Department of
Finance
An Roinn
Airgeadais
www.finance-ni.gov.uk

Department of Finance
Records Management Policy

Implementation Date: 1 September 2016

Next Review Date: 1 September 2019

Introduction

1. The Department of Finance (DoF) is an information-based organisation. The service that it delivers to its customers, whether internal or external, depends on its efficiency in creating, using and storing information. Records must meet legislative, operational and archival requirements and support accountability in decisions taken by the organisation. It is therefore vital that management of this information is prioritised as an administrative discipline, which controls all aspects of the record from creation through to disposal in an appropriate manner.

Overall Commitment

2. The Department is committed to providing and complying with effective records management procedures which are integrated as key activities within the organisation by ensuring that:

    - the creation, management, review and disposal of records is carried out in a manner which accurately documents the functions of the organisation and is compliant with associated policy;

    - the records management function supports the regulatory environment within which it operates;

    - procedures, guidance and training are available to assist staff in producing records which reliably represent accurate information that was used in, or created by, the business process and which will enable integrity and authenticity to be demonstrated;

    - activities relating to records management from creation to disposal are adequately resourced, managed and monitored;

    - appropriate security measures are in place for storage, management and transportation of sensitive departmental information;

    - the departmental file plan is managed and maintained to retain records in a structured manner;

    - Information Asset Owners are appointed to each business area to ensure that departmental information assets are accessed, controlled and managed accordingly; and

- appropriate and secure procedures and processes are in place for sharing of information.

Role of Records Management

3. Records management is the term used to describe an administrative system by which the organisation seeks to control the creation, retrieval, storage, preservation or disposal of its records.

4. A record can be described as recorded information, in any format or media, created or received and maintained as evidence by the Department in the transaction or pursuance of business.

5. Effective records management will enable the Department to:

    - access records when required, providing timely information for operational need;

    - provide secure and legally admissible records demonstrating accountability;

    - ensure records, particularly those containing personal or sensitive information, are not retained for longer than is legislatively, legally or administratively necessary;

    - store historical records of past activity to provide a corporate memory;

    - make better use of space and storage facilities both physically and electronically;

    - optimise use of staff time;

    - improve control over records;

    - comply with legislation and departmental policy; and

    - reduce costs.

Responsibilities

6. *All staff*
   All staff in the department are responsible for:

    - ensuring they have a clear understanding of records management and demonstrate commitment to duties relating to record keeping;

    - creating records which are consistent, reliable, accurate and complete;

    - identifying records which should be captured because of their business function or content;

- recognising e-mails which are records and filing accordingly;

- capturing records which authentically document activities in the course of which they were produced;

- storing records in the appropriate area of the file plan within the Records NI system and in physical storage;

- applying security and access controls to records, where appropriate;

- ensuring that searching, viewing and browsing records is done only for departmental business purposes;

- finalising documents when appropriate to ensure they become departmental records; and

- applying appropriate disposal and retention actions to records based on the departmental Retention and Disposal Schedule.

Recordkeeping responsibilities should be defined, agreed and documented in Personal Performance Agreements as well as contracts relating to service provision on behalf of DoF, when working in partnership with both internal services and external bodies.

Records management training needs should be analysed by line managers, particularly if staff are finding it difficult to fulfil their records management responsibilities because they do not have the necessary records management skills or guidance.

7. *Business Area Information Managers*
   Business Area Information Managers (BAIMs) co-ordinate the compliance and monitoring of the records management policies and procedures throughout the Department. BAIMs may transfer or delegate some responsibility to appropriate members of staff within their business area.

8. *Departmental Information Manager/Records Manager*
   The Departmental Information Manager (DIM) and the Records Manager produce records management policies and procedures. They also co-ordinate the compliance and monitoring of those policies and procedures throughout the Department through the BAIMs.

9. *Information Asset Owners*
   Information Asset Owners (IAOs) are senior members of staff involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information, ensure

that information is fully used within the law for the public good and provide written input to the SIRO on the security and use of their asset. Business areas need to be able to demonstrate progress in:

- enabling staff to conform to the records management standards;
- identifying resource requirements; and
- areas where organisational or systems changes are required.

10. *Senior Information Risk Officer*
The Senior Information Risk Officer (SIRO) has overall responsibility for the organisational function of records management.

