

Email Usage Policy

(February 2021)

Lead Manager	IT Compliance Manager
Responsible Director	Director of eHealth
Approved By	Information Governance Steering Group
Endorsing Body	Area Partnership Forum
Date Approved	17 March 2021
Review Date	Approval from extraordinary IGSG meeting held on the 17th March 2021 to extend the review period of this policy until such time as GGC.Scot domain has been migrated to NHS.Scot domain and national policies can be adopted.
Version No.	7.2

CONSULTATION AND DISTRIBUTION RECORD			
Contributing Author / Authors		• Brian Miller IT Security and Compliance Manager	
Consultation Process / Stakeholders :		Information Governance Steering Group members (which includes staff partnership representatives).	
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
20/02/17	I Brown	Reference in S5 re advice for patients wishing clinical information emailed to them.	5.3
20/02/17	I Brown	Update contact details	5.3
29/01/18	S Harris	Updated with changes to the secure email boundary	5.4
11/06/18	S Harris	Updated in line with business and technical changes	6.0
21/06/18	S Harris	Updated with comments from IT Security Manager and Mail and Directory Support Team Manager	6.1
25/06/18	S Harris	Updated for address confirmation	6.2
26/07/18	S Harris	Change to Secure Email Boundary, Adoption of Encryption	6.3
29/10/18	S Harris	Updates from IG, Addition of Account Deletion	6.4
12/11/18	S Harris	Updated for secure route to NHS Mail	6.5
21/11/18	S Harris	Updated for comments from APF 21 Nov, account deletion extended to 13 months, creation of Account Disablement and Investigation Process	6.6
03/12/2018	A Banerjee	Added phishing presentation.	6.7
14/12/2018	A Banerjee	Secure Glasgow Gov domains added to secure email bounary	6.8
20/12/2018	S Harris	Inverclyde, West Dunbartonshire and Renfrewshire domains added to secure email bounary	6.9
28/12/2018	S Harris	On premise email service for Lanarkshire, Ayrshire and Arran, Golden Jubilee added to secure email boundary	6.10
11/01/2018	S Harris	East Dunbartonshire, addition to Information Sensitivity and Categorisation	6.10
25/01/2019	A Banerjee	West Dunbarton added to secure email boundary	6.11
12/03/2019	S Harris	South Lanarkshire and Fire Scotland added to secure email bounary	6.12
14/03/2019	S Harris	Scottish Childrens Reporter Administration and NHS Lothian added to secure email bounary	6.13
20/05/2019	S Harris	Data Protection Act (2018) update	6.14
04/07/2019	S Harris	East Renfrewshire added to secure email boundary	6.15
15/10/2019	S Harris	Police Scotland addd to secure email boundary	6.16
2/02/21	S Harris	References to NHS Scotland Office 365 Email Policies and Assurance	7.0

26.04.2021	I Brown	Update to references at request of APF	7.1
16/04/2024	B Miller	Updated revision date	7.2

Contents

1	INTRODUCTION	5
2	POLICY OBJECTIVES.....	5
3	SCOPE	5
4	MAILBOX PROTECTION AND MANAGEMENT	5
4.1	Mailbox Protection.....	5
4.2	Corporate v Personal Use	5
4.3	Address Book Details.....	6
4.4	Account Deletion.....	6
4.5	Planned Absence	6
4.6	Mail Box Access	6
4.7	Email Retention.....	6
4.8	Email Forwarding to a personal address	6
4.9	SPAM and Phishing	7
4.10	Mail Filter	7
4.11	Use of the Generic Mailbox.....	7
4.12	Calendar Management	7
5	Address Confirmation.....	8
5.1	Confirm Recipient Email Address	8
5.2	Distribution List	8
6	INFORMATION SENSITIVITY AND CATEGORISATION.....	8
6.1	GREEN.....	8
6.2	AMBER.....	8
6.3	RED.....	8
7	THE SECURE EMAIL BOUNDARY	9
7.1	NHS.....	9
7.2	Glasgow Gov.....	9
7.3	Inverclyde Gov.....	10
7.4	West Dunbarton.....	10
7.5	Renfrewshire	10
7.6	East Dunbartonshire	10
7.7	South Lanarkshire	10
7.8	Fire Scotland	10
7.9	Scottish Chilrens Reporter Administration	10

