Kingston GP Chambers	IT use and Data Security Policy		Reviewed	June 2023
			Revised	
	Adopted	October 2020	Next review	June 2025

IT Use and Data Security Policy

About this policy

1. Our IT and communications systems are intended to promote effective communication and working practices within Kingston GP Chambers (KGPC). 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.
2. This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers, agency workers and anyone who has access to our IT and communication systems.
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 serious cases, may be treated as gross misconduct leading to summary dismissal.
4. This policy does not form part of any employee's contract of employment and we may amend it at any time.

Personnel responsible for the policy

5. KGPC has responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework.
6. Managers have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

Systems and data security

7. You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).
8. You must not download or install software from external sources without authorisation from the CQC compliance specialist. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice from the CQC compliance specialist.
9. You must not attach any device or equipment to our systems without authorisation. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.
10. NHS Email monitors all emails passing through their system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the CQC compliance specialist 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.

11. You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.
12. 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 information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

Email

13. 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.
14. 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 their line manager or the CQC compliance specialist.
15. 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 your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.
16. 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.
17. 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.
    (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 in the same way as 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 or the internet, or by other means of external communication which are known not to be secure.

18. If you receive an email in error, you should inform the sender.
19. 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.
20. We do not permit access to web-based personal email such as Gmail or Hotmail on our computer systems at any time due to additional security risks.

Using the internet

21. Internet access is provided solely for business purposes. Occasional personal use may be permitted in accordance with this policy.
22. 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 a kind described in paragraph 32, 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.
23. 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 web content which 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.
24. Social media, including chat rooms may only be accessed out of working hours, in line with our Social Media Policy.

Personal use of our systems

25. We permit the incidental use of our internet, email and telephone systems to send personal email, 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.
26. Personal use must meet the following conditions:
    (a) Use must be minimal and take place substantially out of normal working hours.
    (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 and our other policies.

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

Monitoring

28. Our systems have the facility 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, use of our systems including the telephone and computer systems, and any personal use of them, may be 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.
29. 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 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.

Prohibited use of our systems

30. 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 circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by 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 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, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties).
    (f) Any other statement which is likely to create any criminal or civil liability (for you or us).
    (g) 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.

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

Equipment security and Passwords

32. Anyone who has access to KGPC's IT resources are responsible for choosing strong passwords and protecting their log-in information from unauthorised people. You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.
33. You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.
34. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the CQC compliance specialist.

Password Creation

35. All passwords should be reasonably complex and difficult for unauthorised people to guess. You should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
36. In addition to meeting those requirements, you should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.
37. A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalisation. For example, the phrase "This may be one way to remember" can become: "TmB0WTr!".
38. Employees must choose unique passwords for all of their company accounts, and may not use password that they are already using for a personal account. All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.
39. If the security of a password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the password must be

changed immediately. Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

40. You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly.

41. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by the CQC compliance specialist. On the termination of employment (for any reason) you must provide details of your passwords to the CQC compliance specialist and return any equipment, key fobs or cards.

42. If you have been issued with a laptop, tablet computer, BlackBerry, 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 kept 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, for example, passengers on public transport.