Property of Urgent Care 24 Uncontrolled copy when printed

Not to be used without permission of the Board of Urgent Care 24

NHS
Urgent Care 24

Internet & Email Policy

Version	1.3
Location	Policy Folder – Information Technology
Approving Committee:	Urgent Care 24 Executive
Date Ratified:	March 2011
Reference Number:	UC24POL5
Name/Department of originator/individual:	James Carr, Director of Service Delivery and Operational Performance
Name/Title of responsible committee/individual:	Joseph Okwu, IM&T Manager
Date issued:	17 March 2011
Next Review date:	June 2019
Target audience:	All employees, Associate GPs

Version	**Date**	**Control Reason**
1.1	20th November 2012	Version changed, Title of originator amended to new Title name. Associate GPs added to target audience. Director of IM&T title changed to Director of Service Delivery and Operational Performance.
1.2	28th July 2014	Reviewed in line to Annual Review Date.
1.3	4th June 2018	Reviewed in line to Annual Review Date; Name of Responsible Individual updated to reflect current information. Section 4.1.3 updated, 'Facebook'

		removed and replaced with ‘Social Networking’.

CONTENTS

1.0 Purpose 3
2.0 Scope 3
3.0 E-mail 3
3.2 Internal E-mail........ 3
3.3 Internet (external) E-mail 4
4.0 The Internet 4
4.1 Access 4
5.0 Browsing on the Web 5
6.0 Downloading Information........ 5
7.0 Equality and Diversity & Dignity at Work 5
8.0 Security of Information and Storage 6
9.0 Implementation monitoring & review 6

1.0 PURPOSE

1.1 The purpose of this policy is to outline Urgent Care 24's (UC24) policy on the access too and use of E-mail and Internet services within the organisation.

1.2 Urgent Care 24 recognises that the use of technology for communication in the working environment is increasing, and is both quick and efficient, but also recognises the need to determine parameters for the access and use of such services during working time.

1.3 Misuse of any UC24 IM&T equipment or systems under this policy may be viewed as Misconduct/Gross Misconduct and may result in disciplinary action under UC24 Disciplinary Procedure or in the case or Associate GPs locums no further work being offered. It is important that all users are aware of this policy and read its contents.

1.4 The aim of the policy is to enable UC24, its employees, Associate GPs, Locums and anyone working on behalf of UC24 to gain maximum value from e-mail and the Internet, but also to alert all users to the dangers that can arise if the technology is misused, and to the consequences of misuse.

1.5 The IM&T facilities and systems are UC24 property, and are intended for business use. Whilst personal use is prohibited, this must be within the guidelines outlined below.

2.0 SCOPE

2.1 This policy applies to all employees of UC24, Associate GPs, Locums and anyone working on behalf of UC24 (for the purpose of this policy all these groups will be referred to as users.)

3.0 E-MAIL

3.1 Inappropriate (Jokes, images) or emails should not be sent to other UC24 colleagues, anyone working on behalf of the organisation or to any other external sources.

3.2 **Internal E-mail**

All users have access to the internal Adastra e-mail system which is used for internal communications. Each individual user will have a user name and password that is unique. Passwords **must not** be shared with other users and should be changed from time to time to guard against unauthorised access. If anyone becomes aware that others may know their password, they must change the password immediately.

To prevent unauthorised e-mail access or use, anyone using the computer should log off or lock their computer when it is unattended.

3.3 Internet (external) E-mail

3.3.1 E-mail is now available to a large number of UC24 staff, and promotes efficient and effective communications across the organisation. Accounts must be set up by the IM&T Department, who will also set the access parameters for the system.

3.3.2 Internet e-mail is not a secure method of data communication. The sending of confidential information by e-mail should be minimised, and if unavoidable, the sender should take steps to ensure that the e-mail can only be received and read by the intended recipient.

3.3.3 The UC24 disclaimer must be applied to all e-mail messages sent externally.

3.3.4 Care must also be taken when opening e-mail attachments received from external sources as these may contain viruses. Any concerns should be raised with the IM&T Department. For general guidance on downloading information and anti-virus procedures, see Section 7 of the policy, and UC24 Information Security Policy.

3.3.5 Internet (external) e-mail should principally be used for business purposes. Whilst personal use is prohibited, this should be limited to occasional use in the same manner that occasional personal use of the telephone is permitted. Individuals must be aware that use of e-mail will be monitored and that consequently high personal usage levels will be identified and may be grounds for action.

3.3.6 By using e-mail facilities (either internal or external), users accept that UC24 reserves the right to monitor individuals' use of e-mail, and take action in any cases where the e-mail facility is being abused. The content of e-mails must not be in breach of other UC24 policies such as Bullying and Harassment, Equality and Diversity.

