Email Retention and Usage Policy

1. Introduction

Email messages sent in the course of University business can be viewed as corporate records, and therefore have to be managed as records. We must make sure we retain any emails that are recorded evidence of business activity for an appropriate period of time.

There are also legal reasons why we must manage our emails correctly. We have to respond to requests for information received under the Freedom of Information Act 2000 ("FOIA") and the Data Protection Act 1998 ("DPA"). We must therefore be able to locate all relevant records and information that have been requested, or be able to confirm that they have been deleted appropriately. The DPA also states that we must not retain personal data for any longer than is necessary, so we cannot permanently hold onto all emails sent and received if they contain information about individuals.

This policy and associated guidance is intended to help employees determine whether, and for how long, to retain information that is sent or received by email. It also sets out rules on when, and for what purpose, you should use your University email address.

2. Scope

This policy applies to all emails sent and received by University staff in the course of University business.

Related policies and guidance documents are as follows:

- Guidance on Email Etiquette and Managing Emails as Records
- Staff Email Policy
- Records Management Policy and Records Retention Schedule
- Freedom of Information Policy
- Data Protection Policy
- Information Security Policy

3. The Policy

Usage of University Email

Reasonable personal use of your University email address is allowed as long as it does not impact on your work. These messages should be labelled 'Personal' in the subject line.

You should not use your University email address to sign up for personal accounts on websites such as Amazon, eBay, Facebook, Twitter or PayPal.

Don't send University work to your home email account. Remote access to University IT services, including email, is provided to allow you to work away from the office.

Be aware that anything that you write in an email relating to University business may be subject to disclosure under FOIA or DPA. Email messages can also be used as evidence in legal proceedings.

Retention of Emails

University employees are responsible for managing their email records in the same way that they are responsible for managing other business records. Each member of staff has a set mailbox quota for storage of email. If you exceed the maximum quota for your mailbox you will be unable to send or receive emails.

How long an email should be retained is governed by the information contained within it, not the medium on which it is stored. The University Records Retention Schedule sets out classes of information held along with the recommended period for which they should be kept. There is guidance on Managing Emails as Records which gives more advice on applying these principles.

Do not use .pst files (Outlook 'personal folders') to archive emails. If they are stored on your hard drive then they may be lost if you leave the University or overlooked if they are requested under FOIA. If they are stored on the network the .pst files are liable to become corrupt, and you may lose your information. For advice on email storage, contact the IT Service Desk (it.servicedesk@ncl.ac.uk).

You should set your Deleted Items folder to empty itself on closure of the Outlook application. Deleted Items should not be used as a file store. Emails deleted from your Deleted Items folder will be stored centrally for 90 days after deletion in case they need to be recovered. After this period they will be permanently deleted.

Monitoring of emails

Newcastle University reserves the right to monitor emails sent and received relating to University business in accordance with the Regulation of Investigatory Powers Act 2000, the Data Protection Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

4. Monitoring and Review of this Policy

This policy will be reviewed periodically by the NUIT Information Security Team. Anyone found to be in breach of this policy may be subject to action through the University's disciplinary procedures.

Steve Williams, Director of University IT
November 2011
(Reviewed February 2015)