Document details:

Title	IT Systems Use Policy and Mobile Phones
Document ID	EXT012
Version number	1.03/0123
Status	Published
Published date (web)	01/23
Author	Clover
Approved by	Board of Directors
Review date	01/24
Review frequency	Annual

Revisions:

Version	Date	Description	Revision
1.01	01/22	Original document	Original copy
1.02/0123	01/23	Updated	All details by Clover
1.03/0123	09/23	Updated	Added page 1 document details

Dependencies and related policies or process:

Document	Location
Information Security Policy	Information-Security-Policy-statement-1.pdf (grillatech.com)
Disciplinary Policy	Internal document

IT Systems Use Policy and Mobile Phones

1. Definitions

The company provides computers, software and network services for the purpose of business-related work, which will simply be referred to as 'IT Systems' throughout this policy. Examples of such are, but not limited to:

- Email
- Internet Access
- File Storage
- Printers
- Educational Software
- Wi-Fi
- Company phones
    - Including making and receiving calls
    - Retrieving voice mail messages on company phones
    - Sending or receiving text messages including photo images
    - Logging onto the internet via a hand held device.

Within this policy the term 'User' relates to employees, contractors, visitors and board members.

2. Introduction

The company provides access to IT systems to its users where relevant and useful for their jobs or training. This policy describes the rules governing the use of IT Systems at the company. This policy should be read alongside other key policies.

3. Purpose of Policy

IT systems are integral to the success of the business. However, it is important every person at the company who uses them understands how to use them responsibly, safely and legally.

This IT systems use policy aims to:

- reduce the online security risks faced by the company
- advise users on what they can and can't do whilst using company IT systems at work.
- ensure users do not view inappropriate content at work
- help the company satisfy its legal obligations regarding IT systems use
- ensure users comply with legal and policy obligations whilst using IT systems

4. Policy Scope

This policy applies to all users of the company IT systems. It applies no matter whether IT systems access takes place on company premises, while travelling for business or while working from home.

It applies to the use of any device that is owned by the company, or that is connected to any company networks or systems. For example, it applies both to an individual using the IT systems at their desk, and to users who connect their own tablets or smart phones to the company wireless network.

5. Equipment

Users must safeguard the information created in the computer network by minimising the use of the local hard disc for storage purposes and by preventing their terminal from being used by an unauthorised person.
Users must take care of, protect and maintain in good state the equipment issued to them, and not modify or move the equipment without authorisation.

6. Personal Use

The company allows users to use IT systems for personal reasons, with the following stipulations:

- Limited, occasional, or incidental use for personal, non-business purposes is understandable and acceptable. Users are expected to demonstrate a sense of responsibility and not abuse this privilege, otherwise access will be removed.
- IT systems are provided by the Company primarily for business use. Users must not use the IT system for activities of personal gain.
- All rules described in this policy apply equally to personal use as well as work use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.
- Personal use must not affect the IT service available to other people in the company. For instance, downloading large files could slow access for other users.

Users must note that they have no right to privacy when using the company systems, whether for work or personal use. See section 12 for further detail on monitoring.

7. Confidentiality and Security

Used unwisely, IT systems can be a source of security problems that can cause significant damage to the company's data and reputation. Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware onto any of the Company's IT systems. Users must not gain access to websites or systems for which they do not have authorisation, either within the business or outside it.

Company data should only be uploaded to and shared via approved services. The Services Director can advise on appropriate tools for sending and sharing large amounts of data.

Users must not steal, use, or disclose someone else's login or password without authorisation. Users must keep passwords confidential and change them if they have reason to believe they have been compromised. If any user becomes aware of another's user identification, then they must notify them of the breach of security. When leaving a terminal unattended or on leaving the office users should ensure they log off the system to prevent unauthorised individuals using their terminal in their absence.

If you use company electronic equipment (including company laptops, Tablets and mobile phones) (which is connected to the Business infrastructure in accordance with this policy) outside the office, you are responsible for the security of that equipment. You must not leave such equipment unattended – you must always carry it with you or lock it out of sight.

When not in use, you must ensure that Bluetooth and wireless interfaces on mobile devices are switched off to prevent their detection by thieves. You must exercise extra care when working in public areas (such as trains) to ensure that information is not viewed by anyone else.

If you work from home on a computer provided by the company, the use of this equipment is strictly confined to you. This means that you must not allow anyone else to use the equipment, alter the configuration or view any information on it.

Users must review prior to sending any official document or information that is sent using the IT systems to determine the appropriate security measures for reducing the chance of that information being revealed to an unauthorised person.

Confidential information must not be sent externally and in some cases internally, by any means without express authority and unless the messages can be lawfully encrypted. Users must always consider the security of the company's systems and data when transmitting data outside of the company. If required, help and guidance is available from Management or the Services Director.

Grillatech use SaaS (Software as a Service) suppliers. Therefore, you must not download any information stored on portable computers/laptops to local back up, as all data is backed-up in the cloud to avoid data loss. You must not enter personal data from company records onto a home computer.

8. Inappropriate Content and Uses

It is important users understand that viewing or distributing inappropriate content is not acceptable under any circumstances. Users must not view, download, create, distribute or retain any inappropriate content or material.

