# IT AND COMMUNICATIONS POLICY

## 1. Policy statement

1.1 Our IT and communications systems are intended to promote effective working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use and the action we will take if you breach these standards.

1.2 Breach of this policy may be dealt with under our Disciplinary and Capability Policy and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

## 2. Security and passwords

2.1 You are responsible for the security of the equipment or devices allocated to or used by you and you must not allow them to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment. You should keep your passwords confidential and change them regularly.

2.2 You must only log into our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.3 If you are away from your computer you should lock it or log out. You must log out and shut down your computer at the end of each working day.

## 3. Data security

3.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

3.2 You must not download or install software from external sources without prior authorisation. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation.

3.4 We may monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

3.5 Inform your manger or a member of IT support immediately if you suspect your computer may have a virus.

## 4. Email

4.1 When sending emails and other communications at work you must:

4.1.1 adopt a professional tone and observe appropriate etiquette; and

4.1.2 remember that e-mails and instant messages can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

4.2 When sending emails and other communications at work you must not:

4.2.1 send anything that could be interpreted as abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate;

4.2.2 send or forward private communications which you would not want a third party to read;

4.2.3 send or forward chain mail, junk mail, cartoons, jokes or gossip; or

4.2.4 send messages from another person's account.

4.3 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

5. **Using the internet**

5.1 Internet access is provided primarily for business purposes.

5.2 You must have regard to the requirements of paragraph 11 below and must not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste, pornographic or immoral. Even web content that is legal in the UK will be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, viewing such content will be a breach of this policy.

5.3 We may block or restrict access to some websites at our discretion.

6. **Using your own devices for work**

6.1 Data contained within company email accounts and on the Company's systems, however these accounts and systems are accessed, is the property of the Company. You are responsible for the security of any Company data held on a remote device that you own or that is in your possession. You should be aware that if using equipment on, for example, public transport, documents can be read by other people and should guard against this.

6.2 You must report the loss or theft of any portable devices that contain Company data or information or documents or that have access to your Company email account to a manager immediately.

6.3 If you are using laptops or Wi-Fi enabled equipment you must be vigilant about its use outside the office and take precautions against importing viruses or compromising the security of our IT Systems. Our IT Systems contain information which is confidential to the Company and which is subject to data protection legislation. Such information must be treated with extreme care.

6.4 If you are working from home, you are responsible for ensuring the security of confidential information.

7. **Using your personal devices at work**

7.1 You should ensure that you keep use of your mobile phone or other devices to a minimum while working.

7.2 If there is a need for you to take an urgent phone call or read an urgent instant message, you should do so in a private, staff only location where you are not visible to audience members, customers or clients.

8. **Intellectual property and confidential information**

8.1 You should not do anything to jeopardise the Company's intellectual property and other confidential or privileged information or that of the Company contacts or third parties through the use of the IT Systems.

8.2 In addition, you should not misappropriate or infringe the intellectual property of other companies and individuals. Such action could create legal liability for the Company as well as for you.

8.3 You must not use the Company's logos, brand names, slogans or other trademarks, or post any of the Company's confidential or proprietary information without prior written permission.

8.4 To protect yourself and the Company against liability for copyright infringement, where appropriate, you must reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask a manager before making the communication.

9. **Personal use of our systems**

9.1 We permit the incidental use of our IT to use the internet for personal purposes. Permission for personal use must not be abused. We may withdraw permission for it at any time or restrict access at our discretion.

9.2 Personal use must meet the following conditions:

9.2.1 it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);

9.2.2 it must not affect your work or interfere with the business;

9.2.3 it must not commit us to any costs or incur any charges; and

9.2.4 it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Privacy Notice and Disciplinary and Capability Procedure.

10. **Monitoring**

10.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

10.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

10.2.1 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

10.2.2 to find lost messages or to retrieve messages lost due to computer failure;

10.2.3 to assist in the investigation of alleged wrongdoing; or

10.2.4 to comply with any legal obligation.

11. **Prohibited use of our systems**

11.1 Misuse of our systems or internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

11.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

11.2.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

11.2.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

11.2.3 a false and defamatory statement about any person or organisation;

11.2.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

11.2.5 unauthorised software;

11.2.6 any statement which is likely to create any criminal or civil liability (for you or us); or

11.2.7 music or video files or other material in breach of copyright.

12. **Data protection**

When processing or interacting with the personal data of clients and customers and other third party individuals, you must adhere to our Data Protection Policy.