7.10	East Renfrewshire.....	10
7.11	Police Scotland	10
8	EMAIL ENCRYPTION.....	10
9	COMPLIANCE AND MONITORING	11
10	ASSOCIATED LEGISLATION/POLICIES/STANDARDS.....	11
11	POLICY REVIEW.....	12
12	FURTHER ADVICE OR QUERIES	12
13	EMAIL USE TIPS - DO AND DO NOT	13
14	APPENDIX A Notification of Planned Absence.....	14
15	Information Security and Governance for Office 365 Email – NHS.Scot	15
15.1	Email Policies	15
15.2	Secure Email Assurance Documents	15

1 INTRODUCTION

This policy has been developed following an assessment of the primary risks and vulnerabilities associated with the use of email within NHSGGC. It is intended to ensure safe, effective and efficient email use and forms part of the overall Information Security policy for NHSGGC. The policy and guidance should, when considered in the context of individual 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 this policy.

GGC users are migrating to NHS Scotland's new email service NHS.Scot which uses Microsoft Office 365. A set of national policies govern the use of NHS.Scot. GGC staff are expected to comply with the national policies. As these policies mature then the GGC Email Usage Policy will be further changed.

2 POLICY OBJECTIVES

The **Objectives** of this policy are to provide guidance on

1. Mailbox protection and management
2. Information Sensitivity and Categorisation
3. The Secure Email boundary
4. Encryption and when to use it
5. Compliance

3 SCOPE

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.

4 MAILBOX PROTECTION AND MANAGEMENT

4.1 Mailbox Protection

Logon credentials including user identifier and password should not be shared. If you need to share access to your mailbox use delegated permissions which provides an audit trail. This can be permanent or enabled for a specific event such as planned leave (Follow the guidance in "[How to Set Up Delegate Email Access](#)". To prevent unauthorized use of your user session if you are going to be away from your computer, it should be locked'. This is done by using the  +L keys;

4.2 Corporate v Personal Use

Only use your corporate NHS email address name@ggc.scot.nhs.uk or name@nhs.net for health and health and social care business.

Do not register your corporate address for personal use, particularly for on line transactions like shopping or social media.

Do not use personal email systems or include personal email addresses for any health and social care business.

NHSGGC emails sent in a business or clinical capacity must be for legitimate business purposes.

Do not subscribe to internet services that send regular email messages other than in circumstances where such messages are in direct support of your professional role (e.g. drug alerts, fraud alerts, public health alerts, professional body).

4.3 Address Book Details

Critical to the safe delivery of email is that the recipient is correctly identified. Make sure that your details as displayed in the email Global Address List (GAL) are current and complete including enough demography to identify you. This must include line manager who will be the authoriser of access to the account in times of leave or sickness. <http://ggcdirectory.ggc.scot.nhs.uk/ActiveDirectory/search.aspx>

4.4 Account Deletion

Where an individual email account has not been used for thirteen months then the address and inbox will be deleted. (The network account and file shares will also be deleted at this time.)

4.5 Planned Absence

When you are planning not to use your account for twelve months, usually as a result of leave or secondment, notify the service desk providing the details as Appendix A) This will then be marked with a planned return date and “not for deletion”.

4.6 Mail Box Access

In time of leave or sickness the user’s manager, (as defined in the GAL or other referenceable source) or clinical director can authorise mail box access through the IT Service Desk. This will be with delegated rights.

4.7 Email Retention

Email is a communication tool to support the secure exchange of information. It is not designed as a document management system. Relevant data contained within emails should be incorporated within the patient record or business system.

Documents, emails or messages that are required for retention/compliance purposes should be stored in accordance with Information Governance policies.

4.8 Email Forwarding to a personal address

Emails within GGC, NHS .scot or GGC corporate use of Office 365 are secure for corporate purposes. Email must not be forwarded to personal accounts which have unknown security standards.

4.9 SPAM and Phishing

SPAM is electronic junk mail. Some SPAM will contain malware.

Phishing is an attempt to get you to provide sensitive information based on false request, e.g. offer of free pizza, complete your HMRC tax return, change your password.

NHS email filters will block the majority of SPAM and Phishing attacks.

However, if you are unsure of the source of an email or attachment you should leave it unopened and inform Spam@ggc.scot.nhs.uk.

