




## GDPR Information Security Policy

|             |                              |              |   |
|-------------|------------------------------|--------------|---|
| Status:     | Controlled                   | Written By:  | D. Stringer   |
| Version:    | 1.1                          | Title:       | HR coordinator  |
| Issue Date: | 4 <sup>th</sup> January 2024 | Approved by: | P R Cox   |
|             |                              | Title        | Director  |
|             |                              | Signed:      |  |

## GDPR - INFORMATION SECURITY POLICY

### 1. INTRODUCTION

We provide employees with access to various computing, telephone and postage facilities (“the Facilities”) to allow them to undertake the responsibilities of their position and to improve internal and external communication.

### 2. SCOPE AND APPLICABILITY

This Policy applies to all individuals that use or operate within our IT Systems, including networks, Laptops, desktops, telephones or any other facility that is provided for communication purposes.

This Policy applies to the use of:

- local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks;
- desktop, portable and mobile computers and applications (including personal digital assistants (PDAs);
- mobile telephones
- electronic mail (Email) and messaging services.

**Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.**

### 3. PURPOSE

This Policy sets out the Company’s policy on the use of the Facilities and it includes:

- Responsibilities and potential liability when using the Facilities;
- The monitoring policies adopted by the Company; and
- Guidance on how to use the Facilities.

This Policy has been created to:

- Ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring;
- Protect the Company and its employees from the risk of financial loss, loss of reputation or libel; and
- Ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

#### **4. COMPUTER FACILITIES - USE OF COMPUTER SYSTEMS**

To comply with this policy it should be noted that unless written prior authorisation has been received by departmental managers, the Facilities must be used for business purposes only.

In order to maintain the confidentiality of information held on or transferred via the Company's Facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Company's network. Despite the use of a password, the Company reserves the right to override passwords and obtain access to any part of the Facilities.

Individuals are ultimately responsible for keeping passwords secure. They must not give it to anyone, including colleagues, except as expressly authorised by the Company. Passwords should be changed every 90 days.

Individuals are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Company or its clients other than in the normal and proper course of carrying out duties for the Company.

#### **5. IT SECURITY PROCEDURES**

In order to ensure proper use of computers, all individuals must adhere to the following practices:

- Anti-virus software must be kept running at all times;
- All users accessing domain joined computer must seek IT permission to be able to use USB storage on the company network. If this permission is not requested, USB/CD media will be rendered un-accessible.
- Obvious passwords such as birthdays and spouse names etc. must be avoided. The most secure passwords are random combinations of letters and numbers. Password minimum complexity requirements are in force when creating/updating existing passwords;
- When you are sending data or software to an external party by Data storage media always ensure that the disk has been checked for viruses by the Group IT Support Department and password protected if required, before sending it;
- All files must be stored on the network drive which is backed up regularly to avoid loss of information; and
- Always log off the network before leaving your computer for long periods of time or overnight.

#### **6. SOFTWARE**

Software piracy could expose both the Company and the user to allegations of intellectual property infringement. The Company are committed to following the terms of all software licences to which the Company is a contracting party. This means, in particular, that:

- Software must not be installed onto any of the Company's computers unless this has been approved in advance by the Group IT Support Department. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities; and
- Software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of the IT Department.

## **7. LAPTOP COMPUTERS**

At various times during employment with the Company, individuals may use a laptop. These computers, along with related equipment and software are subject to all of the Company's policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a laptop creates additional problems especially in respect of potential breaches of confidentiality. When using a laptop:

- Individuals are responsible for all equipment and software until it is returned. The laptop must be kept secure at all times;
- It should only be used by the person authorised to use the equipment and software;
- Individuals must not load or install files from any sources without the Group IT Support Department inspecting such files for viruses;
- All data kept on the laptop must be backed up regularly in order to protect data against theft or mechanical failure or corruption;
- Individuals should password protect confidential data on disks or on the hard drive to protect against theft;
- If individuals become aware of any mechanical, electronic, or software defects or malfunctions, they should immediately bring such defects or malfunctions to the attention of the Group IT Support Department;
- Upon the request of the Company at any time, for any reason, Individuals will immediately return any laptop, equipment and all software to the Company; and
- If for any reasons individuals are using their own laptop to connect with the Company's network or to transfer data between the laptop and any of the Company's computers it is essential that they ensure that they you have obtained prior consent from the Group IT Support Department, and their Department Head in order to comply with its instructions and ensure that any data downloaded or uploaded is free from viruses.

## **8. E-MAIL (INTERNAL OR EXTERNAL USE)**

Internet e-mail is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything that the Company or individuals would not wish to be made public. If individuals are sending confidential information by e-mail this should be sent using password protected attachments.

