Computer Use Policy

Introduction

Employees are given access to the Company's computer, internet and telecommunications facilities in order to carry out the functions of their employment and to assist them in the performance of their work.

This policy should be read in conjunction with the Company's Data Protection Policy. The policies aims to protect the Company's facilities, resources, clients and reputation as a trusted provider of secure IT services, by:

- highlighting individual responsibilities for keeping hardware, software and telecommunications equipment safe and secure;
- helping users to understand the definition of personal data and how this personal data must be collected, handled and stored by the Company to meet the Company's data protection standards;
- helping users to understand their own individual responsibilities for any electronic information they use, produce and store on behalf of the Company or our clients;
- ensuring that the Company does not expose itself to any litigation connected to the data it produces, uses or stores;
- maintaining a positive reputation within social media and on the internet;
- ensuring that employees understand the Company's expectations of them regarding personal use of facilities;
- ensuring that employees understand their obligations and rights under the Data Protection Act 1988 and the General Data Protection Regulations which became law on 25th May 2018.
- Ensuring that employees understand when and why the company may decide to exercise its right to monitor the use of its computers, internet and telecommunications facilities.

Employees are asked to sign a User Agreement attached in Appendix 3, demonstrating that they have read and understand this policy and the Company's Data Protection Policy.

These policies are not contractual, however failure to comply with any of its requirements may lead to disciplinary action being taken against users, including dismissal in cases of gross negligence or misconduct.

1. Passwords and security

Once an employee has signed their user agreement he or she is given a password and is then authorised to use the Company's computer, internet and telecommunications facilities, including having access to the Company's computer network.

All laptops, computers, servers, tablets and smartphones are synchronized via Office 365.

Our servers are set to "change password on first log in" therefore new employees have to create their own password as soon as they log in. Thereafter employees must choose their own passwords which must be longer than eight characters and be sufficiently strong to prevent brute force including upper case, lowercase, numbers and punctuation.

Users must not disclose their password to anyone else and if they need to write it down they will be expected to keep it in a safe place.

If possible, accounts should also be protected using 2FA (Two Factor Authentication) using either email, SMS or an authenticator app.

Users are responsible for the security of their own computer and any information held on it.

All computers should be 'locked' by the user if they are left unattended and due care must be taken to ensure the general security of any area in which that computer is being used or stored.

Users are responsible for the security of their own computer and any information held on it. All computers should be 'locked' by the user if they are left unattended and due care must be taken to ensure the general security of any area in which that computer is being used or stored.

Users must report any suspicious activity, for example an employee trying to gain access to another employee's computer.

If a user is not available for work, other employees of the Company may access their computer to make information needed for any particular business function available to their manager or colleagues.

2. Use of email at work

Employees should exercise the same care in drafting emails as with any other written communication. All messages should be constructed professionally in terms of spelling and grammar. They should be filed electronically in the appropriate subject file including attachments.

Electronic signatures are attached automatically to all external emails, which includes the Company Logo, so they are not required to be added in the email application itself.

All emails should wherever possible be responded to on the same day they were received, or on the next working day. At weekends and public holidays this period is extended. If a response cannot be provided at that time e.g. where further information or consideration is needed, an acknowledgment should be sent with an anticipated response date.

If a user is going to be out of the office for a day or longer and are unable therefore to check their emails then they should put their "out of office assistant" message on.

Users should be aware that their emails may be checked if they are absent from work and there is a business related reason to do so.

Users should familiarise themselves with what constitutes "Copyright" and "Intellectual property" and take care not inappropriately use any material subject to copyright or intellectual property belonging to other companies.

The Company reserves intellectual property rights on any material developed by employees during working hours and/or for business purposes. The company also copyrights some material. Employees must take extra care not to share the Company's intellectual property or copyrighted material unless required to do so by their line manager.

