IT Computer Usage Policy

Introduction

Floorskills Limited investment in IT is considerable, and the company is highly dependent on computer technology in the delivery of its' services. Consequently, this Policy sets out to both protect the criticality of the IT contribution to the business and support the smooth and efficient operation of company systems at operational level.

This policy defines how the company expects its' employees to contribute to these aims as well as clarifying responsibility for the issue, safe and effective use of computer equipment and systems within Floorskills Limited. It stipulates what action individual employees must take to ensure efficient and safe operation of the equipment and system.

This Policy also covers the responsibilities for the issue and use of company laptops and other remote equipment and their accessories.

The name and contact details for Floorskills Limited IT Service Provider can be obtained from H.R.

1. Network Access

Access to, and usage of, Floorskills Limited's company Computer Network is strictly limited to authorised employees and authorised contractors only. No one else should have access to the network without the approval of the Managing Director.

2. Hardware and Software

2.1. Floorskills Limited will provide the necessary hardware and software to enable employees to carry out their roles within the company. Only equipment provided by the company for this purpose should be used.

2.2. The company will maintain and repair said equipment using a company approved ICT Service Provider.

2.2.1. It is the sole decision of the Managing Director which ICT Service provider(s) is used.

2.3. Only company approved and authorised software must be installed on company computers, desktops or laptops.

2.3.1. The company will treat the installation of unlicensed/ unauthorised software, including screensavers, as a serious breach of the IT Policy and will invoke disciplinary action under the Disciplinary Policy against any employee caught infringing this instruction.

2.4. The company will maintain all software licenses to ensure compliance with legislation and the operation of its' business.

2.5. The Senior Management Team/ Directors are responsible for identifying the need to purchase new equipment, accessories, or associated software.

2.5.1. Any requests for modifications, enhancements, or upgrades to existing equipment and software must be discussed with the relevant department Senior Manager in the first instance.

2.6. Problems with hardware or software should be reported to the ICT Services Provider as soon as possible.

3. Use of Laptops

3.1. The company determines which roles have the use of a laptop versus a desktop PC.

3.1.1. Where an employee has been allocated a laptop for their personal business use, they will be subject to the company's Terms and Conditions for the use of laptops and other portable equipment. See the Laptop Agreement which covers the security and safekeeping of all portable devices and equipment allocated to employees, or used by them, on an intermittent basis.

3.1.2. The re-allocation of company laptops is the decision of the Managing Director.

3.2. The security and safekeeping of laptops, and other portable equipment issued by the company, becomes the responsibility of the employee to whom it is issued and who uses it.

3.2.1. This includes storing the equipment in a suitably secure and dry place when not in use, not leaving it in an unattended or hot vehicle, or visible within unsecured premises not owned by Floorskills Limited. In such circumstances the laptop should be locked away or stored within a locked facility when not in use.

3.2.2. The employee to whom the laptop has been issued should treat the equipment with due care and attention and take every appropriate step to ensure the life and performance of the equipment.

3.2.3. Any accidents or incidents which could result in damage to the equipment, or be likely to affect its performance e.g. coffee spilt across it, it being dropped or left in an extremely hot environment, should be reported to H.R.

3.3. Should the laptop, or any of its' accessories:

- be stolen, and the company considers that reasonable and necessary steps were not taken to ensure its' security, or
- be damaged through an employee's negligence or poor use, then the employee concerned will be liable to recompense the company for the loss or repair of the equipment.

Then the company will deduct the cost of repair or replacement from the employees' salary, or other payments owing to them – should this come to light at the end of employment for example.

3.4. All remote equipment must be returned to the company when requested, either for periodic checking, upgrading or housekeeping or when the employee leaves.

4. Data/ Electronic Information

4.1. All information/ data held on the company's systems is deemed the property of Floorskills Limited

4.2. The company has the right, and as a condition of employment employees' consent, to the examination, use and content, of all data/ information processed and/or stored by employees on the company's systems.

4.3. Department Managers are responsible for ensuring compliance with Data Protection legislation with regard to data processed and stored within or by their departments.

5. Backing - Up

5.1. The ICT Services Provider is responsible for ensuring the effective and efficient backing-up for server held software and data.

5.2. Users of networked desktop PCs should avoid storing data on their local hard drives. Data stored in this manner may be lost if a problem develops with the PC and may not be recovered. Data should be stored within the file directory structure used by the office.

