Pav Dental

IT and Communications Systems Policy

Contents

1. About this policy

1.1. Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

1.2. This policy does not form part of any contract of employment or other agreement to provide services, and we may amend it at any time

1.3. Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in severe cases, may be treated as gross misconduct leading to summary dismissal.

2. To Whom does this policy apply?

2.1. This policy applies to all employees, self-employed team members, self-employed contractors, casual workers, agency workers, volunteers, interns, and anyone accessing our IT and communication systems.

3. Who is responsible for this policy?

3.1. The Company has delegated responsibility for overseeing its implementation to Hassan Bhojani (PM).

3.2. Any questions you may have about the day-to-day application of this policy should be referred to the PM.

4. Equipment security and passwords

4.1. You are responsible for the security of the equipment allocated to or used by you and must not allow anyone else to use it except in accordance with this policy.

4.2. You are responsible for the security of any computer terminal you use. You should lock your terminal or log off when leaving it unattended or when leaving the practice to prevent unauthorised users from accessing the system in your absence. Anyone not authorised to access our network should only be allowed to use terminals under supervision.

4.3. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting your PM.

4.4. You should use passwords on all IT equipment, particularly items you take out of the office. You must keep your passwords confidential and change them regularly. Unless authorised by PM, you must not use another person's username and password to make them available or allow anyone else to log on using your username and password. On termination of employment (for any reason), you must return any equipment, key fobs, or cards.

4.5. If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data maintained on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, such as passengers on public transport.

5. Systems and data security

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

5.2. You must not download or install software from external sources without authorisation from the PM. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by PM before downloading. If in doubt, staff should seek advice from the PM.

5.3. You must not attach any device or equipment to our systems. This includes any USB flash drive, tablet, smartphone, or similar device, whether connected via the USB port, infra-red connection, or in any other way.

5.4. We monitor all emails passing through our system for viruses. You should exercise caution when opening unsolicited emails from unknown sources or an email that appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the PM immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

5.5. You should not attempt to gain access to restricted areas of the network or any password-protected information except as authorised in the proper performance of your duties.

5.6. You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains confidential information subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

6. Email

Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

6.1. You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being or have been harassed or bullied or is offended by material received from a colleague via email should inform the PM.

6.2. You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where the recipient may forward your email. Avoid saying anything that would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

6.3. Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.4. In general, you should not:

(a) Send, forward or read 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, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list.

(d) Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals.

(e) Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature, like a name written at the end of a letter.

(f) Download or email text, music or any other content on the internet, which is subject to copyright protection unless it is clear that the owner of such works allows this.

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

(h) Send confidential messages via email, the Internet, or other means of external communication that are known not to be secure.

6.5. You should inform the sender if you receive an email in error.

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

6.7. If communicating with patients regarding their dental care directly or with third parties in relation to a patient's dental care, where possible, NHS mail accounts should be used and encryption implemented when applicable.

7. Using the internet

7.1. Internet access is provided solely for business purposes.

7.2. When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of the kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered under paragraph 9.

7.3. You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even legal web content 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.

7.4. Except as authorised in the proper performance of your duties, you should not under any circumstances use our systems to participate in any Internet chat room, post messages on any Internet message board or set up or log text or information on a blog or wiki, even in your own time.

7.5. The following must never be accessed from our network or using a device you have been issued with by us: online radio, audio and video streaming (including streaming of, or downloading of television, radio or films), instant messaging, [webmail (such as Gmail or Hotmail)] and social networking sites (including, but not limited to, Facebook, TikTok, Twitter, YouTube, Google+, Instagram, Snapchat, Pinterest, Tumblr, Second Life). This list may be modified from time to time.

8. Personal use of our systems

8.1. We permit the incidental use of our Internet, email, and telephone systems to send personal emails, browse the Internet, and make personal telephone calls, subject to certain conditions set out below. 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.

8.2. Personal use must meet the following conditions:

(a) Use must be minimal and take place substantially outside of normal working hours (that is, during lunch hours, before 9.00 am or after 5.30 pm).

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

(c) Use must not interfere with business or office commitments.

(d) Use must not commit us to any marginal costs.

(e) Use must comply with this policy (see in particular paragraph 5 and paragraph 6) and our other policies, including the Equality, Diversity & Human Rights Policy, Bullying and Harassment Policy, Data Protection Policy, and Disciplinary Policy.

8.3. You should be aware that personal use of our systems may be monitored (see paragraph 8) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

9. Monitoring

9.1. Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons and to carry out legal obligations in our role as an employer, use of our systems, including the telephone and computer systems, and any personal use of them, maybe continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

9.2. A CCTV system monitors the workplace. See the CCTV policy for further details. OR A CCTV system monitors the exterior of the building **>>DETAILS OF OTHER AREAS<<** 24 hours a day. This data is recorded. **>>Remove if not applicable<<**

9.3. We reserve the right to retrieve the contents of email messages or to 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.

(d) To comply with any legal obligation.

10. Prohibited use of our systems

10.1. Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Policy. Misuse of the internet can, in some circumstances, be a criminal offence. It will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or creating, viewing, accessing, transmitting or downloading any of the following material (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 or customers.

(c) A false and defamatory statement about any person or organisation.

(d) Material that is discriminatory, offensive, derogatory, or may cause embarrassment to others (including material that breaches our Equality, Diversity & Human Rights Policy and our Bullying and Harassment Policy).

(e) Confidential information about us, our business, or any of our staff, clients or customers (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).

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

Any such action will be treated very seriously and is likely to result in summary dismissal.

10.2. Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Policy. If necessary, such information may be handed to the police in connection with a criminal investigation.

Document Control

Title:	IT and Communication Systems Policy
Author/s:	Hugo Barton – Healthcare Law

Owner:	DCME Team
Approver:	DCME Team
Date Approved:	10/05/24
Next Review Date:	02/05/25

Change History				
Version	**Status**	**Date**	**Author / Editor**	**Details of Change** (Brief detailed summary of all updates/changes)
0.1	Final	10/05/24	Hugo Barton - Healthcare Law/HD & PG	Brand new policy developed by Healthcare Law, launched on DCME Portal

The latest approved version of this document supersedes all other versions, upon receipt of the latest approved version all other versions should be destroyed, unless specifically stated that previous version(s) are to remain extant. If in any doubt, please contact the document Author.

Approved By: Hassan Bhojani, Waleed Javed
Date Published: 19/09/2024