Users should not open emails or click on links or attachments in emails from untrusted sources. More details around spams and phishing can be found in the Be Cyber Safe page in Staffnet.

http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/BCS/BeCyber%20Documents/Phishing_Procurement%20-V5.0.pdf

4.10 Mail Filter

GGC uses mail filtering to reduce SPAM, phishing and malware. These email filters may block some legitimate emails and/or block URLs inside the body of an email.

The filter can produce two messages.

1. Email subject line is pretexted with [BlockedURL] tag and replaces the text in the URL inside the email body with additional texts like BLOCKEDsitename[.]detail[.]comBLOCKED. This means that the email contains any URL with neutral reputation and the email filter does not have much information about the URL. You can copy the URL with the additional texts, paste them into an Internet Browser and removed the BLOCKED and [and] to get to: sitename.detail.com. This should be only done for site you trust.
2. The email subject line is pretexted with [MaliciousURL] tag. When part of an email the URL is removed completely for safety.
3. To request unblocking contact Spam@ggc.scot.nhs.uk.

Emails originating from outside NHS GGC will have an [ExternaltoGGC] tag in the subject line. You should take additional caution before clicking on any links or download attachments provided in the email.

4.11 Use of the Generic Mailbox

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](#)'.

4.12 Calendar Management

You must not hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person.

5 Address Confirmation

The vast majority of email-related privacy breaches have been as a result of sending information to the wrong person including in part due to an out of date distribution list

5.1 Confirm Recipient Email Address

Particularly for sensitive information users must confirm the recipient email address before sending. This includes sending and responding to patient emails. This can be done by checking a directory, sending a test email or speaking to the recipient.

5.2 Distribution List

If a distribution list has to be used confirm that it only contains the intended recipients, that their role has not changed and it is still appropriate for them to receive the mail.

6 INFORMATION SENSITIVITY AND CATEGORISATION

Higher sensitivity is not determined simply by the type of document (e.g. X assessment form or Y appointment letter). Instead, a judgement needs to be made as to the impact that would be caused if the information was lost or misused.

Personal or identifiable information should not be added to the subject line when emailing. Users should instead add “Sensitive Confidential Information” as this will reduce the risk of a data breach when email notifications pop up.

6.1 GREEN

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person’s name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person’s physical or mental state.

6.2 AMBER

The largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person’s safety (e.g. loss of an address but no evidence to suggest direct harm would result).
- Any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

6.3 RED

Information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases)
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

7 THE SECURE EMAIL BOUNDARY

With ongoing technical and organisational changes outside of NHSGGC the historical secure email boundary of partner organisations and networks no longer applies. **The revised secure email boundary for GGC.Scot.nhs.uk is domains ending in .Scot.NHS.Uk, where there is a secure route as defined in this policy.** When sending RED or AMBER data outside the secure email boundary, an additional measure **EMAIL ENCRYPTION** must be used.

There are secure email routes in place for the following email domains and are considered secure for exchanging Sensitive Information

7.1 NHS

- NHS Mail
- Scot.NHS.UK

7.2 Glasgow Gov

- All *glasgow.gov.uk
- Cbglasgow.co.uk
- Citybuilding.co.uk
- Citymarketsglasgow.co.uk
- Cityparkingglasgow.co.uk
- Citypropertyglasgow.co.uk
- Clydegateway.com
- Cordia.co.uk
- Cucity.co.uk
- Encorehospitalityservices.co.uk
- GRA.co.uk
- Rsbi.co.uk

7.3 Inverclyde Gov

- Inverclyde.gov.uk

7.4 West Dunbarton

- West-dunbarton.gov.uk
- dab-vjb.gov.uk
- Clydebankproperty.com
- wdc.gcsx.gov.uk

7.5 Renfrewshire

- Renfrewshire.gov.uk

7.6 East Dunbartonshire

- Eastdunbarton.gov.uk

7.7 South Lanarkshire

- Southlanarkshire.gov.uk

7.8 Fire Scotland

- Firescotland.gov.Uk

7.9 Scottish Childrens Reporter Administration

- SCRA.GSI.GOV.UK

7.10 East Renfrewshire

- Eastrenfrewshire.gov.uk

7.11 Police Scotland

- scotland.pnn.police.uk

8 EMAIL ENCRYPTION

Red or amber data being sent outside of the mail system must be encrypted which provides a secure delivery method when correctly addressed. (Section 5 above addresses checks that should be made to ensure correctly addressed)

Encryption can be applied by adding [secure] or [SECURE] to the subject line.