Particular care should also be taken when sending confidential information, outside of the Company, since information could potentially be forwarded on to unintended recipients or accessed by unauthorised users. Where possible users should encrypt or password protect any attachments. If users are in any doubt as to whether certain information is confidential, they should discuss the matter with their line manager. One option is to zip any confidential files using 7-zip which includes an option for AES-256 encryption.

Care should be taken not to overload people with unnecessary emails, they should not be distributed to people who have no need to receive them i.e. users should select the correct individual/s or user groups.

If staff receive inappropriate email or become unintentionally connected to a website, which contains offensive or inappropriate material, the member of staff should disconnect from the site immediately and inform their manager.

The Company email should not be used for personal matters and users should not connect to personal email accounts using Company computers whilst at work.

3. Use of the internet at work

The internet must not be used in any way that might bring the Company into disrepute or to breach any copyright or intellectual property rights.

Users of the internet must not subscribe to any payable services without having obtained the written permission from their line manager. The user will be held accountable for any unauthorised commitment to expenditure made online.

Any user found to be accessing or downloading material of a pornographic or sexual nature, will be subject to disciplinary action for gross misconduct.

4. Use of telephones

The Company's telephone system is intended for business purposes only. Personal calls should be kept to an absolute minimum and, where at all possible, avoided during working hours.

Personal smart phones should not be set to receive Company emails unless expressly agreed by the line manager.

Phones issued by the Company for business purposes may be used outside of working time at the discretion of the line manager. Users should familiarise themselves with the terms and conditions of the phone contract in order to ensure there is no additional cost to the Company.

The Company also reserves the right to remove or restrict internet access on Company smart phones.

Mobile phones with access to company data must not be 'rooted' under any circumstances.

Any damage to a Company phone should be reported immediately and users may be asked to reimburse the Company for any costs associated with damage other than normal wear and tear.

Employees issued with a mobile or smart phone, are responsible for its security at all times. These devices should be locked with a unique password which must be kept confidential and not made available to anyone other than as authorised by the Company.

Employees who experience abusive calls in the workplace should refer to the Company's Guidance on Handling Abusive calls in the Workplace provided below and/or speak to their line manager for guidance.

5. Use of social media

Users may not make use of Company facilities to access social media sites. There may be times however when social media forms part of an employee's role. Employees should take particular care when using social media sites at work.

It is recognised that some employees use social media regularly outside of working time. It is important to remember that employees have a right to a private life and therefore connecting to colleagues and references to the Company are discouraged.

Where employees post material on social media, in circumstances where they are, or may be, identified as employees of the Company, they must at all times observe the following principles.

Employees should not:

- post on behalf of the Company unless specifically authorised to do so by your line manager;
- engage in any online activity which may damage the Company's business or reputation;
- post material which is offensive, abusive or derogatory;
- disclose confidential information;

- use the Company logo (or any registered trademark of the Company) unless authorised to do so by your line manager.

Some employees may require guidelines to follow when using social media as part of their role. In these cases social media users should:

- ensure that any material posted is not misleading, it must be factually correct;
- ensure that any material reflects well on them and on the Company;
- ensure that postings are within their area of personal knowledge or expertise;
- ask permission to publish or report on conversations that are meant to be private or internal to the Company;
- ensure that postings are honest, relevant, courteous, and appropriate;
- engage only in constructive dialogue;
- avoid engaging in contentious issues where they may not represent the Company's official view;
- keep it appropriate and polite when disagreeing with others' opinions. If a conversation becomes antagonistic, do not get overly defensive, disengage from the dialogue in a polite manner that reflects well on the Company;
- not say anything that would not appropriate a public gathering anywhere in the world;
- seek guidance before participating in social media when the topic being discussed may be considered sensitive e.g. a bad news story or commercially sensitive material;
- apologise quickly and honestly for any mistakes made and learn from them for future social media activity;
- remember that online activity is public, permanent and may be accessed at any time in the future by outside organisations including regulatory authorities and the press.

If an employee is in any doubt as to whether a particular posting falls within these guidelines, he or she should discuss it with his or her line manager before posting.

