NHS
Herts Valleys
Clinical Commissioning Group

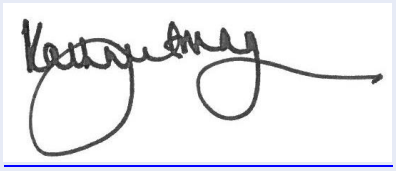
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Email and Internet
Could this policy be incorporated within an existing policy?	No	
Does this policy follow the style and format of the agreed template?	Yes	
Has the front sheet been completed?	Yes	
Is there an appropriate review date?	Yes	
Does the contents page reflect the body of the document?	Yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	No	Policy about usage of IT resource
Are all appendices appropriate and/or applicable?	Yes	
Have all appropriate stakeholders been consulted?	Yes	
Has an Equality Impact Assessment been undertaken?	Yes	
Is there a clear plan for implementation?	Yes	
Has the document control sheet been completed?	Yes	
Are key references cited and supporting documents referenced?	Yes	
Does the document identify which Committee/Group will approve it?	Yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)	Yes	Will be published on intranet

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Chief Finance Officer	Date	13 March 2018
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Chief Executive	Date	13 March 2018
Signature			

Formatted: Font color: Text 1

NHS
Herts Valleys
Clinical Commissioning Group

Email and Internet Policy

Version Number	3.0
Ratified By	Senior Leadership Team
Date Ratified	13 March 2018
Name of Originator/Author	Trudi Mount, Head of IM&T Ruth Boughton, Information Governance Manager
Responsible Director	Chief Finance Officer
Staff Audience	All Staff
Date Issued	March 2018
Next Review Date	March 2019

NHS
Herts Valleys
Clinical Commissioning Group

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
0.1		First Draft	Mar 15	TLM
1.0		Final Version	Jul 15	TLM
2.0		Annual Review	June 16	RB
3.0		Annual Review Approved by the Virtual Information Governance Group Approved by the Executive Team	Dec 17 Jan18 March 2018	RB

NHS
Herts Valleys
Clinical Commissioning Group

CONTENTS

1. INTRODUCTION

This policy sets out the CCG's commitment to preserve the confidentiality, integrity and availability of electronic communications and to ensure that such communications are effectively and lawfully managed.

2. PURPOSE

This policy aims to ensure that:-

- Email and the internet as used by the CCG is secure and operated in accordance with relevant guidelines.
- That the confidentiality and integrity of information sent via Email is maintained at all times.
- Staff are aware of their responsibilities and adhere to the policy.
- Procedures are in place to detect and resolve possible security breaches.

3. DEFINITIONS

3.1. Email

Refers to all Email services used by the CCG – including NHS Mail accounts and the policy applies to all sites where Email can be accessed.

3.2. Internet

Refers to all internet sites used by the CCG and its staff from all locations where the internet can be accessed.

3.3. Users

All staff employed by the CCG both in permanent roles, contracts and on secondment are required to comply with this policy.

4. ROLES AND RESPONSIBILITIES

4.1. Roles and Responsibilities within the Organisation

All staff have a responsibility to act in compliance with this policy when using Email and the internet.

Managers should ensure staff are aware of the policy and that staff act in accordance with this policy.

4.2. Consultation and Communication with Stakeholders

This policy has been developed by the CCG's ICT Provider in conjunction with the CCG Head of IM&T and Information Governance Manager.

5. CONTENT

The CCG's ICT provider has a comprehensive Email and Internet Policy, see Appendix A, which all CCG employees must abide by. Below is a summary of this policy and its main salient points. All staff should read the full document.

5.1. Electronic Mail and Internet Services

E-mail and Internet services are provided solely for the conduct of official CCG business and are subject to the CCG's Information Security Policy.

These services and the associated systems and information are the property of the CCG. This includes all hardware, software and all data that are stored within the systems, any messages, attachments and downloads.

5.2. Permissible Uses of Electronic Mail and Internet

5.2.1. Authorised users

Staff will be given a username and/or a smartcard and a password to access their computer and systems they are authorised to use. Contractors and other persons working on behalf of the CCG may be given authority to use these services in accordance with relevant policies.