Inappropriate content is content that could be considered obscene, offensive or disrespectful to others. It can include text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law. Users should ensure they are familiar with the company Disciplinary Policy and ensure their use of IT systems complies with the requirements in this policy.

Additional examples of inappropriate use are:

- Acting on or encouraging illegal or criminal activities
- Sending offensive or harassing material to others
- Broadcasting unsolicited personal views on social, political, religious or other non-business-related matters
- Communicating material that could damage the company image or reputation
- Creating or transmitting material that might be fraudulent, defamatory, untrue, unlawful or incur liability for the company
- Excessive use of company equipment for personal use which impacts on work performance
- Deliberately disrupting systems and users both internal and external.

This list is not exhaustive and the company retains the final decision as to whether it considers particular material to be inappropriate under this policy. As a general rule, material would be regarded as inappropriate if any person in the Company might be offended by any of the contents or if the company would be embarrassed if it were known that its systems had accessed the particular web pages. If the user is unsure whether the company would consider particular material to be appropriate, they should not access it or distribute it.

If a user receives material which contains or they suspect contains inappropriate material or they inadvertently access such material on the Internet, they must immediately report this to the HR Advisor or Team Leader/Manager. Users must not, under any circumstances, forward the material, show it to anyone else or otherwise distribute it.

9. E-mail Usage

Conduct

Messages sent via the e-mail system are to be written in accordance with the standards of any other form of written communication and the content and language used in the message must be consistent with best Company practice. Messages should be concise and directed to those individuals with a need to know. General messages to a wide organisation should only be used where necessary and ALWAYS use the blind carbon copy facility (BCC) to protect customer/client confidentiality.

Legal Implications

Users must be aware that it is possible to create legally binding contracts without intending to via e-mail correspondence. E-mail must not be used for communications that could lead to a binding contract being formed or which would have the effect of obligating the company in any way, unless the user has the clear authority to make the commitment in question.

Messages sent over the e-mail system can give rise to legal action against the company. Claims for defamation, breach of confidentiality or contract could arise from a misuse of the system. It is therefore vital for e-mail messages to be treated like any other form of correspondence and where necessary hard copies should be retained. Users are also reminded that messages are disclosable in any legal action commenced against the company relevant to the issues set out in the e-mail.

Incorrectly delivered email

Should a user receive an e-mail message which has been wrongly delivered to their e-mail address they must notify the sender of the message, except in the case of spam mail which should be deleted immediately. Further, if the email message contains confidential information they must not disclose or use that confidential information. Should they receive an e-mail that contravenes the company policies the e-mail should be brought to the attention of their Manager.

Internal shared documents

If emailing internally regarding a document on a shared network drive, it is generally best to include the name and location of the file, rather than sending the file itself. Mailing the actual file itself is best reserved for if you need a record of that particular version of the file.

10. Housekeeping of Computer Systems

You must not use CDs, USB/pen-drives, or external hard drive's onto the Business systems to avoid risk of viruses. You should log out of computer systems or lock (Ctrl-Alt and Del) your workstation when you are not at your desk. You should log out of your computer at the end of the working day. All computer-based information must be stored on network servers and not on local drives. You must not remove any computer equipment from any Company premises without authorisation.

11. Copyright

The company respects and operates within copyright laws. Users must not use the company's IT systems to breach copyright law. Examples of copyright breach include:

- Publishing or sharing any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- Downloading illegal copies of music, films, games or other software, whether via file sharing services or other technologies.

12. Policy Enforcement - Monitoring Usage

Users must be aware they have no right to privacy when using the company systems. The company monitors use of the IT systems, to examine and review the data accessed and stored. Further investigation will take place where there is a legitimate need or concern. Examples of such situations include:

- where an employee off sick or on holiday
- to find lost messages or to retrieve data lost by computer failure,
- to assist in the investigations of wrongful acts or
- to comply with any legal obligation.

Any such examinations or monitoring will only be carried out by authorised staff.

Hard copies of data stored and/or communications may be used as evidence in investigations and/or disciplinary proceedings.

Users should always ensure that business information sent over IT systems is accurate, appropriate, ethical, and legal.

All data written, sent or received through the company's computer systems is part of official company records. The company can be legally compelled to show that information to law enforcement agencies or other parties.

13. Potential sanctions

Knowingly breaching this policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Users may also be held personally liable for violating this policy.

Where necessary, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

14. Company Mobile Phones Usage

If a Company Mobile Phone is provided, the Company will cover the cost of a standard handset, monthly line rental and call charges.

We recognise that there may be occasions when Company Mobile Phone Users may wish to use a Company Mobile Phone for personal use. This should be kept to a minimum.

Excessive personal usage of a personal device during working hours or misuse of the Company Mobile Phone could also lead to action being taken under the Disciplinary policy

Please take care of your Company Mobile Phone and remember that it remains Company property and must be returned (to your line manager), together with SIM cards, chargers and any other peripherals purchased by the Company, when you upgrade your phone or leave the Company.

Operating a Mobile Phone whilst driving

You are not permitted to use a mobile phone (or any other hand-held communication device) whilst driving your vehicle during the course of carrying out the duties of your employment.

A hand-held communication device is one which can be used for accessing oral, textual or pictorial communications.

15. Changes to Policy

This policy is does not form part of an employee's contract of employment. It may be amended at any time through appropriate methods of communication.