



Department of  
**Finance and  
Personnel**

[www.dfpni.gov.uk](http://www.dfpni.gov.uk)

**DEPARTMENT OF FINANCE AND PERSONNEL  
E-MAIL MANAGEMENT POLICY STATEMENT**

**Version 2  
Implemented: 1<sup>st</sup> September 2007  
Review: 1<sup>st</sup> September 2009  
Information Management Unit**

## Introduction

1. This document sets out the policy of the Department of Finance and Personnel (DFP) in relation to e-mail management on departmental or agency information and communications technology (ICT) resources. The policy applies to all DFP staff and others given permission to use departmental or agency resources to access e-mail, and is designed to supplement **NICS guidance CSC 02/03** on Internet and e-mail use.
2. This policy should be read in conjunction with the Records Management Policy Statement, which states how the Department will manage its records, including electronic records.
3. E-mail can deliver significant business benefits when used appropriately. As a method of communication it is quick, inexpensive and convenient. However, careless or negligent use has the potential to result in an inefficient use of departmental resources and in extreme cases may lead to complaints or legal proceedings against DFP or individual members of staff.
4. A 3 month rule has been imposed on all e-mail accounts. E-mails that have not been saved into TRIM and remain within Outlook will be automatically deleted from mailboxes and associated folders, sent items and deleted items after 3 months.
5. E-mails should be saved from Outlook into TRIM as soon as possible after being received. If the e-mail is not relevant for business purposes it should be deleted. An e-mail is important if it:
  - Has long term administrative or historical value.
  - Contains information, advice or explanation not duplicated elsewhere.
  - Relates to decisions taken and has evidential value.
  - Was drafted as a result of policy or legislation.

## Disclosure

6. Staff should be aware that e-mail messages could potentially be used as evidence in legal proceedings. In addition the department could also be liable for any negligent advice given by email, just as through other means of communication. It is also possible that an internal e-mail in one department may be disclosed in proceedings involving another.
  
7. Staff should be aware that electronic records, which include e-mails relating to business activity and transactions, are the primary corporate record of the Department and are designated as public records under the Public Records Act (NI) 1923 and Disposal of Documents Order 1925. Electronic records are subject to the DFP Records Management Policy Statement and should therefore be dealt with according to the guidance provided in the Records NI Procedures Manual. It is vital that all e-mails which relate to business activities or transactions are filed in the appropriate area within the departmental file plan in TRIM to ensure a complete and accurate record is retained.
  
8. E-mail is part of the corporate record of the department and as such is liable for disclosure in response to information access requests under the following legislation:
  - Data Protection Act 1998
  - Freedom of Information Act 2000.
  - Environmental Information Regulations 2004

Information regarding this legislation can be found at <http://www.informationcommissioner.gov.uk/>

Copies of the legislation are also available from the DFP Information Management Unit.

9. This policy is intended to protect the interests of DFP, as well as the interests of staff, and to ensure that individuals are not at risk of disciplinary action, criminal proceedings or civil action as a result of misunderstanding or lack of guidance.

## **Guidance**

10. It is the responsibility of all staff to ensure that Departmental policies and procedure for managing records including e-mails are adhered to. Management of electronic records will be provided in the Records NI Procedures Manual, which is available on the DFP Intranet. All staff should familiarise themselves with the content of this document to ensure that their interests and those of the Department are protected.

## **Security**

11. This policy also applies when using non-DFP resources, e.g. home computers or personal e-mail to conduct official business. Staff must not use non-NICS equipment or facilities for business unless they have prior permission to do so. If permission is granted they must ensure that such use does not compromise the security of official data or expose DFP systems or equipment to risk of disruption from any source, such as virus attack or unauthorised access. Staff should seek advice, as necessary, about IT security matters via their usual departmental IT contacts. Departmental guidance on IT Security can be found on the Intranet.
12. Staff must accept as a condition of use, that their usage of the Department's ICT facilities may be routinely monitored and should have no expectation of privacy, whether it is in the conduct of official business or for personal use.

13. It is the responsibility of each individual to ensure that the guidance set out in this policy and CSC 2/03 is adhered to at all times. This policy applies only to the use of e-mail and Internet usage. Failure to comply with the policy could result in disciplinary action, which may include dismissal. Users should note that they may be personally liable to prosecution and open to claims for damage should their actions be found to be in breach of the law. The Department will fully co-operate with law enforcement authorities to identify and take action in such cases. Should any business area or agency have a more stringent policy in place, the guidance provided in it should take precedence.