E-mail should be treated as any other documentation. If an individual would normally retain a certain document in hard copy you should retain the e-mail.

Do not forward e-mail messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the e-mail.

E-mail inboxes should be checked on a regular basis.

As with many other records, e-mail may be subject to discovery in litigation. Like all communications, individuals should not say anything that might appear inappropriate or that might be misinterpreted by a reader or bring the Company into disrepute.

Individuals should not use the Company email system for private messages during the course of work activities unless absolutely necessary and in these circumstances the following message should be contained within the email that is sent:

“This e-mail does not reflect the views or opinions of our organisation”

Use of e-mail facilities for personal use is permitted during lunch breaks providing that:

- Such e-mails do not contain information or data that could be considered to be obscene, racist, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter; and
- Such e-mails are not used for the purpose of trading or carrying out any business activity other than Company business.

In the event that individuals are away from the office and use e-mail as an external means of communication they must ensure that the autoreply service is used to inform the sender that they are unavailable. Failure to do so could lead to disciplinary action. If there is any doubt as to how to use these Facilities please contact the Group IT Support Department.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited.

**NB: The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.**

## **9. INTERNET**

Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. Individuals are responsible for ensuring that they are the only person using the authorised Internet account and services.

Downloading any files from the Internet using the computer Facilities is not permitted. If there is a file or document on the Internet that is required, the individual should contact the Group IT Support Department to make arrangements for it to be evaluated and checked for viruses. It will be at the discretion of the Group IT Support Department on whether to allow such download.

Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use is strictly prohibited.

**NB: The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.**

Posting information on the Internet, whether on a newsgroup, via a chat room or via e-mail is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and the Company could face legal claims for monetary damages.

Using the Internet for the purpose of trading or carrying out any business activity other than Company business is strictly prohibited.

Subject to the above you are allowed to use the Internet for personal use during your lunch break. Use of the Internet for personal use at any other time is strictly prohibited.

For the avoidance of doubt the matters set out above include use of 3G/4G Data.

## **10. MONITORING POLICY**

The Policy of the Company is that we monitor use of the Facilities.

The Company recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

The Company may from time to time monitor the Facilities. Principle reasons for this are to:

- Detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies;
- Ensure compliance of this Policy;

- Detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Company;
- Ensure compliance by users of the Facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time; and
- Monitor and protect the well-being of employees.

The Company may adopt at any time a number of methods to monitor use of the Facilities. These may include:

- Recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;
- Recording and logging the activities by individual users of the Facilities. This may include opening e-mails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited;
- Physical inspections of individual users computers, software and telephone messaging services;
- Periodic monitoring of the Facilities through third party software including real time inspections;
- Physical inspection of an individual's post; and
- Archiving of any information obtained from the above including e-mails, telephone call logs and Internet downloads.

If at any time an employee wishes to use the Facilities for private purposes without the possibility of such use being monitored they should contact their Department Head or the nominated deputy. This person will consider such request and any restrictions upon which such consent is to be given. In the event that such request is granted the Company (unless required by law) will not monitor the applicable private use.

The Company will not (unless required by law or in receiving legal or professional advice):

- Allow third parties to monitor the Facilities; or
- Disclose information obtained by such monitoring of the Facilities to third parties.

The Company may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

## **11. BUILDING SECURITY**

Confidential and sensitive data is secured in the building. This is both in paper form (such as files of paperwork) and electronically (such as computers, storage devices and servers).

To improve the security and confidentiality of information, we require the following:

1. Do not allow entry to our premises to any unknown person
2. Ensure all visitors are signed in and are issued with an appropriate visitors pass and that they are advised to wear these passes visibly at all times

3. If you see someone you do not recognise and you cannot see that they are wearing a pass, ask to see their pass
4. If you see someone you do not recognise and they cannot show you a pass, immediately escort the person to reception to be signed in
5. Do not allow visitors to access roam the premises without being accompanied
6. Ensure you collect your visitors from reception
7. Ensure passes are returned and the visitor is signed out
8. Do not hold door open for people you do not recognise
9. Clock in and clock out in the instructed manner
10. Report anything suspicious to your manager

## **12. CLEAR DESK**

To improve the security and confidentiality of information, we have adopted a Clean Desk Policy for computer and printer workstations.

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Whenever a desk is unoccupied for an extended period of time the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives.
2. All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins.
3. Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and fax machines should be treated with the same care under this policy:
  - a. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the "Locked Print" functionality should be used.
  - b. All paperwork left over at the end of the work day will be properly disposed of.

## **13. GENERAL GUIDANCE**

Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.



**Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities or a breach of this policy may be treated as gross misconduct and may lead to dismissal.**