5.2.1. Electronic data and information belonging to the company should ONLY be stored on company equipment and systems. Data should NEVER be stored at home.

5.2.1.1. Employees found making unauthorised copies of information or saving to any other devices may be subject to the Disciplinary procedure.

5.2.2. Assessors are required to upload learners' data to Learning Assistant at least weekly and preferably within 48 hours of receiving the data. This data is subsequently backed up to a cloud for additional security and protection.

5.2.3. The use of external hard-drives or memory sticks is strictly limited to approved roles as determined by the Senior Managers. For example, Assessors and Tutors who work remotely.

5.2.3.1. Only encrypted memory sticks issued by the company should be used. These can be obtained from H.R.

5.2.3.2. Memory sticks should only be used between work laptops and/ or desktop PCs. They should not be used in personal computers.

5.2.3.3. The memory sticks should be virus checked each week

5.2.4. Alternatively, work undertaken on any other computer, for whatever reason, should be emailed by the employee to themselves and then saved in the normal way.

5.3. Failure to observe the back-up requirements could lead to disciplinary action.

5.4. Tutors are provided with Dongles to facilitate the use of the Internet at facilities where they are delivering training.

5.4.1. These can be obtained from the Finance and H.R. Controller

5.4.2. Dongles will need to be signed for on collection and return after use.

5.4.3. Just as with all other company remote equipment, Tutors are expected to take all necessary steps to ensure the safety and care of the Dongles whilst in their possession.

5.4.4. Any issues or loss/ damage must be reported to H.R.

6. Anti-Virus Protection

6.1. The company will install effective virus security software on all machines for which it is responsible, and upgrade this periodically as necessary.

6.2. Remote and laptop users must comply with requests to assist in upgrading equipment issued to them for remote use.

6.3. Employees should virus-scan all media (CDs, memory sticks) before first use.

6.4. On detection of a virus employees should notify the ICT Service Provider immediately. They will provide assistance.

6.5. Under no circumstances should employees attempt to disable or interfere with the virus scanning software.

7. Health and Safety

7.1. Health and safety with regards to computer equipment and computer workstations should be managed within the context of the Health & Safety policies and procedures within Floorskills Limited.

7.2. Managers are responsible for ensuring health & safety legislation and procedures with regards to computer equipment are implemented within their Departments.

7.3. The retained Health & Safety Advisor and/or ICT Services Provider will keep abreast of IT-related legislation and advise the Senior Management Team accordingly.

8. Training

Department Managers are responsible for ensuring that appropriate computer training is identified and provided for their Departments and individual employees.

9. User Accounts

9.1. H.R. will notify the ICT Services Provider of new members of staff in advance to allow the creation of network and e-mail accounts and system permissions.

9.2. H.R. will notify the ICT Services Provider of the departure of staff to allow the deletion of network and e-mail accounts.

10. Use of Passwords

10.1. Access to Floorskills Limited computers must be password protected.

10.1.1. The ICT Services Provider will ensure pass wording is part of the security strategy.

10.1.2. Employees must observe the required behaviour and protocols regarding the use and maintenance of passwords as described below.

10.2. Employees are required to use their passwords, and not put in place any process which bypasses the requirement for a password.

10.3. Employees must take every possible precaution to safeguard the security of their personal password(s) to protect access to company data and systems.

10.3.1. Passwords must not be stored by the computer or shared with other employees or persons outside the company.

10.4. If an employee has reason to believe that their password(s) has been 'discovered', then they should change it immediately.

10.5. Problems with passwords should be reported to the relevant Senior Manager/ H.R. / ICT Services Provider.

11. Systems Usage

11.1. All employees should ensure that their computers are fully shut down and turned off at the end of the working day.

11.2. Computers should also be locked or shut down when left unattended for any significant period of time e.g. over the lunch break or attending meetings.

11.3. With regards to file management, Department Managers will determine the top- level folders/directories and associated permissions for their department and inform the ICT Services Provider. The ICT Services Provider will create or modify the folders accordingly.

11.4. Within their respective top-level folders, employees should only create sub-folders

12. Contravention of the IT Policy

12.1. Contravention of the Floorskills Limited IT Policies or any act of deliberate sabotage to systems may be considered a disciplinary offence or dismissal.