Stanfords
Training Ltd

Policy Title:	Information Security
Policy Description	The objectives of this policy are to ensure that all of the Company's computing facilities, programs, data, network, telecommunications, CCTV and equipment are adequately protected against loss, misuse or abuse. Also to ensure that all users are aware of and comply with this policy and that all users are aware of and comply with the relevant UK legislation.
Approved By:	Stanfords Training Management
Policy Owner:	Stanfords Training Ltd
Date Issued: Policy Review Date	01/11/2025 31/10/2026

1. Background & Context

Information systems are critical in supporting business and activities. The availability, confidentiality and use of information systems is fundamental to the success of the company. The integrity of data within those systems is also key.

Stanfords Training Ltd aims to ensure appropriate availability, confidentiality and use of information systems and data by operating in compliance with relevant legislation alongside related company policies.

The objectives of this policy are to:

i. ensures that all of the company's computing facilities, programs, data, network, telecommunications, CCTV and equipment are adequately protected against loss, misuse or abuse.
ii. ensure that all users are aware of and comply with this policy.
iii. ensure that all users are aware of and comply with the relevant UK legislation.
iv. ensure that users understand their own responsibilities for appropriate use and protection of any systems or data they have access to.
v. ensure that users comply with the Prevent duty guidance in relation to counter terrorism and the prevention of radicalisation

2. Ownership

The company Management Team (MT) is responsible for approving Information Security (IS) policies.

The IT Manager is responsible for managing the company network and Internet access and for providing support and advice in relation to the network and resources.

The company Data Protection Officer is responsible for advising with respect to overall compliance with the Data Protection and Freedom of Information Acts.

However, it is the responsibility of each individual to ensure his/her understanding of and compliance with this policy.

3. Authority & Scope of this Policy

The Information Security policy applies to all staff, learners and partners/clients of the company as well as any third party authorised by the company to access its information systems or data. They relate to the use of:

> Any facilities owned, leased, rented or on-loan by the company including data processed using those facilities which is protected by the terms of the Data Protection Act.
>
> Any systems or resources connected to the company network directly or indirectly at any time.

Any company-owned/licensed data or programs, be they on company or on private systems.

Any data or programs provided to the company by sponsors or external agencies. This policy will be reviewed annually and revised according to:

- Developments in systems & ICT.
- Amendments to legislation.

4. Responsibilities for Information Security

The Managing Director has overall responsibility for information security and compliance with UK GDPR and this policy.

The Data Protection Officer (DPO) oversees data-protection compliance, maintains the Record of Processing Activities, and manages data-breach reporting to the ICO within 72 hours where required.

All staff and contractors must follow this policy, complete regular data-protection training, and report any actual or suspected breaches immediately to the DPO or IT Manager.

Data Breach Management
Any suspected or actual data breach (loss, unauthorised disclosure, or access) must be reported immediately to the DPO.
The DPO will:

- Record the breach in the incident log;
- Assess the risk to individuals;
- Notify the Information Commissioner's Office (ICO) within 72 hours, where required; and
- Notify affected individuals if there is a high risk to their rights and freedoms.
  Breach-management outcomes will be reviewed and used to improve security controls.

5. Systems & Processes

5.1 Compliance with Legislation

This policy operates in accordance with the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Investigatory Powers Act 2016 and Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Freedom of Information Act 2000 (where applicable)

- Communications Act 2003
- Guidance from the Information Commissioner’s Office (ICO)
- JCQ and awarding-body security requirements for assessment materials

All users must comply with the abovementioned legislation, and any individual can be held personally responsible for any breach of the legislation.

In order to comply with the Data Protection Act, Stanford Training is registered with the Information Commissioner’s office as a Data Controller. In accordance with the Act, the company has notified the Information Commissioner regarding its use of various types of data.

5.2 Acceptable Use of Resources/Systems

Information systems and resources are made available to company staff for use in relation to their work. It is accepted that reasonable personal use of these systems and resources may be made outside of working periods. Any such use of company information systems, including e-mail, internet, online social networking media and any related systems or resources, must be made with due respect to others at all times.

No information which may be considered inappropriate or defamatory may be composed, published or transmitted using company systems or resources. Any such inappropriate conduct or misuse of company systems will be deemed a disciplinary matter.

The Acceptable Use of IT Student, The Acceptable Use of Internet/Intranet for Staff and Contract Personnel and Social Media policies for both staff and students can be found on the company intranet.

5.3 Monitoring of Electronic Systems & Communications

Company-provided Internet/Intranet and email privileges are company resources and, as such, may be monitored for unusual activity. Correspondence via email cannot be guaranteed to be private and, hence, confidential correspondence should be sent by other means than via company systems. The distribution of information using any company-provided systems is subject to scrutiny and the company reserves the right to determine the suitability of information being transmitted.

All confidential data sent by email must be transmitted using secure methods, such as encryption or password-protected attachments, and shared only with verified recipients. Staff must not use personal email accounts for company business.