Failure to follow these guidelines or the publishing of derogatory and or confidential Company information found to be published on any kind of social media may result in disciplinary action.

6. Protection of computers, telecoms and related equipment

All employees are expected to take all appropriate measures and precautions to prevent the loss, theft, damage or unauthorised use of equipment including the following:

- keep equipment in a locked and secured environment when not being used;
- do not leave equipment for prolonged periods of time in a vehicle, especially in extreme temperatures;

- keep food and drinks away from all equipment and work areas;
- do not leave equipment unattended at any time in an unsecured location e.g. in an unlocked empty office;
- keep equipment in sight at all times while in public places, such as public transportation, restaurants, etc.

Should any equipment be lost or stolen, the employee must:

- immediately report the incident to his or her line manager;
- obtain an official police report documenting the theft;
- provide a copy of the police report to his or her line manager.

If the employee fails to adhere to these procedures, the employee will be held legally and financially responsible to the Company for the replacement of such equipment.

Should any equipment be accidentally damaged, the employee must report the incident to his/her line manager immediately.

Users will be expected to pay for any loss incurred by the Company through the theft or accidental damage of hardware that is due to their negligence.

Users must not attempt to fix, modify or upgrade equipment in any way without the express permission from their line manager.

Employees should not use any computers, telecommunications or related electrical equipment that does not belong to the company whilst undertaking their duties without the express permission of their line manager.

7. Protection of software and electronic data

When saving information or data employees should be aware of whether or not the data could be regarded as confidential personal.

Confidential information or data would include but not be limited to client information, proprietary information, trade secrets or any other privileged information.

Personal information or data is outlined clearly in the Company's Data Protection Policy.

External storage devices should not be used unless provided by the Company and only used for the purpose they are given. They should be kept securely and appropriately password protected.

Electronic data containing sensitive or confidential information must not be forwarded outside of the Company without express permission of the line manager. Any confidential information must be password protected or the sender must ensure that only the intended recipient will be able to access the information.

All employees also have obligations regarding the protection of personal data under the Data Protection Act 1988 and the General Data Protection Regulations which became law on 25th May 2018 and therefore must be aware of both this policy and the Company's Data Protection Policy.

Employees are introduced to both this policy and the Data Protection Policy during their HR induction. They are also given G.D.P.R. training to complete.

In order to avoid virus infection employees must not download any games, desktop themes or any other unauthorised software onto any computer. A list of authorised software is listed in Appendix - 1 Authorised Windows software list.

Any software loaded onto company computers must have an appropriate license and be approved prior to its installation.

Users should protect their computer and the Company network from damage due to virus infection by taking great care when:

- using disks from outside of the workplace
- opening unsolicited e-mail attachments
- browsing the internet

Any suspected infection of a computer by a virus should be reported to the line manager immediately, in accordance with Section 8. Security incident reporting.

If you are in any doubt as to the validity of an email or website then discuss it with your line manager before opening or entering.

All information stored on Company computers or external storage devices are considered to be the property of the Company.

8. Monitoring of computers, internet and telecommunications use

The Company has a legitimate interest in protecting its business and reputation and ensuring that employees conduct themselves professionally, ethically and lawfully, performing their work to the level expected of them.

If the Company suspects that an employee is using the Company's computer, internet and telecommunications facilities improperly, it reserves the right to investigate internet sites visited, examine email trails, intercept emails and monitor phone calls. Employees should be aware that despite the deletion of messages, access to deleted messages is still possible.

Users may be asked to account for any activity that appears to be time wasting, unauthorised use of Company facilities for personal use e.g. inappropriate use of phones, email activity or connecting to inappropriate internet sites.

Information which the Company obtains about use of the Company's email and internet facilities, or telecommunications equipment may be disclosed to law enforcement officials.

Employees should be aware that all calls made and received on the Company phone system will routinely be monitored and recorded to assess employee performance, customer satisfaction and to check that the phone system is not being used in an unauthorised manner.