5.2.2. Purpose and use

Email and Internet resources usage must be related to the legitimate business activity of the CCG or its partners.

Incidental and occasional personal use of Email and Internet may be permitted at the discretion of the appropriate senior manager. Any personal use will also be subject to the provisions of this policy

5.2.3. Transmission of Confidential Information

All personal confidential data (PCD) must be encrypted, in accordance with Department of Health standards, before or during transmission. Refer to Appendix C of this document [Guidance on the use of E-Mail when sending PCD] and the NHS Mail Guidance for further information

All exchanges or transmission of unencrypted PCD must have the prior authorisation of the CCG's Caldicott Guardian and/or SIRO.

5.2.4. Prohibited uses of e-mail and internet

CCG staff should not:-

- Use another person's identity (username/password or smartcard) to access E-Mail and Internet services;

- Use E-Mail and the Internet for personal monetary gain or for commercial purposes that are not directly related to the CCG's business;
- Personal use that creates a cost or inconvenience for the CCG;
- Intercept or open Email or electronic files addressed to another recipient without their permission (except for authorised employees in the course of the CCG's business);
- Use Email to harass or intimidate others or to interfere with the ability of others to conduct the CCG's business;
- Disguise an Email identity in an attempt to deceive the recipient of the source or identity of the sender;
- Use Email for any purpose restricted or prohibited by law or regulations;
- Include work in Emails that violate copyright laws. Employees have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding Emails and attachments;
- Attempt unauthorised access to Email or attempt to breach of any security measures on any systems;
- View, distributing or contribute to illegal or inappropriate materials on the internet, including material that might be offensive to others;
- Distribute chain letters, inappropriate humour, explicit language or offensive images or material;
- Download any files that could jeopardise the security and integrity of the CCG's networks or systems;
- Make excessive use of work time and facilities for private purposes.
- Send and receive NHS related information, especially PCD using public Email systems (Gmail, Hotmail, Yahoo, Facebook, Twitter etc.) other than in compliance with Appendix 3 of this document and policy document [Guidance on the use of E-Mail when sending PCD] or as part of an approved CCG communications strategy (e.g. CCG Twitter accounts)

5.2.5. Restrictions on Internet Sites

Restrictions will be placed on access to any internet site that could be regarded as a threat to services, systems and resources, that interferes with the use of the network or other services or to any site that is considered inappropriate.

This will include, (but is not limited to):

- Sites that attempt to propagate malicious code or any other threat;
- Sites containing information that is inappropriate, offensive or unlawful, (such as pornography, racial bias, social networking, gambling and games)
- Downloads or data transfers that threaten or interfere with network or other resources (such as executable files and media streaming)
- Sites that provide 'cloud-based' storage functionality (such as huddle, SkyDrive, iCloud, Dropbox, etc.) except where explicitly approved

Variation/s to this policy must be made to the HBL ICT Head of Infrastructure and must be approved by the HBL ICT Director of ICT Services and the CCG Head of IM&T/IG Manager.

Restrictions may be changed or introduced without notice or consultation to preserve the confidentiality, integrity and availability of critical network resources.

5.2.6. Unsolicited or 'junk' mail

This is Email received from senders you do not know or companies you do not do business with. Examples are unsolicited advertising for goods or services or warnings of supposed new viruses. These Emails should be deleted without opening them. Do not forward or reply to such Emails or visit sites contained in such Emails.

6. MONITORING COMPLIANCE

This policy will be reviewed annually in line with the CCG ICT Provider policy refresh. The policy is the responsibility of the CCG Head of IM&T/IG Manager.

Any incidents arising that relate to the use of Mobile Computers/Storage Devices will be reported via the CCGs Incident Reporting process.

Compliance with this policy will be monitored both electronically and by means of audits and spot checks.

6.1. Disciplinary Action

Breach of any aspect of this policy will be subject to disciplinary action in line with the CCG's disciplinary policies. Serious breaches will be regarded as gross misconduct and may result in dismissal.