4.0 THE INTERNET

4.1 Access

4.1.1 Access to the Internet must be arranged by the IM&T Department. The IM&T Department may also set restrictions on sites that can be accessed.

4.1.2 The Internet should principally be used for business purposes. Whilst personal use is prohibited, this should be limited to occasional use in the same manner that occasional personal use of the telephone is permitted. Individuals must be aware that use of the Internet will be monitored and that consequently high personal usage levels will be identified and may be grounds for further action.

4.1.3 Social networking, gaming and gambling websites have been recognised as being accessed too often, access to these web-sites is not authorised and may result in disciplinary action.

4.1.4 The above guidelines apply equally to the use of any equipment which is the property of UC24 (i.e. PCs located at Urgent Care 24 premises and portable computers, whether located at Urgent Care 24 premises or at employees' homes or any other location or mobile phone devices). Employees who have their own portable computer equipment are not permitted to use UC24 network to access the Internet.

5.0 BROWSING ON THE WEB

5.1 Once Internet access has been provided, employees must be aware that browsing on the Web can be both time-consuming and unproductive and should therefore only be accessed during official breaks not during working time. Time spent on the web should be limited in general to:

- Searching for information that is necessary for the individual to do their job
- Occasional personal use e.g. booking of travel tickets, but not extensive browsing of web sites, chat rooms and bulletin boards

5.2 Any purchases made on UC24 behalf over the Internet must be made from secure sites (denoted by a padlock symbol on screen). Browsers must be set to notify the user when entering and leaving secure sites. Disabling of such warnings is forbidden.

6.0 DOWNLOADING INFORMATION

6.1 Although it is possible for the IM&T Department to bar access to certain sites, the Internet is growing so rapidly that it is impossible to prevent all access to inappropriate sites. Downloading of material that could be considered offensive, obscene or indecent is strictly forbidden. If such material is accessed by employees this may lead to disciplinary action.

6.2 Downloading information also brings the risk of importing a virus that could pose a risk to the entire network. All machines with Internet access must also be fitted with anti-virus software. Attempts to disable virus protection or content software will be treated as disciplinary offences.

6.3 No unauthorised software should be downloaded or installed from the Internet. In addition no employee should introduce external software, hardware or discs unless this has been checked by the IM&T Department and is virus free - this also includes information that can be downloaded onto machines from mobile phones, flash (pen) drives and I-pods. For further guidance see UC24 Information Security Policy.

6.4 As a rule all software for use within UC24 should be obtained from controlled sources by the IM&T Department.

7.0 EQUALITY AND DIVERSITY & DIGNITY AT WORK

7.1 UC24 IT equipment may not be used for

- The transmission of any material that infringes the copyright of another person
- Violating the privacy of other users
- Disrupting the work of other users
- The creation, use, retention, distribution or transmission of any offensive, obscene, pornographic, or indecent images, data, software or other material
- Material which is designed to cause annoyance, inconvenience or needless anxiety
- Materials that are, or might be offensive or abusive in that its content is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful.
- Material which potentially infringes other UC24 policies e.g. bullying and Harassment, Equality and Diversity

7.2 This list is not exhaustive and there may be other instances of unacceptable use.

7.3 Users should also be aware that in the vast majority of UC24 premises including the call centre, the actual connection to the internet is provided by the building's owners and not UC24. As part of this agreement to use such connections we are bound by the procedures of the particular Trust. Therefore should there be an incident regarding inappropriate use of the connection, Urgent Care 24 would have to consider the disciplinary procedures of that Trust in conjunction with our own.

8.0 SECURITY OF INFORMATION AND STORAGE

8.1 Security and confidentiality of information is of prime concern to Urgent Care 24 and all confidential, personal, or patient information must be safeguarded against unauthorised access. Further details of this are set out in UC24 Information Security Policy, which is available to all users.

8.2 Staff must not create forward rules on their UC24 accounts and direct their work emails to a personal account (e.g. Hotmail, Google, Yahoo or other email accounts) outside the organisation.

9.0 IMPLEMENTATION MONITORING & REVIEW

9.1 All users must be aware that all e-mail and Internet communications via UC24 equipment may be subject to daily monitoring to ensure that use is in compliance with this policy.

9.2 Users should be aware that N3 connected computers pass through sophisticated firewall and content screening devices which are capable of logging the exact information that has been accessed together with the time and date of when access was attempted. Such information would be used as evidence should an incident be brought to the attention of the IM&T Department.

9.3 Managers are responsible for ensuring the efficient use of services and systems in accordance with this policy and for ensuring that employees are aware of the policy and any subsequent changes to it.

9.4 The HR team are responsible for ensuring that all new employees receive a copy of this policy, and sign a copy of the Information Security Agreement to ensure they have read it. Individual signed documents will be held on personal files.

9.5 This policy will be reviewed on at least an annual basis owing to the pace of change and to reflect current employment legislation.