THE STATE HOSPITALS BOARD FOR SCOTLAND

EMAIL POLICY

Policy Reference Number	IG23	Issue: 1
Lead Author	Information Security Officer	
Contributing Authors	O365 Project Team	
	eHealth Sub Group	
Advisory Group	eHealth Sub Group	
Approval Group	Policy Approval Group	
Implementation Date	31 August 2021	
Next Review Date	31 August 2024	
Accountable Executive Director	Director of Finance and eHealth	

The date for review detailed on the front of all State Hospital policies/ procedures/ guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/ procedure/ guidance at any time due to organisational/legal changes.

Staff are advised to always check that they are using the correct version of any policy/ procedure/ guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies/ procedures/ guidance can be found on the intranet: http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

Contents **Page**

1. Introduction / Purpose

The purpose of this policy is to outline the acceptable use and behaviour of all State Hospital Boards for Scotland (TSH) staff and their use of business email that will be provided to support them in undertaking their role and fulfilling their duties and responsibilities.

Users should be aware that all emails are now legally admissible documents and certain emails may be subject to records management.

This policy will provide clear guidance to users of the email service so that they may comply with the various related legislation and will inform users of what information can be shared with NHS colleagues, business partners, volunteers and any patient representatives via email.

2. Scope

Use of the email service shall be intended for business use only unless determined, in advance, otherwise. All emails shall be subject to monitoring and auditing. Users should have no expectation of privacy while using the email service.

This policy covers all internal and external emails sent and received by users of the service in TSH and applies to all staff, volunteers and contractors or persons that have been provided with a business email account. The term ‘email users’ will be used to cover all those listed.

This policy should be read in conjunction with the national policy, listed within the References section.

Where there is a conflict of information, this policy overrides the national policy listed.

3. Roles & Responsibilities

3.1 Responsibilities of Users

All email users must abide by this policy.

Email users will treat all emails in accordance of all records management policies/procedures/processes and manage all emails accordingly. All emails should be made available, where requested, and if necessary saved to shared drive/folder/mailbox to be retrieved if necessary, at a future date. Email users’ managers and directors will define those emails that are to be saved in this way.

Email users must, when requested, undertake the appropriate searches and submit all information requested to the staff member processing the information request e.g. subject access request (SAR), freedom of information request (FOI) etc, within the defined timescales.

3.2 Responsibilities of TSH

TSH will provide access to the email service.

3.3 Responsibilities of NHS Scotland (NHSS)

Details on the responsibility can be found within the document located here.

4. Policy

4.1 Authorisation of Access

Access to the email service will only be granted on receipt of the appropriate access request form.

TSH hold the right to withdraw access to the email service with no prior notice or notification, this will be in accordance with HR policies.

Email users will use their own unique username and passphrase to access the email service and are advised that use of another email users credentials will breach TSH IT security policies.

Sharing passphrases or allowing another email user to access the email service also constitutes a breach of IT security policy.

4.2 Specific Obligations

All email users must ensure they familiarise themselves and comply with related policies, guidance and legislation as listed within the References section to ensure that individuals rights to confidentiality are respected.

Users must not knowingly:

- Send any email/materials/files of a defamatory, illegal, hateful, sexually explicit, obscene, pornographic or otherwise objectionable nature to cause distress or offence.
- Send communications that knowingly cause distress or offence to another email user, or that is intended to annoy, harass or intimidate another person.
- Attempt to introduce viruses. The transmission or propagation of any malicious code is expressly forbidden.
- Waste resources by sending or inviting large amounts of unnecessary email including chain mail, jokes or any other frivolous email.
- Use the email system for excessive personal use – see Section 4.3.
- Use the email system for personal gain, for example, running a business from work or selling personal items.
- Register their NHS email address for non-work related communication/websites.
- Send work related email from personal, non-work related email accounts. Work related email must only be sent from official NHS email accounts.

Email users should be aware that all emails generated within the email service are viewed as property of NHSS and may be legitimately requested under the Freedom of Information (Scotland) Act 2002 and Data Protection Law.

All emails entering the organisation or originating from the organisation are automatically filtered to ensure that the email system is being used appropriately. Emails may be blocked if they are viewed as a risk to information systems. No local blocking of emails will occur; this will be under the control of NHSS.

All emails generated within NHSS are viewed as the property of NHS Scotland and may constitute a corporate record. Certain emails can also be legally binding documents. Email users have the responsibility to read, and where appropriate, action all emails that they receive.

