


# ACCEPTABLE USE OF IT SYSTEMS POLICY

# ACCEPTABLE USE OF IT SYSTEMS POLICY

## 1 POLICY STATEMENT

This policy is designed to protect Skills to Group, our employees, learners, customers and Stakeholders from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime.

Everyone who works at Skills to Group is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy of how it impacts their role they should speak to their manager or the IT Support Technician.

## 2 SCOPE

This is a universal policy that applies to all Users and all Systems.

Some aspects of this policy affect areas governed by local legislation in certain countries (employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at Skills to Group who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

## 3 USE OF IT SYSTEMS

3.1 All data stored on Skills to Group's systems is the property of Skills to Group. Users should be aware that the company cannot guarantee the confidentiality of information stored on any Skills to Group system except where required to do so by local laws.

3.2 Skills to Group's systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not in any way be detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by Skills to Group, other than trivial amounts.

3.3 Skills to Group trust employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain, they should consult their manager.

3.4 Skills to Group can monitor the use of its IT systems and the data on it at any time. This may include, except where precluded by privacy laws, examination of the content stored within the email and data files of any user and the examination of the access history of any user.

3.5 Skills to Group reserves the right to regularly audit networks and systems to ensure compliance with this policy.

## 4 DATA SECURITY

4.1 Users must not send, upload, remove on portable media or otherwise transfer to a non Skills to Group system any information that is designated as confidential, or that they should reasonably regard as being confidential to Skills to Group, except where explicitly authorised to do so in the performance of their regular duties.

4.2 Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with Skills to Group's safe password policy of one random 8 letter word.

4.3 Users who are supplied with computer equipment by Skills to Group are responsible for the safety and care of that equipment and the security of software and data stored on it and other Skills to Group systems that they can access remotely using it.

4.4 All work stations (desktops and laptops) should be secured with a lock-on-idle policy active after, at most, 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

4.5 Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities, as far as is reasonably practicable, and compatible with the designated purpose of those systems.

4.6 Users must at all times guard against the risk of malware (e.g. viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Skills to Group's systems by whatever means and must report any actual or suspected malware infection immediately.

## 5 UNNACEPTABLE USE

5.1 Skills to Group employs the use of Firewall security to block sites which it deems to be inappropriate, which is regularly reviewed. This includes the use of both staff and learner's own devices when connected to the main skills group internal network

5.2 All employees should use their own judgement regarding what is acceptable use of Skills to Group's systems. The activities below are provided as examples of unacceptable use,

however, it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with an obtain approval from their manager before proceeding:

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection legislation.

- All activities detrimental to the success of Skills to Group. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g. streaming video, playing networked video games).

- All activities that are inappropriate for Skills to Group to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, cyberbullying or harassment, inciting hate, websites and videos showing extremism.

- Circumventing the IT security systems and protocols which Skills to Group have put in place.

## 6 ENFORCEMENT

6.1 Skills to Group will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgement regarding acceptable use.

While each situation will be judged on a case-by-case basis, employees and learners should both be aware that consequences may include the termination of their employment and or training.

6.2 Use of any of Skills to Group's resources for any illegal activity will usually be grounds for Summery dismissal and Skills to Group will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.

## Document Control

This policy will be reviewed annually or earlier if deemed necessary

Date Last Reviewed: February 2025
Date to be Reviewed: February 2026

**Authorised By**



**Signed**

**Mark Boulting**
**Managing Director**