Statutory and Regulatory Environment

11. There are a number of pieces of legislation which impose the need for effective management of all Departmental records, both paper and electronic

12. The records of DoF, like those of other Departments, are public records under the terms of the Public Records Act (NI) 1923. It is therefore a legislative requirement for the Department to implement records management as set out in this Act and in the Disposal of Records Order (S.R. & O. 1925 No.167). The legislation lays down the procedures both for the destruction of records deemed to have no long-term value and for the preservation and transfer to PRONI of records selected for permanent preservation.

13. The Freedom of Information Act 2000 (FOIA) provides a statutory right of access to information held by public authorities (subject to exemptions). Public authorities are obliged to comply with the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000, which is intended to support the objectives of FOI legislation by outlining the management practices that should be followed by public authorities in relation to the creating, keeping, managing and disposal of their records. All information held by the Department is subject to the FOIA. No distinction is made regarding information held in remote locations or offsite storage. Staff should ensure that they are familiar with the content and requirements of the DoF Freedom of Information Policy Statement.

14. The Data Protection Act 1998 (the DPA) entitles individuals to access their personal information, which is being processed by another, on request. The Department is committed to managing records and applying appropriate security measures in compliance with the principles of data protection and in line with DoF Data Protection Policy Statement.

15. Environmental Information Regulations 2004 (EIR) stem from European rather than national legislation. EIRs provide the public with

a statutory right of access to environmental information held by public authorities.

16. Each business area should also consider and take into account any legal or regulatory obligations specific to their function.

Access and security

17. Whilst departmental policy places emphasis on open and transparent information, there are occasions when staff should consider if any of the information held within a document or file/container needs to be limited to a specific group of staff or, exceptionally, to only one or two individuals.

18. The Department remains committed in delivering openness and transparency of information, but is equally protective in ensuring sensitive information is appropriately restricted and only accessible to the relevant groups or business area.

19. Compliance checks will be carried out to ensure sensitive/personal information is appropriately restricted. Where access controls have not been appropriately applied to sensitive/personal Information, staff may be challenged.

20. Audit logs will also identify inappropriate viewing, previewing and/or editing of such information. The titling of some documents can clearly distinguish them to be personal or sensitive however, on occasion, these documents may have inadvertently not had the appropriate access controls applied. Staff must not view, preview or and/or edit such documents, but should inform their line manager or BAIM who will liaise with DoF Information Management Unit.

21. Staff are personally responsible for the safe-keeping of personal data in their possession and should ensure this is only accessed and processed in line with business need. Staff should also be aware that they must not search for or view information which is not appropriate to them or their business area. Any staff viewing or carrying out excessive searches for information (personal or otherwise) will be challenged and may face disciplinary action.

Responsibility for Historical Records

22. A record becomes historical when it reaches 20 years old and has been deemed to have permanent value for legal, administrative or research purposes. These records will be protected by the Department in consultation with the Public Record Office of Northern Ireland (PRONI).

23. The records selected for permanent preservation are outlined in the DOF Disposal Schedule and transferred to PRONI. Before transfer

can take place, the records must be reviewed under Part VI of the Freedom of Information Act 2000 (FOIA). Once transferred, these records become the responsibility of PRONI.

E-mail

24. The principles of this policy apply equally to e-mail and it is necessary to transfer e-mails relating to business activity and transactions to the appropriate area of the file plan within the Records NI system to ensure a complete and accurate representation of the record.

25. A 3-month rule has been imposed on all e-mail accounts. E-mails that have not been saved into Records NI system and remain within Outlook will be automatically deleted from mailboxes and all associated folders after 3 months.

Policy Awareness

26. A copy of this policy statement must be provided to all new members of staff and interested third parties. Existing staff and relevant third parties will be advised of the policy which will be posted on the Departmental intranet site and will be available through the publication scheme, as will any subsequent revisions. All staff and relevant third parties must be familiar with and comply with the policy at all times. This policy will be reviewed every three years, at a maximum.

Further Information

27. Any queries about information access legislation in the Department should be addressed to the relevant Business Area Information Manager or the Information Management Unit. Further information can also be provided by the Information Commissioner's Office.

Associated Documentation

28. This policy should be read in conjunction with:

- DoF Data Protection Policy
- DoF Access to Information Policy
- DoF Information Security Policy
- Departmental Guidance on Data Sharing

29. Copies of all these policies are available on DoF's internet and intranet sites.