Stanfords Training may monitor systems, networks, and premises for legitimate business and security purposes in line with the Investigatory Powers Act 2016 and Regulation of Investigatory Powers Act 2000. CCTV and system monitoring must be proportionate, transparent, and subject to documented privacy impact assessments.

In addition, telephone communication and CCTV may be monitored in connection with:

- crime prevention or detection.
- the apprehension and prosecution of offenders.
- ensuring compliance with legislation.
- ensuring compliance with company policies, procedures, codes of practice and values.

5.4 Physical Security

Physical security is the first line of defence in information security. There is no value in storing information securely on a computer if the original information is left on a desk in an unlocked room. Whilst it is not always possible to operate a clear desk policy, original documentation or printouts should be securely stored when not in use.

All documentation containing confidential information should be destroyed by shredding or other means when no longer required. It is not appropriate to put this material into waste or recycling bins.

In areas where confidential information is processed, access should be restricted to those personnel who work directly in those areas. Doors should not be left unlocked by cleaners and other support staff.

Since the majority of computers in the corporate environment will be connected to a network allowing them to potentially access confidential information it is important that these machines are either logged out or shut down when not in use. If the computer is left it should be locked using CTRL-ALT-DELETE as a minimum.

Most secure computer applications have inactivity timeout. It is important that this function is enabled, and no attempt is made to interfere with this functionality.

Laptops which are left on desks should be secured using Kensington type locks to prevent their removal. It should not be presumed that a locked door is sufficient security

If IT services encounter a laptop which is not secured in the above manner it may be removed and retained.

5.5 Password Policy

Passwords are a fundamental aspect of computer security and are usually the front line of protection for corporate data. A poorly chosen password could result in the compromise of the company’s entire corporate network, and as such, everyone is responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Users are responsible for the security of their passwords and accounts. The company recommends the following password rules:

- The password should contain characters from three of the following four categories:
- Latin uppercase letters (A-Z).
- Latin lowercase letters (a-z).
- Numbers (0-9).
- Special characters e.g. !@$%^.
- Minimum password length: 12 characters or longer passphrase.
- Passwords must not be shared or reused across systems.
- Multi-Factor Authentication (MFA) is required for administrative accounts, cloud services, and any remote access.
- Access rights must follow the principle of least privilege and be reviewed quarterly.
- Approved password-management tools may be used for secure credential storage.

The password must not contain common usage words such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1).
- The password should not contain any of the examples in this document.
- The password should not be a word found in a dictionary (English or foreign).
- Passwords must not be the same as usernames.
- Do not write usernames or passwords down or store them in a file on a computer.
- Do not use the same password for company accounts as for other non-company access
- (e.g., personal ISP account, option trading, benefits, etc.).
- Where possible, don't use the same password for various company access needs.
- Do not share the company usernames or passwords with anyone.
- Don't reveal usernames or passwords in an email message.
- Don't type a password while anyone is watching
- Do not use the "Remember Password" feature of applications (e.g. Outlook, Internet
- Explorer etc.).

If you suspect an account or password has been compromised, report the incident to IT Services and they will assist in the change of all passwords.

5.5 Computer and Network Management

The company has a staff network, a student network and an open wireless network for non-company devices. Staff will be provided with a login to the staff network and should always regard this as their primary connectivity.

Company devices should only be connected to the open network in exceptional circumstances that prevent the use of the primary network for the device.

Students will be provided with a login to the student network automatically on enrolment. This account will be removed at the end of the academic year.

Only IT staff may physically connect devices to the computer network.

Only devices owned and operated by the company may be connected to the staff and student networks unless prior consent has been obtained from the IT Manager.

Staff can request a login to the student network from IT services.

IT services reserve the right to bar any device that is exhibiting characteristics which are detrimental to the overall network performance.

Equipment connected to the staff network is usually located in 'staff only' areas. For the purposes of this document, a ‘staff only’ area is defined either as an area which students may not enter or, exceptionally, an area which students may not enter unless they are accompanied at all times by a member of staff.

Computers connected to the staff network may only be used by students when they are directly and continuously supervised by a member of staff.

The company provides central on-line storage for computer files for all staff. This is provided at both an individual level (user store) and for workgroups to share files (shared store). This storage is necessarily limited by available resources and requires active management by those using that storage.

Staff must check their user store regularly to ensure that outdated or inappropriate material (such as personal photographs, personal music files or software installers) is removed.

When a member of staff leaves the company, his or her line manager is responsible for:

- ensuring that the contents of that staff member’s computers, mobile devices and user stores are checked for essential information that may be required by the company.
- arranging for those data and documents to be transferred to an appropriate location.
- ensuring that the user store is deleted, and all personal information removed from any computers and mobile devices prior to the staff member leaving.

All external data communications will be conducted through the company’s connection or other approved links.

No other permanent external network connections may be made without the prior consent of the IT Manager.

The IT Manager must be advised, in advance and at the earliest opportunity, of any plan to add items of equipment to or to replace or to re-locate equipment that is connected or may require connection to the company's computer network.

5.6 System Access controls

System access is administered using a series of related processes. These can be found on the staff intranet.

