FUW GROUP
ACCEPTABLE USE POLICY

Overview

The purpose of this policy is to define the acceptable practices and the restrictions regarding how company technology, equipment, and systems are to be used. It describes what employees can and can't do when using corporate computers, networks, websites or systems. It is the responsibility of all users of the FUW Group's services to read and understand this policy. This policy may be updated from time to time, in order to comply with the company's legal obligations and best practices.

Scope

This Acceptable Use Policy applies to any FUW Group's staff or contractors using the company's systems, computer equipment and network services. This includes employed staff, temporary staff and contractors granted access, including access to the guest wireless. It is designed to protect the FUW Group's employees, customers and other partners from harm caused by the misuse of our IT systems and our data.

This policy is a non-contractual document and is subject to change. The most recent copy will always be made available on the company Intranet, or directly from the FUW Group's IT Department on request.

Employees must know and abide by all applicable company policies dealing with security and confidentiality of company records, when conducting business operations, working for the FUW Group:

1. Company IT equipment

Company owned devices are assigned to individual users by the Head of IT and are recorded in the company Inventory database. Access to any of the services in use at the FUW Group is monitored to ensure that no personal devices are used for business work.

1.1. The use of personal devices (such as: computers, laptops, tablets, iPads, mobile phones, etc.) is strictly forbidden for work for the FUW Group.

1.2. It is strictly forbidden to share the use of any Group's company devices with friends and family including anybody working for the FUW Group.

1.3. All employees are required to use only specific IT devices (such as: computers, laptops, tablets, etc.) assigned to them by the Head of IT and it is strictly forbidden to borrow others' even on temporary bases.

1.4. No change of ownership is allowed and no IT work devices can be passed on, even after employees have left, unless agreed with the Head of IT.

1.5. Users must not access or attempt to use any company owned computing facilities, tablets, without authority. This includes using a password which belongs to another

user, however obtained. Any attempt to alter or delete material belonging to other users or to tamper with hardware or software, will be an offence against company regulations and may also constitute a criminal offence.

1.6. Computer screens must be locked when left unattended, at all times.

1.7. Colleagues who have been given permission not to use Remote Desktop can only install software strictly necessary for their role; the installation of applications needed for personal use, is strictly forbidden.

1.8. Employees are allowed to access only information that is needed to perform their jobs or assist others in doing so as part of the valid scope of their duties.

1.9. All staff need to be responsible for the content of all data, including text, audio, and images shared internally or externally. All communications must have the employee's name attached.

1.10. Employees must be responsible for all actions/transactions performed with their accounts.

2. Access to all services in use at the FUW Group

2.1. All staff must use Remote Desktop which has been implemented to reduce cyber vulnerability threats on our systems, therefore both Union and Insurance employees must use RD for all work for the business. Some exceptions apply to: the use of video calls and for employees using Graphic Packages and software incompatible with the RD platform which will need to be agreed between the Head of IT and the employee's line manager.

2.2. All employees are responsible for notifying both the Head of IT and the external technical team, in case the Two Step Verification setup on all the FUW Group systems and services has stopped working, which might allow hacking attacks and employees being locked out of accounts.

3. Use of mobile phones for work for the FUW Group

Work mobile phones are issued to Managers, Account executives and County executives and other users as instructed by the management.

Restrictions have been applied to all FUW Group's work mobile devices, to ensure data confidentiality protection against unauthorised users, therefore the use of personal phones is strictly restricted to the setup of Multi Factor Authentication using the Google Authenticator app.

3.1 No company Google accounts (with access to both emails and data) must be added to personal mobile devices.

3.2 Personal mobile phones can only be used for Multi Factor Authentication to access business systems in use at the FUW Group.

3.3 No change of ownership is allowed and no work mobile phone devices can be passed on, even after employees have left, unless agreed with the Head of IT.

3.4 FUW Group's work mobiles can strictly be used for business only and not for any personal matters.

3.5 In the event that a work mobile is found not password/PIN protected, the user must add the password/PIN number and communicate it to the Head of IT. Should a work mobile phone be returned by a leaver with an unknown password the mobile would be locked and unusable. The company reserves the right to recover the price of the mobile phone from the person responsible for the issue.

3.6 To reduce Cyber security vulnerabilities, no personal and work mobile phones, must be connected to the Staff Wi-fi which gives direct access to all the other devices on each FUW Group's office network.

4. Services: Internet/Intranet access

4.1 All employees (apart for very few exceptions when using software incompatible with RD), must access Internet through the Remote Desktop platform. Such access provides protection through a secure firewall and a range of technical systems, to attempt to reduce the risk posed by hackers, criminals and fraudsters who may attempt to attack our systems.

4.2 Users are advised that the Group Internet service is solely for work related matters.

4.3 Internet, as a secondary use, all employees are permitted to utilise the system for their own personal use during lunch breaks only.

5. Office Internal Network and Wi-fi

5.1 When working from the FUW Group's offices all computers/laptops belonging to the office internal members of staff, must be connected to the LAN by Ethernet cable to allow connection to copiers for printing. If you do not have an Ethernet cable, please see the Head of IT.

5.2 The use of Wi-fi is not allowed for work devices such as laptops and computers because of the impact of possible interferences affecting the signal and devices' performance.

5.3 Visitors are only allowed to use the Guest Wi-fi (for both work and personal devices) and must not be given the Staff Wi-fi password, to protect the office network from hacking attacks.

5.4 The use of public unsecured Wi-Fi networks is strictly forbidden for access to all the FUW Group's services. While using free public Wi-Fi can be convenient, there are cybersecurity vulnerabilities which might jeopardise the safety of our company data.

6. Social Media

6.1 Work use
Please refer to the standalone social media FUW Group's policy for acceptable use.

6.2 Personal use

a) Personal use of social media must be restricted to outside working hours and from a personal device.

b) Company owned devices can be used for this purpose, only during lunch breaks. The FUW Group would expect personal use of social media to be carried out at home, on personal devices, after working hours.

Policy Violation and the Consequences of Policy Violation

All employees working for the FUW Group must adhere to the guidelines in this policy at all times. Violation of the Acceptable Use Policy represents the misuse of company technology, systems, and equipment whether done deliberately or inadvertently.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from business downtime. Should any employee be unclear on the policy or how it impacts their role, they should speak to their line manager or the Information Governance Team.