6.2. Access and disclosure of electronic communications

6.2.1. General Provisions

As far as is permitted by law the CCG reserves the right to access and disclose the contents of any email or electronic communications without the consent of the user. This right will be exercised when there is believed to be a legitimate business reason to do so including, but not limited to, those listed in Paragraph 6.2.3 below and with the authority of a Director of the CCG.

Email may constitute "personal records" and be subject to the provisions of the Data Protection Act 1998 and the Access to Health Records Act. The data subject has the right to access any such records.

6.2.2. Monitoring of communications

To the extent permitted by law, all electronic communications and their content will be monitored for purposes of:

- Ensuring compliance with the CCG policies and procedures and compliance with legislation and statute law

The CCG retains the right to access, review, copy and delete any material created, stored or transported on its systems. This includes but is not limited to messages sent, received or stored on the email system and any material accessed or downloaded from the internet.

Volumes of electronic communication will be monitored routinely including the source, destination and subject of the communication.

6.2.3. Inspection and disclosure of communications

The CCG reserves the right to inspect and disclose the contents of electronic communications:

- To discharge legal obligations and legal processes and any other obligations to employees, clients, patients, customers and any third parties (in particular, when disclosure is requested under provisions of the Data Protection Act(1998)/ GDPR (General Data Protection Regulations) or the Freedom of Information Act(2000)).
- To locate substantive information required for the CCG business that is not readily available by other means.
- To safeguard assets and to ensure they are used in an appropriate manner.
- In the course of an investigation into alleged misconduct,

6.2.4. Special procedures for monitoring and disclosure.

Prior approval must be obtained from the appropriate Director to gain access to the contents of electronic communications or data stores, and disclose information gained from such access.

7. EDUCATION AND TRAINING

All staff should read this policy as part of their induction.

8. REFERENCES

This policy is compliant with relevant legislation, Department of Health and NHS regulations and guidance and the policies and procedures of partner organisations; principally:-

- UK and EU legislation, including :
  - Data Protection Act (1998),
  - General Data Protection Regulations (GDPR) replaces DPA in May 2018.
  - Freedom of Information Act (2000);
  - Human Rights Act (1998)
  - the Computer Misuse Act 1990,
  - Communications Act (2003) & Electronic Communications Act (2006)
  - Regulation of Investigatory Powers Act (2000)
  - Copyright, Designs and Patents Act (1988)
  - Health and Social Care Act 2012
  - Caldecott 2 Review
  - Care Act 2014
- Department of Health and NHS Regulations and Guidance, including :
  - Guide to Confidentiality in Health and Social Care
  - NHS IM&T Security Manual,
  - NHS Information Governance Standards
  - NHS Statement of Compliance

- Standards for Information Security Management ISO27001 & ISO27002
- Policies and procedures including:
  - Policies, procedure & guidance on the management of patient/client records

9. ASSOCIATED DOCUMENTATION

Standing Financial Instructions

Data Quality Policy

Information Security Policy

Information Risk Policy

Guidance on the use of E-Mail when sending PCD

NHS Mail Guidance – Sending an encrypted email and sharing sensitive information by email.

Mobile Device Security Policy

Telecommunications Policy

Information Governance Policy & Strategy

Incident Policy

Confidentiality Policy

APPENDICES

10. Appendix A

Email and Internet Policy 9.2.docx

11. Appendix B

Acronyms

NHS = National Health Service

CCG = Clinical Commissioning Group

IT = Information Technology

ICT = Information and Communications Technology

IM&T = Information Management and Technology

EU = European Union

SIRO = Senior Information Risk Owner

DH = Department of Health

UK = United Kingdom

PCs = Personal Computers

HSCIC = Health and Social Care Information Centre

PCD = Personal Confidential Data

12. Appendix C – E-Mailing Personal Confidential Data

The details within this Appendix are to be used as a supplemental guide to the document 'Guidance on the use of E-Mail when sending PCD'.

Introduction

The Secretary of State for Health has directed that all E-Mails containing personal confidential data must be encrypted unless there is some substantial reason that overrides or modifies the confidentiality due to the person - see Paragraph 14.6, below. This applies both to information in the body of the E-Mail or in any attachments to the E-Mail.

The Trust has 2 methods available for sending encrypted E-Mail and these are described below.