5.7 Use of Removable Media

Removable media includes but is not limited to:

- USB “sticks” or memory sticks, memory pens, USB flash drives etc, MP3 Players.
- SD cards, micro-SD cards and telephone SIM cards.
- Mobile Phones/camera phones and cameras.
- External Hard Drives, CD Discs, DVD Discs, Tapes.
- Laptops, Personal Digital Assistants PDA’s and tablet computers.
- Only encrypted USB drives or company-issued devices may store confidential data.
- Loss or theft of any device containing company or learner data must be reported immediately to the IT Manager and DPO.
- Devices used for assessment delivery or learner information must be protected by full-disk encryption and remote-wipe capability where possible.

It is recognised that there are circumstances where data needs to be moved using portable media. The company’s best practice is that data should normally be held on company central servers. Access to these servers onsite or via secure remote access methods reduces risk and assists with secure management of data. Portable media should only be used where there is a clear and justifiable requirement to move data outside of the secure servers. This use of portable media relates to the classification of data held on the media.

You should refer to your line manager if you need clarification on the classification of the data you are storing or transmitting. If you are unable to determine the classification of the data, then it should be treated as confidential.

Confidential

This includes information covered under the Data Protection act including personal identifiable information i.e. name, address, phone number, medical details, bank details, student names and grades etc., data or information which may be commercially sensitive.

Please note this information may be in a database, spread sheet, word document, PowerPoint presentation or another format.

Data classified as confidential as defined above must not be stored on removable media without password protected encryption.

There are two methods to do this:

- With a small number of files, the use of the password protection facility in Office Applications is appropriate. For assistance with password protecting files refer to the relevant Office application Help facility and search for password.
- When you have a larger number of files the use of encryption software to encrypt the memory device is recommended. Recommendations for current encryption software are available from IT Services.

This facility can be installed onto existing USB memory sticks or Laptop Hard drive.

Unrestricted

This classification covers all information which is not covered under the confidential classification. Information in this classification may normally be in the public domain or would cause no issue to the company if it were to be in the public domain.

Data classified as Unrestricted can be stored without additional protection. You must safeguard any important data from loss through human error or equipment failure by ensuring there is a backup.

Do not store the only copy of any company information on a memory stick, CD or other media

General guidelines

It is recognised that there are circumstances where data needs to be moved using portable media. The company's best practice is that data should normally be held on company central servers. Access to these servers onsite or via secure remote access methods reduces risk and assists with secure management of data. Portable media should only be used where there is a clear and justifiable requirement to move data outside of the secure servers.

Data storage media should carry ideally an identifying label. This can, for example, be in the form of a fob or an adhesive label. This is to assist with the recovery of misplaced items.

This policy applies to storage of all information belonging to the company irrespective of the owner of the media. e.g. in the case of personally owned laptops or memory sticks etc.

Information is classified as Confidential, Internal Use, or Public.

Personal and confidential data must only be accessed for authorised business purposes.

All portable devices and removable media containing confidential data must use approved encryption (AES-256 or equivalent).

Confidential data taken off-site must be transported securely and stored only on encrypted devices.

Data-retention periods follow the company's Data Retention Schedule and are reviewed annually.

5.8 Breaches of Information Security

Anyone suspecting that there has been, or is likely to be, a breach of Information Security should inform the IT Manager or the Data Protection Officer immediately. The IT Manager or the Data Protection Officer will advise the company on appropriate courses of action

In the event of a suspected or actual breach of security, the IT Manager may, after consultation with the manager in question, make inaccessible or remove any unsafe user accounts, logins, data and/or programs from the network and report this to a member of the Management Team.

If a breach of Information Security affects the security of personal information relating to any data subject(s), the Data Protection Officer may authorise any user account to be locked, and its contents made available to authorised individuals for investigation. Such a breach may lead to civil or criminal proceedings.

Senior post-holders have the authority to take any action deemed necessary to:

- protect the company against breaches of security.
- manage any identified breach of security.
- limit the risk or damage resulting from any potential or identified breach of security.

5.9 Policy Awareness and Disciplinary Procedures

New members of staff will be directed towards this policy by the personnel department on appointment. Learners will be directed towards this policy during enrolment or induction. Existing staff, learners, partners and authorised third parties with access to the company network will be advised of the existence of this policy statement.

Failure of an individual student or member of staff to comply with this policy may lead to instigation of the relevant disciplinary procedures. The failure of a client, partner or third

party to comply may lead to the cancellation of a contract or partnership. In certain circumstances, legal action may be taken.

6. Training and Awareness

All employees and contractors must complete annual data-protection and information-security training, including updates on phishing awareness, password security, and secure handling of assessment materials. Refresher sessions will be delivered whenever legislation or awarding-body requirements change.

7. Contracts

Any complaints, concerns or queries relating to this policy or related codes of practice should be directed to the IT Manager in the first instance.

Associated Policies:

- Acceptable Use of IT – Student
- Risk Management
- Equality and Diversity
- Safeguarding