NHS
West Essex
Clinical Commissioning Group

Acceptable Use of Electronic Communications Policy

Policy Reference: IG10

Brief Summary: This policy provides guidance to all staff on appropriate and inappropriate use of electronic communications and computer systems such as e-mail, internet, telephones, mobile devices and remote working across the CCG.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	03/11/2014	Draft	New Document	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.2	07/12/2014	Draft	Amended following from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.3	05/03/2015	Final	Approved by West Essex CCG	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
0.4	07/10/2016	Final	Approved by West Essex CCG Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019
Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

NHS West Essex Clinical Commissioning Group (the CCG) recognises that the safety and uses of its computers and other electronic communications, including portable and mobile device systems, is an integral part of its business and commitment to improve the quality of services and the safety of staff and members of the public.

Staff are now able to gain access, including remotely, to information and work systems from multiple devices in numerous locations It is therefore of vital importance to ensure that computer usage and electronic communications such as e-mail and the Internet are effectively managed and that appropriate policies and guidance are in place for all staff.

For the purpose of this policy electronic communication facilities include but are not limited to:

- Electronic Mail
- Internet usage
- Remote / home working
- Use of Personal Computers (PCs), laptops, tablets, Personal Digital Assistants (PDA)
- Telephone usage (including mobile phones, Dictaphones, voicemail)

2. Purpose

The Acceptable Use of Electronic Communications Policy has been produced to protect:

- The privacy of patients' / service users, staff and other personal information held on the CCG's systems in accordance with the national information governance agenda.
- The integrity of the CCG's systems including reliability, availability, correctness and completeness of data.
- The CCG and their staff from allegations of inappropriate or profligate use.
- The privacy of electronic communications to and from CCG staff.
- All systems "stakeholders" from malicious attack, including viruses, offensive and pornographic materials.
- The intellectual property rights of the software providers.

3. Scope

The scope of this policy is to provide guidance to all staff on appropriate and inappropriate use of electronic communications and computer systems such as e-mail, internet, telephones, mobile devices and remote working across the CCG.

This policy also applies to all staff entrusted with a supplied portable computing and data storage device, staff working with the CCG's information or accessing the CCG's network remotely from a location which is not a routine work base, or using equipment that is not directly managed by the CCG IT provider. Staff compliance with this policy covers:

- Acceptable and unacceptable use of the CCG's telephone, e-mail and internet
- Connection to the CCG's network which includes remotely and with portable devices
- The processing of the CCG's information away from the organisation's premises
- The secure transfer of information
- The security of portable devices and information
- The use of home computers and personal mobile phone and tablet services.

All staff are advised to familiarise themselves with this policy and to have due regard for professional behaviour and etiquette when working for, or on behalf of, the CCG.

4. Definitions and terms

Staff: Individuals working for or on behalf of the organization, including permanent, temporary, agency and contractors.

The use of portable computing and data storage devices includes:

- Laptops
- Notebooks
- iPads / iPods or other similar devices (tablets) capable of connecting (whether by a 'wired' or wireless connection) to a computing device and storing information
- Smartphones which are capable of connecting to a wired or wireless connection and are able to store a wide range of information
- External portable Hard Disk Drives (HDDs)
- USB Memory or 'Flash' Sticks and memory cards, capable of storing information
- Solid state memory cards capable of storing information and being connected to the organisation's computing devices either by themselves or via another device
- Future technologies, for example, Google Glass

Media Supporting Storage includes (but is not limited to):

- Floppy Disks
- CD Disks, both recordable (CDR*) and Re-writable (CDRW*)
- DVD/Blue-ray disks, both Recordable (DVDR*) and Re-Writable (DVDRW*)
- Paper output from printers

- Legacy storage systems – for example: Zip disks and other magnetic tapes capable of recording and storing

Remote working is accessing the organisation's resources whilst working away from a normal fixed place of work, via any of the following:

- Mobile computing: this is working at any location using mobile devices and / or removable data
- Virtual, tele and homeworking: Working at any location other than your normal work base requiring periods of access to CCG information resources
- Remote connection: authorised staff can access data held on the organisation's secure server remotely using a strongly authenticated VPN (Virtual Private Network). The system allows access from any internet connection with a CCG owned asset. It is not possible to use a VPN via your own home PC.

