MEDICUS HEALTH PARTNERS
Forest Road Group Practice Lincoln Road Medical Practice* Curzon Avenue Surgery*
Dean House Surgery Connaught Surgery* Freezywater Primary Care Centre*
Riley House Surgery Moorfield Road Health Centre* Green Street Surgery*
*Carlton House Surgery*Enfield Island Surgery* Willow House Surgery*
*Southbury Surgery*Bush Hill Park Medical Centre*Trinity Avenue Surgery
1st Floor Forest Primary Care Centre 308A Hertford Road Edmonton,
London N9 7HD

IT and Communications Systems Policy

Amendment history			
This policy will be reviewed annually			
Date	**Version**	**Author/Contributor**	**Amendment details**
27/07/2019	01	MHP	MHP standardised policy to be used across all sites
25/03/2020	02	MHP	Updated template to include Trinity Surgery

Contents

IT and Communications Systems Policy

Our IT and communications systems and all related software (referred to below as "information 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.

This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers, agency workers and anyone else who has access to our IT and communication systems wherever they are working and whether during working hours or not.

Misuse of information 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.

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

Responsibility for this policy The Medicus Health Partners board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to Site Managers.

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.

The managing partner and IT lead will deal with requests for permission or assistance under any provisions of this policy, and may specify certain standards of equipment or procedures to ensure security and compatibility.

Equipment security and passwords

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.

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.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting GP IT Department.

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. 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. On the termination of employment (for any reason) you must provide details of your passwords to your line manager and return any equipment, key fobs or cards. 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.

Systems and data security

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

You must not download or install software from external sources without authorisation from the IT Department. 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, you should seek advice from the IT Department.

You must not attach any device or equipment to our systems without authorisation from the IT Department. 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.

We monitor all emails passing through our 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 IT Department 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.

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.

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 subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

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 and via NHS Mail. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

You should access your NHS emails at least once every working day to stay in touch by remote access when working across practice sites, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked “high priority” within 24 hours.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via email should inform their line manager or managing partner.

You should take care with the content of 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.

Email messages may 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.

You should not:

1. Send or forward private emails at work which you would not want a third party to read;
2. Send or forward chain mail, junk mail, cartoons, jokes or gossip;
3. 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;
4. Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

5. 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;
6. Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
7. Send messages from another person's email address (unless authorised) or under an assumed name; or
8. Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

If you receive an email in error you should inform the sender.

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.

Using the internet

Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out below.

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. 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 "Prohibited use" below.

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, 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.

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.

The following must never be accessed from our network: online radio, audio and video streaming, instant messaging and webmail (such as such as Gmail or Hotmail) and social networking sites (such as Facebook, Twitter, Bebo, Instagram, YouTube, Second Life). This list may be modified from time to time.

Personal use of our systems

We permit the incidental use of our information 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 its discretion.

Personal use must meet the following conditions:
1. Use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);
2. Personal emails should be labelled “personal” in the subject header;
3. Use must not interfere with business or office commitments;
4. Use must not commit us to any marginal costs; and
5.Use must comply with this policy and our other policies including the Equal Opportunities Policy, Harassment Policy, Data Protection Policy.

You should be aware that personal use of our systems may be monitored (see below) and, where breaches of this policy are found, action may be taken under the our Disciplinary Procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive.

Monitoring

Our information systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations as an employer, use of the information 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.

A CCTV system monitors the exterior and reception areas of the buildings of the practice sites 24 hours a day which are recorded.

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):

1. To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;
2. To find lost messages or to retrieve messages lost due to computer failure;
3. To assist in the investigation of alleged wrongdoing; or
4. To comply with any legal obligation.

Prohibited use of our information systems

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):

1. Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
2. Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
3. A false and defamatory statement about any person or organisation;
4. Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equality Policy or Harassment and Bullying Policy);
5. Confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
6. Any other statement which is likely to create any criminal or civil liability (for you or us); or
7. 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.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with the 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.