NHSMail Service

The NHSMail service is provided by the NHS nationally and available to all NHS staff. It is the only nationally approved method of sending PCD relating to patients.

NHSMail addresses take the form: *username@nhs.net*

The important part is the ***.nhs.net*** suffix which identifies it as an NHSMail address. (The Trust's standard E-Mail addresses have a suffix *.nhs.uk.* It is not an NHSMail service.)

Using the NHSMail service you can send E-Mails containing PCD to:

- Other NHSMail addresses i.e., with the suffix: *.nhs.net*
- To the secure E-Mail services with the following addresses:
  - username@hscic.gov.uk
  - username@x.gsi.gov.uk
  - username@gsi.gov.uk
  - username@gse.gov.uk
  - username@gsx.gov.uk
  - username@police.uk
  - username@pnn.police.uk
  - username@cjsm.net
  - username@scn.gov.uk
  - username@gcsx.gov.uk

You cannot send E-Mails containing PCD from your NHSMail account to any other address.

(If you do not have an NHSMail account you can enrol yourself at www.nhs.net or contact the ICT Service Desk)

- **Limited Facility on the Trust's Outlook Service**

The Trust's standard Outlook E-Mail service has an address in the form:

- **@hertfordshire.nhs.uk**
- **@hchs.nhs.uk**
- **@hertspartsft.nhs.uk**
- **@hpft.nhs.uk**
- **@enhertsccg.nhs.uk**
- **@hertsvalleysccg.nhs.uk**
- **@lutonccg.nhs.uk**
- **@bedfordshireccg.nhs.uk**

Please refer to document 'Guidance on the use of E-Mail when sending PCD' for further details.

When using Outlook encryption you need to be aware of the following limitations and take the recommended action:

- Outlook will warn you if it cannot encrypt the E-Mail. This can happen for a variety of reasons: the recipient cannot read encrypted E-Mail, it is being sent to a group address etc. You will need to use an alternative means of sending the person identifiable information.

- Encrypted Outlook E-Mails can only be read by the addressee and cannot be read by any delegates nominated by the addressee. You must address the E-Mail to all the people who need to read it.

- Encrypted E-Mails will not always be found when searches are performed for Data Protection Act or Freedom of Information Act requests. Encrypted E-Mails must be saved outside the Outlook system either by:

    - exporting them to a file and storing them on the appropriate place on SystmOne or a shared network drive;

    - or by printing them and filing the paper copy in the data subjects file.

As a general rule, Caldicott principles must be applied when sending E-Mails containing PCD. Such E-Mails should only be addressed to individuals who have a right to see the information; **such E-Mails must never be addressed to a circulation list**.

- **E-Mailing information to Patients/Service Users**

PCD may be sent to the patient/service user it relates to by E-Mail provided the person has given their consent.

This consent and the E-Mail address must be obtained in writing – not by E-Mail – and the E-Mail address verified before personal information is sent.

Please refer to document 'Guidance on the use of E-Mail when sending PCD' for further details.

- **Exceptions to the Encryption Rules**

There will be circumstances when the need to send information quickly is of greater importance than maintaining confidentiality, e.g. in the best interests of the data subject.

You must seek the advice of the Trust's Caldicott Guardian in these circumstances. Exception can be made on a case by case basis or for a specific regular information exchange. Such exception will be recorded in the Trust's Caldicott Issues Log.

NHS
Herts Valleys
Clinical Commissioning Group

Appendix D -

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Email, Intranet and Internet Policy
What is it that is being proposed?	This policy sets out the CCG's commitment to preserve the confidentiality, integrity and availability of electronic communications and to ensure that such communications are effectively and lawfully managed
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements and CCG processes.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets out the information governance requirements in relation to sending emails and use of the intranet/internet.
On what evidence/information have you based your decision?	The policy refers to the safe sending of information and safe and appropriate use of the internet
How will you monitor the impact of policy or service?	Via the IG Toolkit
How will you report your findings?	To the Senior Leaders Team via toolkit action plans and compliance reports

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact

Assessment is not required.	
Assessors Name and Job title Date 02/01/2018	Ruth Boughton Information Governance Manager