regulations:

- **Data Protection Act 2018**: Governs the protection of personal data and aligns with the General Data Protection Regulation (GDPR).
- **Computer Misuse Act 1990**: Addresses unauthorised access to computer systems and related offences.
- **Regulation of Investigatory Powers Act 2000 (RIPA)**: Governs the lawful interception of communications.
- **The Privacy and Electronic Communications Regulations (PECR) 2003**: Covers privacy in electronic communications.
- **Freedom of Information Act 2000**: Governs access to information held by public authorities.
- **UK General Data Protection Regulation (UK GDPR)**: Provides a framework for data processing, ensuring data is used fairly, lawfully, and transparently.

3. Acceptable Use

This section defines the proper use of School of Coding & AI HE IT resources, including hardware, software, internet access, and communication tools.

- Internet Usage: Internet access must be used for legitimate work purposes. Personal use should be limited and must not interfere with job responsibilities. Accessing inappropriate content, such as illegal or offensive material, is strictly prohibited.
- Email: Email accounts provided by School of Coding & AI HE must be used for official communications. Personal use is discouraged, and any misuse, including sending malicious attachments or phishing, will be treated as a violation of this policy.
- Social Media: Employees are expected to use social media responsibly. Any posts, comments, or actions that may damage the Institute's reputation, reveal confidential information, or breach the privacy of individuals are forbidden.
- Personal Devices: Employees using personal devices to access School of Coding & AI HE data must ensure the devices are secured with appropriate safeguards, such as strong passwords and encryption.



4. Cybersecurity Protocols

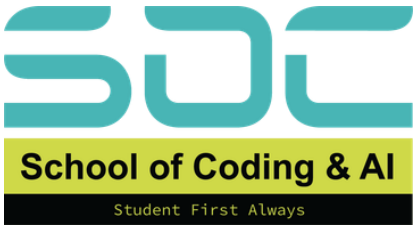
School of Coding & AI HE has implemented a range of cybersecurity measures to protect its IT infrastructure and data.

- **Firewalls and Intrusion Detection**: Firewalls and intrusion detection systems (IDS) are in place to monitor and control network traffic and detect potential threats.
- **Antivirus and Anti-Malware**: All computers must have up-to-date antivirus and anti-malware software installed. Regular scans will be conducted to detect and remove any malicious software.
- **Regular Software Updates**: Employees are required to install updates for operating systems and applications promptly. School of Coding & AI HE IT staff will ensure that critical updates and patches are applied regularly.
- **Password Management**: All users must create strong passwords and change them regularly. Passwords should not be shared or reused across multiple accounts.
- **Two-Factor Authentication (2FA)**: Where applicable, 2FA will be enforced for accessing critical systems and data to provide an additional layer of security.
- **Encryption**: Sensitive data, whether stored or transmitted, must be encrypted to protect against unauthorised access.
- **User Access Controls**: Access to IT systems and data is based on role-specific needs. Employees must not access, share, or modify information unless they have proper authorisation.

5. Data Breach Response

In the event of a data breach, School of Coding & AI HE has established a formal response procedure to mitigate the impact and ensure compliance with legal requirements.

- Breach Detection and Reporting: All employees must report any suspected or confirmed data breaches to the IT Security Officer immediately. Detection measures, including monitoring tools, will be in place to identify breaches.
- Investigation and Containment: Upon receiving a breach report, the IT Security Officer will initiate an investigation to determine the cause, scope, and severity of the breach. Immediate steps will be taken to contain the breach and prevent further unauthorised access.
- Notification Procedures: If the breach involves personal data, affected individuals will be notified without undue delay, as required by the Data Protection Act 2018 and GDPR. The Information Commissioner's Office (ICO) will also be informed within 72 hours of discovery if the breach poses significant risks.
- Corrective Measures: Following the breach, remedial actions will be taken, such as updating security controls, reviewing access policies, and providing staff with additional training to prevent future breaches.



- Incident Review and Documentation: A full review of the incident will be conducted to assess what went wrong and how it can be prevented in the future. Detailed records of the breach and subsequent actions will be maintained in accordance with regulatory requirements.

6. Compliance and Enforcement
Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, as well as legal action. All employees are expected to review and understand this policy, and periodic training will be provided to ensure ongoing compliance with IT and cybersecurity requirements.

7. Review and Updates
This policy will be reviewed annually or whenever there are significant changes to IT infrastructure, legal requirements, or security threats.

This policy ensures School of Coding & AI HE remains compliant with all relevant legislation while maintaining a secure and efficient IT environment.