Voicemails may also be checked when an employee is absent for any reason, it may therefore be unavoidable that personal messages are heard in these circumstances. Employees needing to make particular sensitive or private personal phone calls are advised to use the phone located in the meeting room which is not subject to any form of monitoring or recording.

Any user found to be using the Company's computer, internet or telecommunications facilities for unauthorised activities during working hours may be subject to disciplinary action.

9. Security incident reporting

All users must be vigilant and report immediately to the IT Manager or the Managing Director, any security incident, which may represent an actual, suspected or potential breach of security.

A compromise would be suspected through unusual activity on computers, changed documents, unusual undeliverable emails, BitDefender virus alerts or ConnectWise Automate alerts. In these circumstances the IT Manager will change the password by logging in and resetting via web interface. If the password on the router has already been altered and we cannot login, IT Manager will reset the router.

Other examples that should alert employees to a potential security incident would be:

- Virus or internet spyware such as advert 'popups'
- Where a manufacturer notifies you of a security weakness in their product
- Employees sharing password
- Loss or theft of equipment holding confidential or potentially damaging data
- Unauthorised access to data and systems both internal and external

10. Visitors and contractors

Visitors to the Company, even those engaged to perform technical support on the Company systems, must be supervised and monitored at all times whilst working on the Company's networks or with computer equipment.

Where possible, contractors will be expected to provide service level agreements or sign a contract regarding confidentiality.

11 Application updates and security

We recognise the importance of only running applications on our devices which

are supported by suppliers that produce regular fixes for any security problems.

All of the applications or software we use internally on any devices including Company mobile phones, must therefore either be paid for on subscription, which includes support, or be purchased as a perpetual license with support included or is a more general product that is kept up to date with security releases to the public.

All current software that we permit is listed in Appendix 1 - Authorised Windows software list (specific product or manufacturer).

All employees who choose to receive company emails on their personal mobile phones must also, must also adhere to the above stipulation i.e. all applications must be either paid for on subscription, which includes support, or be purchased as a perpetual license with support included or is a more general product that is kept up to date with security releases to the public.

A list of Apps known to meet the above stipulations is provided in Appendix 2 - Authorised Smart Phone App list. Should you wish to add an App to the list you should notify the IT Manager who will review the list periodically.

Any applications on devices that are no longer supported and no longer received regular fixes for security problems are deleted promptly.

12 Administrator Accounts

We recognise that using administrator accounts all-day-long exposes the device to compromise by malware. It is important therefore to ensure that our employees only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes). Similarly, we recognise that administrator accounts should not be used for accessing email or web browsing.

All staff who have separate administrative logins are technical staff who understand the importance of web safety.

13 Starters and Leavers

The IT Manager creates user accounts when we employ new staff. The IT Manager creates the account and it is logged as part of the induction process within SharePoint\Management.

The IT Manager is responsible for issuing the new member of staff with the User Agreement and agrees to abide by this policy, before he/she is given a login.

We recognise that user accounts not in day to day use, present a significant security risk. It is therefore important that all laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of our business.

Our accounts are all on our internal Active Directory server synched with Office

365. When an employee leaves the organisation The IT Manager immediately removes or disable any user accounts on all devices as part of our "Offboarding Process".

Appendix 1

Authorised Windows software list (specific product or manufacturer)

a. 7-Zip
b. Adobe
c. BitDefender
d. ConnectWise
e. Chrome
f. HP
g. Java
h. Maytas
i. Microsoft
j. Firefox
k. Zoom

Appendix 2

Authorised Smart Phone App list

Apps may only be installed from the Android Playstore or the Apple Appstore. In addition Android Play Protect needs to be left turned on.

Appendix 3

User Agreement

I have read, understand, and agree to be bound by the conditions contained in the Computer, Use Policy and policy and the Data Protection Policy.

I understand that any breach of these conditions may result in disciplinary action being taken against me and which could result in my dismissal from the Company.

Name:	
Signed:	
Date:	

The Company will retain a copy of this document