If emails are not monitored whilst on leave, email users must ensure that on their return, all emails received during the absence are read and actioned. Staff must not set out of office messages that advise emails received whilst on leave will not be read and will be deleted. Doing so would constitute a breach of this policy. It is best practice to put an appropriate “out of office” message onto your email account which advises the period of absence and a suitable alternative contact.

Email users must not auto-forward emails to non NHSS email accounts.

4.3 Personal Use

Email users are permitted to use the email service for non-work related matters where it does not intrude with the users’ work, colleagues, patients or the environment; does not appear to have

been sent on behalf of the organisation; does not bring TSH or NHSS into disrepute; and does not contravene this policy.

Non work related activity must be limited to non-working time. Personal use of the email system during work time is not appropriate, and any such misuse may be considered a disciplinary matter.

Email users must be aware that personal emails generated within the NHS Scotland email service are viewed as property of NHS Scotland and may constitute a corporate record and may be legitimately requested under the Freedom of Information (Scotland) Act 2002 and Data Protection Law.

Users must be aware that personal use of the email system could result in a tax liability for the individual member of staff.

Users must not store personal files (not business related, such as photographs, music or documents) within the email system.

4.4 Emails Containing Clinical Content

Clinical email is defined as email with clinical content, often including patient identifiable information, sent between clinical sites.

Always consider anonymization of personal identifiable information where possible. Information is said to be anonymised when identifiers; such as name, address, full postcode and any other detail that might identify an individual are removed.

Use the 10-digit CHI number, Surname and Forename to ensure positive identification of the patient. In the absence of CHI, staff should use Surname, Forename and D.O.B.

Review your processes regularly to justify the need to store or transfer patient identifiable information in any format.

Emails relating to patients should be stored in the EPR in line with the Records Management Guidance.

4.5 Secure Email

When sending personal identifiable or confidential information via email, staff must observe the following:

- Always take precautions to ensure that the email message is not transmitted to the wrong person. If this happens it may result in a breach of confidentiality and this may lead to the individual sending the email being subject to disciplinary proceedings.
- When sending clinical email, either select “Reply to Sender” or select the correct email address from the global address list.
- If using NHSS email, the recipient’s details can be checked by clicking on the email address within the browse section of the Scottish Global Address List (GAL) directory. This will provide more information regarding the recipient e.g. full name, organisation, job title, address and telephone number.
- Always be satisfied that you have the correct email address, if you are unsure; verify the correct email address with your intended recipient, either by phone or by sending a test email.
- Email distribution/circulation lists should be used with caution. It is essential that distribution/circulation lists are updated when staff leave or move post. Prior to sending to a distribution/circulation list, staff must ensure that all individuals on the list have a legitimate need to receive the information contained in the email.

If there is a need to send personal identifiable or confidential information via email to a recipient, that is not included in the safe domain list, users should use enter [secure] into the subject bar. This will ensure the email is sent securely and should only be accessible by those it is sent to.

4.6 Malicious Email

Although email is a convenient and powerful communications tool it also provides scammers and other malicious individuals an easy means for luring potential victims.

NHS Scotland's email service have controls in place to block malicious emails, however there are occasions when certain emails are difficult to block. To assist the controls already in place, you should practice caution when opening any email and never click a link or open an attachment within any email you are not expecting, especially if you do not recognise the sender. Please also be aware this could easily appear to come from someone you do know.

To help combat malicious emails, please follow these recommendations:

If you do not know the sender of an unsolicited email message, DO NOT OPEN IT. While most spam emails are usually just annoying text, some emails could contain a malicious payload and/or other exploit that could steal information.

Never respond to any spam messages, open attachments within it, or click on any links in the message. This also applies for emails that will ask you to reply or email an address using a different email address (usually asking for you to use your non-corporate address)

If you receive a suspect email, please notify the IT Helpdesk in the first instance. Do not forward any emails you suspect of being malicious to anyone else, unless directed by the IT Helpdesk to do so.

5. Equality and Diversity

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and / or discrimination. The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person-Centred Improvement Lead on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments are in place to enable staff to understand and comply with policies and procedures. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

6. Stakeholder Engagement

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
TSH Board	Y
Carers	N
Volunteers	N

7. Communication, Implementation, Monitoring and Review of Policy

This policy will be communicated to all stakeholders within TSH via the intranet and through the staff bulletin.

The eHealth Sub Group will be responsible for the implementation and monitoring of this policy.

This policy will be reviewed every three years, and when appropriate to take into account changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner's Office.

8. References

Email policy specific to NHS Scotland Office 365 Email Service.