**Email Security Policy**

**Email Policy Scope:**

All individuals who are authorised to use ***<Company Name>*** e-mail facilities

are required to comply with this policy.

**Individual Responsibilities:**

* All employees, contractors, sub-contractors and temporary staff are responsible for their personal use of email facilities provided to or used by [the organisation].
* The [Email service Manager] is responsible for providing and maintaining a standard e-mail disclaimer and for setting and monitoring acceptable usage and mailbox rules.
* The [Email service manager] is responsible for identifying appropriate training materials to ensure that users of the e-mail service are aware of the provided email functionality and their responsibilities for good working practices.
* The [Information Security Manager] shall respond to and manage reported information security incidents, and shall ensure adequate corporate anti-virus protection and cryptographic controls exist in line with published NHS Good Practice Guidelines

**Expected and Acceptable Uses:**

***<Company Name>*** e-mail service may only be used for legitimate authorised purposes. Email may not be used for communicating illegal material, defamatory content, personal harassment, non-business purchases, or for publishing unauthorized views or opinions that may be damaging to ***<Company Name>***. Use of the Email service may be monitored for compliance with this policy.

All emails shall have an inserted footer that contains a legal disclaimer. Users of the service may not alter or delete this.

***<Company Name>*** e-mail service may only be used for the communication of

NHS information in accordance with NHS Information Governance Codes of

Practice.

The communication of NHS Confidential or NHS Restricted information by

email must be appropriately protected, using approved cryptographic controls (currently AES 256 bit strength or equivalent). When using NHSmail this technical security protection is automatic.

Email users must avoid opening incoming e-mail attachments that have not been checked for

possible viruses or other malware in case they cause damage or disruption to the service.

**Good Practice:**

Spam, Viruses, Chain mail and Phishing messages:

Email users must remain vigilant to the potential threats posed by email and are required to report any suspicious messages they may receive to the [Information Security Manager] immediately for possible isolation and investigation. It is prohibited to send any such messages onto other email users.

Email users are expected to apply good working practices to avoid where possible:

* the use of group e-mailing functions;
* copying of email to unnecessary recipients;
* the use of the “reply to all” function;
* the use of the blind copying feature.

Email users are expected to comply with published Incident Reporting Procedures for the Email service concerned and as may be periodically revised.

Email users are required to maintain their email boxes in good working order ie to delete e-mail messages when no longer required. Off-line email archive facilities should only be used in accordance with ***<Company Name>*** published guidelines and must take account of records management obligations including Data Protection and Freedom of Information.

Email users may not use the email service for personal transactions that may be confused or perceived as official business.

Emails may only be forwarded in the user’s absence to another email service where a) that email service has been approved in advance for this purpose by [the email service manager]; and b) the other email service provides an equivalent level of information security protection.

Breaches of this email policy may potentially result in local disciplinary action and or criminal prosecurition for the service user concerned.

This policy document is available to [all/specified] members of staff on the [corporate intranet] and is published [ ].

This email policy was approved by [the name of local policy approval authority] on [date].

Signature: Date:

Designation:

[Policy issue version no and publication date]

**Source:** <http://www.itdonut.co.uk/it/staff-and-it-training/your-it-policies/sample-email-use-policy>