

NICS Email Management Policy

DOCUMENT INFORMATION

Title	NICS Email Management Policy	Version	2.0
Author	Information Management Council (IMC)	Date	May 2020

CHANGE HISTORY

Ver.	Ver. Date	Revised	Description	Reviewer	Status
0.1	Jan 2019	IMC	Initial draft		Draft
0.2	Feb 2019	IMC	For consultation with ITAssist		Draft
0.3	May 2019	IMC	For approval by IGB		Draft
1.0	May 2019	IGB	IGB requested changes		Draft
2.0	August 2020	IMC	Sent to IGB for approval		Draft
2.0	August 2020	IGB	Approved		Final

DISTRIBUTION

Name	Position	Contact Details
IGB	August 2020	For approval

Introduction

The NICS is committed to providing and complying with effective records management procedures which are integrated as key activities within the organisation. All Departments have a Records Management Policy and staff should ensure they are aware of the policy as the principles of records management apply equally to email.

The NICS uses the electronic mail client MS Outlook to assist in providing efficient and effective document communication. Outlook is an email and calendar management tool, not a records management system and best practice dictates that emails required for business purposes are saved to HPRM to be retained as the official record. A facility built-in to HPRM allows for the transfer of records to PRONI for permanent preservation at the end of their business use.

To ensure NICS compliance with Data Protection, Freedom of Information, Environmental Information and Records Management legislation, a number of measures are imposed to provide effective management of email, set out below.

1. Mailbox Account Setup & Deletion

- Staff will only retain one primary mailbox account and this will be associated with the Department to which they are attached.
- IT Assist must ensure that a Manager is assigned to the mail account on creation; this should be the Line Manager. This will ensure the mail account can be effectively managed when required by the Departmental Business Relationship Manager (BRM).
- Staff on permanent transfer or secondment will have their old Departmental mail account deleted, and a new one created for the Department they transfer into. It is therefore important to ensure any relevant emails are saved to HPRM prior to the transfer.
- In exceptional circumstances where a staff member may need to retain temporary access to their previous mail account, approval is required by the IAO and the Departmental Information Manager for their former Department.
- Line Managers must ensure that, prior to a member of staff leaving the NICS, their mailbox will have been appropriately reviewed and all necessary action taken to ensure emails required for business purposes have been saved to HPRM. The Line Manager must ensure written notification is forward to IT Assist to delete the leaver's mailbox. This must be actioned within 30 days of the member of staff leaving.
- IT Assist must ensure staff leaving the NICS have their mailbox and account deleted within 30 days of receiving written notification by the line manager.

2. Three-Month Rule

- Since the introduction of RecordsNI as the official document and records management system for the NICS, any email that needs to be retained for Business purposes must be transferred to HPRM within 3 months of receipt.

- The 3-month rule, which is applied to **all** mailboxes, deletes the contents of all mail folders after 90 days. Calendar entries, Contacts and Tasks are not affected.
- Three months is a suitable period of time to determine whether the information contained in an email is required for business purposes.
- Emails must be saved to HPRM in the appropriate area of the Fileplan as soon as it is practicable to do so.
- Emails that are not required for business purposes should be managed accordingly and deleted from your mailbox manually.
- Line Managers must ensure the mailbox of staff on a long term absence (e.g. sickness or maternity leave) is appropriately managed by:
 - Submitting a request to IT Assist imposing an Out of Office on the mailbox, to inform senders of alternative contacts. The staff Line Manager must provide approval for this.
 - Ensuring the mailbox is monitored by another member of staff to deal with any queries that are received. If the Line Manager will be monitoring the mailbox, their Line Manager must give approval, before the request is submitted to IT Assist.
 - The 3-month rule will continue to apply to the mailbox without exception.

3. Mailbox Limits

- Mailbox limits exist for both technical and information management reasons.
- From a technical perspective, applying mailbox limits is best practice and safeguards the mail system against a number of different scenarios which would adversely impact the mail service, such as:
 - Mailbox storage quotas prevent mailboxes from growing beyond the service capacity
 - Quotas help with performance management tasks such as backup/restore, and mailbox migrations
 - Unrestricted growth of mailboxes is a major risk to the performance and health of the Exchange environment; in extreme cases, a single mailbox could consume all available space on a server, causing the mail system to crash. A number of computer viruses are designed to exploit this.
- For the majority of staff a standard limit is applied. A mailbox limit is good practice as it encourages the mailbox owner to proactively manage their information.
- In exceptional circumstances, for example where an inquiry or investigation has been initiated, a user may require a temporary increase to their mailbox. In such cases, the request for an increase must have IAO support and be submitted to their Departmental Information Manager outlining the Business

Case for the increase, for their approval. Requests must not be submitted to IT Assist until this line of approval has been granted.

4. Email System Backup

Departments are required to have robust retention schedules applied to reduce the risk that the information becomes irrelevant, excessive, inaccurate or out of date. This is essential if departments are to meet their legislative responsibilities under General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

- To ensure the mail system server is protected against any immediate loss or availability, it is backed up by IT Assist on a daily basis, purely for the purpose of recovery of the mail system.
- Mail system backups are not retained for the purpose of archiving data, but as contingency for the mail servers. IT Assist considers 3 months retention of the mail system backup as sufficient to satisfy this requirement.
- The mail system backup is not a structured and accessible archive system for the retrieval of emails deleted from staff mailboxes, either manually by staff or as part of the 3-month rule. N.B There is no facility to carry out an email document restore. Staff must therefore effectively manage their mailbox accordingly, ensuring emails required to be retained are saved into HPRM at the earliest point to avoid auto-deletion.
- A mail account restore must only be carried out in line with any disaster recovery process or if a user's mailbox is corrupted and not for any other purpose.

5. Generic Mailbox Accounts

- A completed Generic Mailbox request form must be submitted to the Departmental Business Relationship Manager (BRM) for approval.
- The 3-month rule must be applied to the mailbox.
- The IAO must ensure the mailbox is managed appropriately in reviewing staff access and permissions.

Policy Awareness

A copy of this policy statement must be provided to all new members of staff (as part of their Induction), and to interested third parties such as contract staff. Existing staff and third parties will be advised of the policy, which will be posted on the NICS Managing Information intranet site and on Departmental intranet sites, and will be available through the publication scheme, as will any subsequent revisions. All staff and third parties must be familiar with, and comply with, the policy at all times.

This policy will be reviewed every two years, at a maximum.

The “NICS Email Management Guidance” should also be read in conjunction with the Policy.

Implementation Date: September 2020

Next Review Date: September 2022