For GGC Mail encryption guidance please find the following documents in the Guidance document page of Be Cyber Safe page:

<http://www.staffnet.ggc.scot.nhs.uk/Corporate%20Services/eHealth/BCS/IT%20Guidances/Forms/AllItems.aspx>

- **GGC Email Encryption Sender Guide**
- **GGC Email Encryption Recipient Guide**
- Sending Secure Email Encryption Guide
- Accessing Encrypted Emails Guide for non-O365 users v1.0

9 COMPLIANCE AND MONITORING

In the event of non-compliance NHSGGC is entitled to access the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly controlled and follow a defined **Account Disablement and Investigation Process**.

Emails can be used as evidence in a court of law; can be released under Data Protection Act and Freedom of Information Act (this excludes clinical data unless it is specifically pertinent to an investigation);

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.

10 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 (2012)25 NHS Scotland Mobile Data Protection Standard

http://www.sehd.scot.nhs.uk/mels/CEL2012_25.pdf

Civil Contingencies Act 2004

Computer Misuse Act 1990

Copyright, Design and Patents Act 1988

Data Protection Act 2018

Regulation of Investigatory Powers (Scotland) Act 2000

Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

GGC Email Encryption Sender Guide

GGC Email Encryption Recipient Guide

GGC Standard/policy/guidance

Acceptable Use Policy

IS Policy 1 Governance

IS Policy 2 Risk Management

IS Policy 3 Information Security

IS Policy 4 ISMS

IS Policy 5 Organisation

IS Policy 6 Human Resources

IS Policy 7 Asset Management

IS Policy 8 Access Control

IS Policy 9 Cryptographic
IS Policy 10 Physical and Environmental
IS Policy 11 Operations Security
IS Policy 12 Communications
IS Policy 13 Data Transfer
IS Policy 14 System Acquisition
IS Policy 15 Supplier Relationships
IS Policy 16 Incident Management
IS Policy 17 Business Continuity
IS Policy 18 Compliance
Email Usage Policy
Third Party Access Policy
Internet Acceptable Use Policy
Network Account Deletions Policy
Mobile Devices and Teleworking

The link to these policies can be found [here](#)

11 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.

12 FURTHER ADVICE OR QUERIES

For further advice or queries on this Policy please contact the IT Compliance Manager

Tel: 0141 278 4728

Email: Stephen.harris@ggc.scot.nhs.uk

13 EMAIL USE TIPS - DO AND DO NOT

DO	DO NOT
Use delegated permissions if you need to provide someone else with access to your mailbox/calendar	Share your user identifier and password
Lock your computer to prevent access to your mailbox if you are leaving the computer unattended	Use your corporate address for personal use eg on line shopping social media
Only use your corporate address for health and social care business	Use personal email system for any NHS business
Ensure that your details in the email directory are correct	Subscribe to internet services that send regular email messages other than in circumstances where such messages are in direct support of your professional role
Confirm the recipient address if you are planning to send Amber or Red information	Use email as a document management solution
Use delegate access to provide access to the Generic email accounts	Forward nhs email to personal account
Check if the recipient is within the email system before sending RED or AMBER information.	Open an email or attachment if you are unsure of the source
Encrypt mail if sending RED or AMBER information beyond the Email system ie GGC or NHS Mail.	Hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person.
If you are planning on not using your email account for more than twelve months notify the IT Service Desk.	

14 APPENDIX A Notification of Planned Absence

User Name	
Department	
Email Address	
Dates of Planned Absence	

15 Information Security and Governance for Office 365 Email – NHS.Scot

National Email Policies should be followed. These and supporting Assurance Documents are available at

<https://scottish.sharepoint.com/sites/GGC-Office365KnowledgeCentre>

15.1 Email Policies

O365 Email Policy
O365 Secure Email Policy
O365 Email Acceptable Use Policy
Sending Secure Email Encryption Guide
Accessing Encrypted Emails Guide for non-O365 users v1.0
O365 Email Incident Management Policy
O365 email Data Retention and Information Management Policy
Access to Data Procedure
Access to Data Request Form
GDPR Transparency Information for O365 Email

15.2 Secure Email Assurance Documents

Assurance statement confirming technical security
Clinical Assurance
Secure Email Controls
Secure Email Connectors
Microsoft Office 365 DCB1596 Conformance Statement