5. Roles and Responsibilities

5.1 Accountable Officers for NHS West Essex CCG

The Chief Officer, as the Accountable Officer, has overall responsibility for information governance within the CCG. The Chief Officer is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Chief Officer has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance.

5.2 Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

5.3 Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

5.4 All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

5.5 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate these.

5.6 Information Asset Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

6. Conduct and Use

The CCG's primary aim in providing electronic communication facilities is to support and enable the delivery of the highest quality service to patients and service users.

In the event of any untoward activity the CCG will proceed to act in accordance with the organisation's disciplinary procedures.

The CCG will always comply with any reasonable request from law enforcement and regulatory agencies for logs, diaries and archives on an individual's electronic communication activities.

Staff are expected to conduct themselves honestly and respect copyright, software licensing rules, property rights, the human rights and privacy of users. When using electronic communications staff are expected to use common sense to ensure that the use of these facilities does not leave the CCG or them personally open to a legal challenge.

The CCG does not accept liability for any fraud or theft that results from personal use of the CCG's electronic communications facilities.

6.1 Acceptable use of internet and e-mail

Staff are encouraged to use the internet and e-mails to further the goals and objectives of the CCG. The types of activities which are encouraged include:

Communicating with colleagues, business partners of the CCG and suppliers within the context of an individual's assigned responsibilities.

Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

Personal educational research and recreational use of internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, or the work of others.

6.2 Unacceptable use of internet and e-mail

Personal internet and e-mail use should not interfere with others productive use of resources. Internet and e-mail use must comply with all UK laws, CCG policies and contracts. This includes, but is not limited to, the following:

- The internet must not be used for illegal purposes, including but not limited to: copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation and bullying, forgery, impersonation, gambling or computer tampering (for example spreading computer viruses)

- Offensive, abusive, bullying, harassing, homophobic, sexist, racist, hateful or otherwise discriminatory material;

- Use of the internet in a manner that is not consistent with the strategic objectives or values of the CCG, misrepresents the organisation or violates any of it's policies.

- Access to the CCG's resources or network facilities for those who are not staff (see Staff definition in Point 4) are prohibited, as well as the use for mass unsolicited mailings, uploading and downloading of files for personal use, access to pornographic sites, gaming, dissemination of chain letters and competitive commercial activity unless pre-approved by the CCG.

- Staff should not view, copy, alter or destroy data, software, documentation or data communications belonging to the CCG or other staff without authorised permission.

Any e-mail use that includes creating, sending and forwarding messages containing any of the following may be considered gross misconduct:

- Material that brings the organisation or a colleague into disrepute

- Pornographic, obscene, indecent or sexually explicit material

- Illegal material

- Material which makes improper or defamatory reference to the protected characteristics groups as defined by the Equality Act 2010

- The use of copyright material or the work of third parties without prior consent

- Unsolicited commercial or personal advertising material

- Viruses, spy-ware or mal-ware
- Personal opinions represented as that of the CCG
- "Mass mailing" information, except for important CCG business.

6.3 Criteria for determining acceptable use of internet and email

The following should be considered when deliberating on the acceptable use of the internet and e-mails:

- How it may affect your own work and that of your colleagues
- The impact to the department's service delivery and performance.

6.4 Good housekeeping

- E-mail capacity is not unlimited. All nhs.net e-mail accounts will issue a warning when the mailbox is 90% full. Once full you will not be able to send but will continue to be able to receive a further 200MB of mail before inbound messages will be rejected. Therefore, regular housekeeping is required and e-mails should be deleted, archived or stored as appropriate.
- In the interests of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files, other than those necessary for business purposes and which cannot be accessed through a shared drive. The size and restriction on sending a single email is 20MB. Sending e-mails with large attachments can adversely impact the performance of the network.
- Senders should be aware of the general availability of e-mail addresses, so that urgent information does not lie unread and a reply indicator should be used. Staff should therefore make appropriate use of the Out of Office Assistant facility indicating date of return and alternative contact details.
- Facilities for diverting e-mails during staff absences or for administrators or personal assistants having access to a manager's e-mail inbox should be used within the constraints of confidentiality.

Please note the size of the e-mail is more important than the number.

6.5 Access to another individual's mailbox

In circumstances (such as sick leave or personal emergencies), where delegated access has not been given and there is an immediate business need to have access to information held in a user's account, then the following process should be followed:

- The senior manager of the nominated staff should contact the IT service provider for access.

