Email Usage Policy

Lead Manager	**Head of IT Infrastructure**
Responsible Director	**Director Health Information & Technology**
Approved By	**Information Governance Steering Group**
Endorsing Body	**Corporate Management Team**
Date Approved	**September 2015**
Review Date	**September 2017**
Version No.	**5.2**

CONTENTS **PAGE NO.**

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Isobel Brown, Information Governance Manager • Mike Dench, IT Security Manager
Consultation Process / Stakeholders:	• Information Governance Steering Group members (which includes staff partnership representatives). • Head of Applications and IT managers
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
21/2/14	M Dench	This version introduces the concept of where emails can be sent based upon their security classification.	4.0
10/6/14	R Wright	Edited in content and format to reflect consultation discussion	5.0
29/10/14	M Dench	Additional Paragraph in section 4 – Generic Mailbox Use	5.1
14/9/15	M Dench	Additional secure route to Renfrewshire Council shown in section 5	5.2

Any queries relating to this Policy – contact IT Security Manager at mike.dench@ggc.scot.nhs.uk

1. Introduction

This policy is intended to ensure safe, effective and efficient email use and forms part of the overall Information Security policy for NHS Greater Glasgow & Clyde (NHSGGC).

2. Aim, Purpose and Outcomes

To provide an assured framework within which the security, confidentiality, integrity and safe use of data and information is maintained through:

- data and information is available only to those authorized to view it;
- data and information is not disclosed to those without the authority to use it;
- the inappropriate destruction of information is avoided;
- staff understand the managerial authority that is in place to cover NHSGGC email communications.

This policy has been developed following an assessment of the primary risks and vulnerabilities associated with the use of email within the NHS Scotland environment. The policy and guidance should, when considered in the context of individuals' roles and responsibilities, provide sufficient guidance to ensure appropriate use is made of email. Staff should however seek further guidance should they be unclear about any aspect of the policy.

The document describes the appropriate use of email and is intended to enable staff to feel confident in conducting business through the medium of email.

3. Scope and Coverage

This policy applies to all NHSGGC staff, and independent contractors who use NHS Greater Glasgow & Clyde provided email systems. For the purpose of this policy, this includes those with honorary contracts, partnership and agency staff, volunteers and students.

Within the scope and coverage of the policy, staff must fully comply with the terms and conditions of this document. Failure to comply with the policy set out may be interpreted as a threat to the security of NHSGGC's information assets.

In the event of non compliance, staff will be the subject of investigation and potential disciplinary action. In such circumstances, those with a concern about non compliance will:

- inform the individuals line manager of the situation;
- advise the IT Security Manager who (in consultation with the line manager) will consider recommending termination of the individuals' access to NHSGGC's networking infrastructure and computer network.

4. General Rules

- Protect access to your mailbox:
  - staff must take precautions to ensure that other users cannot access their emails;
  - Logon credentials including user identifier and password should not be shared except in circumstances where an investigation requires to be carried out;

- If you're going to be away from your computer, it should be locked'. This is done by using the  +L keys;

If you're going to be absent from work, you can give a suitably accountable colleague delegated access to your email. This can be done by following the instructions in the Guidance Document "How to Set Up Delegate Email Access"

- Do not use personal email systems or include personal email addresses for any NHS business;

- Only use your name@ggc.scot.nhs.uk or name@nhs.net email address for NHS business.

Access to departmental generic (also known as Clinical) mailbox may only be given by the "Delegate" function, under no circumstances may the email be accessed by sharing the mailbox password. Please read 'Generic Email Accounts' and 'How to set up Delegate Email Access'.

