IT Acceptable Use Policy

Oakland House | 21 Hope Carr Road

Leigh | Lancashire | WN7 3ET

www.ensissolutions.co.uk | 01942 265859

Document Details

Policy Title:	IT Acceptable Use Policy
Date:	16.02.2022
Version:	V2
Prepared By:	Katie Thornton
Quality Assured By:	Stuart Crosby
Authorised By:	Stuart Crosby

Document History

Version	Date	Editor	Reason for Changes
V1	16.02.2022	Katie Thornton	Creation
V2	07/05/2024	Emma Harding	Policy Review

Other Linked Policies

Policy Title
• Safeguarding Policy
• Prevent Policy
• ALN and ALS Policy
• Equality, Diversity, and Inclusion Policy
• GDPR and Data Protection Policies
• AI Guidance Policy

Contents

Overview

An Acceptable Use Policy is about ensuring that you, as an Ensis employee can use the internet, email and other technologies available in offices in a safe and secure way. The policy also extends to technology outside of the office e.g. equipment; printers and consumables; Internet and email; virtual learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to identity theft and therefore fraud. We have also banned certain proxy sites as well as anonymous proxy sites, because they put the company's network at risk. Help us, to help you, keep safe.

Ensis recognises the importance of ICT and the needs of staff to access computer facilities available within the workplace. To allow for this Ensis requires all staff to sign a copy of the Acceptable Usage Policy before they receive their username and password.

Listed below are the terms of this agreement. All staff are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action.

Please read this document carefully and sign and date it to indicate your acceptance of the Policy. Access to the company's ICT facilities will only take place once this document has been signed.

Equipment

Vandalism

Vandalism is defined as any action that harms or damages any equipment or data that is part of the Ensis. Such vandalism is covered by the Computer Misuse Act 1990 (see Glossary). This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware
- Change or remove of software
- Unauthorised configuration changes
- Create or upload computer viruses
- Deliberate deletion of files

Such actions reduce the availability and reliability of computer equipment; and puts at risk other users' data. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities. Staff will be billed for any vandalised equipment.

Use of Removeable Storage Media

Ensis accepts the fact that you may wish to transfer data between home and the workplace by using USB, phone or other portable media devices, however we cannot guarantee that your work will transfer between the devices, nor do we accept any responsibility for these devices when used. Furthermore, we have active security software that is used to keep our network secure, any detection of virus / malware or other unwanted software may result in your device being blocked from the network.

Internet and Email

Content Filtering

Through our Internet Service Provider (ISP), Ensis provides filtering designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. Should you come across any inappropriate website or content whilst using the internet, you must report this to a member of IT support immediately.

The use of Internet, email and the Local Area Network (LAN) is a privilege and inappropriate use will result in that privilege being withdrawn.

Acceptable Use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Only suitable material – the internet is not to be used to download, send, print, display or transmit materials that would cause offence or break the law
- Do not access chat rooms, forums or any other form of online communication unless your position specifically requires it to be accessed
- Do not access online gaming sites
- Do not use the internet to order goods from e-commerce, online portals or any other form of online catalogue service
- Do not use our LAN for any unauthorized services such as gaming, peer to peer clients and FTP Services

External Services

Webmail

Webmail provides access to your email account through a web client, use of webmail is encouraged as a viable method of communicating when away from the office of equipment provided by the business. The following rules must be adhered to at all times when accessing webmail through Ensis' ICT equipment.

- Do not reveal your password to anyone
- Treat file attachments with caution
- We do not accept any responsibility for damage caused to personal systems whilst using webmail on any personal device

Privacy and Data Protection

Passwords

The following but not limited to list explains the use of best practice for passwords;

- Never share your passwords with anyone or ask for another's password
- When choosing your password, you must choose a phrase or word that is easily remembered, a strong password includes at least one capital letter, a number and a special character such as a #
- If you believe that someone has discovered your password, you must change it immediately

Security

- Never attempt to access files or programs to which you have not been given access, attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hacking attempts and be subject to disciplinary action
- You should report any security concerns to a member of IT support immediately
- If you are identified as a security risk, you will be denied access to systems and the network whilst being subject to disciplinary action

Service

Whilst every effort is made to ensure that our systems, both hardware and software are working correctly, Ensis will not be responsible for any damages or loss incurred because of system faults, malfunctions or routine maintenance. These damages include the loss of data, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, your own errors or omissions. Use of any information obtained via Ensis' ICT systems is at your own risk. Ensis denies any responsibility for the accuracy of information obtained whilst using its systems, network and infrastructure.

Mobile Technologies

For reasons of safety and security staff should not use their mobile phone or any other technology in a manner that is likely to bring Ensis into disrepute.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 4G mobile phones also means

that staff may be sent inappropriate images or videos or be encouraged to send back images or video of themselves using integrated cameras.

To reduce the opportunity for those behaviours that could possibly cause upset it is advisable that staff limit their use of mobile technologies to necessary communication outside of working hours.

Network Monitoring

For reasons of safeguarding and wellbeing Ensis use monitoring software across the network, this software monitors activity of connected devices to the network including the Wi-Fi access, for this reason all personal devices should be connected to the Guest network only if access is required, Ensis is under no obligation to supply access for staff to the Wi-Fi network. Only devices owned by the company should be connected to the Staff network.

Glossary

Computer Misuse Act

The Computer Misuse Act makes it an offence for anyone to have;

- Unauthorised access to computer material e.g. if you find or guess a fellow colleague's password and use it
- Unauthorised access to deliberately commit an unlawful act e.g. if you guess a fellow colleague's password and access their learning account without permission
- Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the businesses network system

Data Protection Act 2018

The Data Protection Act ensures that information held about you is used for specific purposes only.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the business. The Act not only applies to paper files it also applies to electronic files.

The Principles of the Act state that data must be;

- Processed lawfully, fairly and transparently
- Collected only for specific legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Stored only as long as is necessary
- Processed in a manner that ensures appropriate security

RIPA – Regulation of Investigatory Powers Act 2002

If a request for authorised access is made, they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for;

- The interception of communications
- The acquisition and disclosure of data relating to communications
- The carrying out of surveillance
- The use of covert human intelligence sources
- Access to electronic data protected by encryption or passwords

If a request for authorised access is made, we will provide the appropriate access to your ICT records and files.