Staff Handbook

Schedule 25 - Fair Processing Notice

Issue 2.1

October 2021

Document History

Title	<Title>: <subtitle>
Andrew Martin	<Author>

Review Panel

Name	Role
Kate Guilding	Company Secretary
Jo Chadwick	HR

Change history

#	date	author	comment
2.1	18th Oct 2021	Victoria Iredale	Updated to current branded paper

Schedule 25

IT and Communications Systems Policy

1. **About this policy**

1.1 Our IT and communications systems are intended to promote effective communication and 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 The Managing Director has overall responsibility for this policy, including keeping it under review.

1.3 Breach of this policy may result in HR taking further action. In serious cases, it may be dealt with under our Disciplinary Procedure and could be treated as gross misconduct.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. **Equipment security and passwords**

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

2.2 You must only log on to 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 desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. **Systems and 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 authorisation from yor Principal Consultant. 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 from your Principal Consultant.

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

3.5 Inform your Principal Consultant if you suspect your computer may have a virus .

4. **Email**

4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by email. You should also include our standard email signature and disclaimer.

4.2 Remember that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails.

4.4 You should not:

(a) send or forward private emails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to others who do not have a real need to receive them; or

(d) send messages from another person's email address (unless authorised) or under an assumed name.

4.5 Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

5. Using the internet

5.1 Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 6.

5.2 You should 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 or immoral. Even web content that is legal in the UK may 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, then viewing it will be a breach of this policy.

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

6. Personal use of our systems

6.1 We permit the incidental use of our systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

6.2 Personal use must meet the following conditions:

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

(b) personal emails should be labelled "personal" in the subject header;

(c) it must not affect your work or interfere with the business;

(d) it must not commit us to any marginal costs; and

(e) it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

7. Monitoring

7.1 Our systems enable us to monitor telephone, email, 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.

7.2 We reserve the right to retrieve the contents of email 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):

(a) to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

8. **Prohibited use of our systems**

8.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

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

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

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

(c) a false and defamatory statement about any person or organisation;

(d) 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);

(e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(f) unauthorised software;

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

(h) music or video files or other material in breach of copyright.