5. Specific Guidance on the Use of Email:

Categories of data

Personal Identifiable Data – defined as data that contains person identifiable information or **otherwise sensitive data**, defined as data that if viewed inappropriately could cause distress, identify individuals, undermine confidence in the service, or release commercially sensitive information

For such data, the following email transmissions are permissible:

Source	Approved Recipient	Actions
@ggc.scot.nhs.uk	@nhs.net @any.scot.nhs.uk @glasgow.gov.uk @glasgow.gsx.gov.uk @glasgowlife.org @glasgowlife.org.uk @cordia.co.uk @west-dunbarton.gov.uk @eastdunbarton.gov.uk @inverclyde.gov.uk @eastrenfrewshire.gov.uk @eastrenfrewshire.gsx.gov.uk @renfrewshire.gov.uk @renfrewshire.gcsx.gov.uk	Add 'official - sensitive personal data' to the subject line.
@nhs.net	@nhs.net @any.scot.nhs.uk @x.gsi.gov.uk @gsi.gov.uk @gsx.gov.uk @pnn.police.uk @cjsm.net @scn.gov.uk	Add 'official - sensitive personal data' to the subject line

	@gcsx.gov.uk @mod.uk @gse.gov.uk	
Where the patient has emailed in including PID or sensitive information, consent to reply to them by email is assumed.	To the email address from which the original email was received and only using the 'reply' function	Add 'official - sensitive data' to the subject line. Such emails should not be forwarded to external recipients other than the person who originated the correspondence.
Where staff wish to initiate communication by email with patients and this includes identifiable or sensitive data, explicit consent must be obtained from the patient prior to communication.	To the email address advised by the patient in the correspondence that consents to the use of email	Verify the 'approved' address prior to sending. Do not address multiple recipients with a single email message Add 'official - sensitive data' to the subject line.
It is acceptable to email **named individuals** at 3rd parties such as delivery companies or charities supporting health with identifiable data, but the sensitivity of the information must be low.	To an organisational email address such as name@company.co.uk	Verify the address prior to sending.

For data that does not have the potential to cause distress, breach confidence, cause financial or other harm, refer to an identifiable person's physical or mental state, **there are no specific handling instructions**. Such emails can be sent to anyone with a legitimate right to view that information.

6. Further Guidance

Permissible activities:

- Email is provided to staff primarily to support NHSGGC business activities however personal use is permitted as long as it is reasonable and in compliance with this policy;
- NHSGGC emails sent in a business or clinical capacity must be for legitimate business purposes;
- Staff should not subscribe to internet services that send regular email messages other than in circumstances where such messages are in direct support of their professional role (e.g. drug alerts, fraud alerts, public health alerts);
- NHSGGC email may not be used for illegal activities such as the onward transmission of copyrighted materials or the inclusion of content that could be perceived as libelous.

7. Managerial Authority and Monitoring Processes

- The Board reserves the rights to examine all emails;
- Emails can be used as evidence in a court of law;
- Email can be released under the Freedom of Information Act (this excludes clinical data unless it is specifically pertinent to an investigation);
- Emails can be released under the Data Protection Act;
- Emails will be filtered by software to detect viruses and SPAM. Emails may be quarantined if the screening software considers them to be within defined risk categories;
- NHSGGC email should not be used on the assumption that emails are private;
- Email may be monitored by NHSGGC technical staff at the request of managers;
- Email usage may be monitored to meet policy, legal and statutory obligations;
- The emailing software will add a disclaimer to all outgoing emails;
- Administrators can remove emails if they consider this action necessary.
- The Board reserves the rights to block email addresses that have been used to send nuisance or harassing emails

8. Associated Legislation / Policies / Standards

The use of email and email content is governed within the context of prevailing law and NHS Scotland guidance. The Principal Acts of Parliament and Scottish Government circulars relevant to this policy are:

- CEL (2008)45 NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- ISO/IEC 27001:2005 Information technology – Security techniques. Further details can be obtained from your local Information Security Officer
- MEL 2000 (17) Data Protection Act 1998
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012
- SGHD HDL (2006) 41
- SGHD MEL (1993) 59
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

9.0 Policy Review

This policy will be reviewed on a bi-annual basis, unless the introduction of any new or amended relevant legislation warrants an earlier review.

10.0 Communication and Implementation

This Policy will be communicated through the Information Governance Framework.

11.0 Further Advice

For further advice on this Policy please contact the Information Security Manager
Tel: 0141 347 8137 Email: Mike.dench@ggc.scot.nhs.uk