- Based on the business need, in the case of access to a mailbox, the request should clearly state if access to the inbox is required, or the entire mailbox including sent items and sub folders.

- Based on business need, in the case of access to a personal drive, the request should state if access to the entire personal drive is required, or if access to a specific file is required

- The staff should be informed of the access, the business justification and the nominated individual who had this and the period of time.

7. Telephone Usage

Voicemail

It may be necessary for the CCG to access voicemail in the case of staff absence, in which case the same process as that for accessing e-mail accounts will be used. However, due to the nature of voicemail it may not be possible to bypass personal messages.

8. Portable computing devices

All staff authorised to use the CCG's portable computing devices must:

- Take all reasonable care to prevent the theft or loss of these devices

- Ensure that the devices are not left unattended for example in a public place or in vehicles

- Take extra vigilance when using any portable computing device during journeys on public transport to avoid the risk of its theft or unauthorised disclosure of the organisation's stored information by a third party "overlooking"

- Ensure that 'non-authorised' users are not given access to the device or the data it contains

- Ensure that the portable device is encrypted

- Ensure that any suspected or actual breaches of security are reported to the assigned Information Asset Owner and the Head of Information Governance

- Ensure that unauthorised software is not installed on the device

- Ensure that information is virus checked before transferring onto the organisation's computers. This will be done automatically for information that is sent via e-mail.

Where it is not possible to encrypt sensitive / personal information, the advice of the assigned Information Asset Administrator (IAA) and the Information Governance Team is to be sought and,

where no solution can be found, the risk is to be articulated to the Senior Information Risk Owner (SIRO) in the CCG

Confidential information should only be stored on a portable device with the permission from the assigned Information Asset Owner (IAO). This should be recorded on the department's Information Asset Register and an updated copy sent to the Information Governance Team.

Where available, only NHS Digital (formerly HSCIC) approved encryption products are to be utilised to secure sensitive / personal information. Where no such products exist the advice of the assigned IAO / IAA or the Information Governance Team is to be sought in all cases.

Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available and the contents must be encrypted.

8.1 Use of non-corporate portable devices

Only CCG assets (or those on an approved list) may be connected to the network. If in doubt, then please refer to the IT Department.

8.2 Return of portable devices

Staff including temporary or contract staff leaving the CCG should return the portable device to their line manager, IAO, IAA or the CWS Head of Strategic IT. All media containing the organisation's information must be returned for retention or appropriate destruction.

9. Tablets

Tablets such as iPads are powerful mobile computing devices, enhanced by a host of readily available applications (apps) developed by 3rd parties. It is important to realise that these apps are not controlled by the NHS and that data moved, manipulated or stored using these apps may not be secure and may contravene UK legislations.

To comply with NHS Information Governance requirements great care must be taken if equipment is used with cloud services. Data governed by the Data Protection Act must not be used or accessed via cloud services without permission from the Information Governance Team, as this risks the data being stored outside of the European Economic Area.

If in doubt, disable the cloud services on your device will ensure data is not inadvertently transferred. Guidance on use of applications can also be provided by the IT Department

10. Remote working

Remote working applies to the use of the CCG's systems and assets for example laptops, tablets, mobile phones and also the use of personal, or other, computer equipment whenever work is undertaken away from CCG premises.

Remote workers must:

- Password protect any work which relates to the CCG's business so that no other person can access the work
- Be positioned to ensure that work cannot be seen by any other person whom it does not concern
- Take reasonable precautions to safeguard the security of the CCG's equipment. This includes not leaving portable media unattended, including in the boot of a car and keeping passwords secret
- Inform the CCG as soon as possible, if either the CCG's equipment in their possession or any computer equipment on which work is undertaken, even if this is personal IT equipment, has been lost or stolen and
- Ensure that any work undertaken remotely is saved on the CCG system or is transferred to the CCG as soon as reasonably practicable.

11. Audit and Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external assessments or other sources of information and advice.

12. Dissemination and Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

13. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

14. Related documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Information Governance Policy
- Confidentiality & Data Protection Act Policy
- Information Sharing Policy
- Safe Haven Policy
- Information Security Policy
- Information Lifecycle Management Policy & Strategy
- Information Risk Policy

15. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are

treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

16. Key Contacts within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance.
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net