Department of
Agriculture, Environment
and Rural Affairs

www.daera-ni.gov.uk

RECORDS MANAGEMENT POLICY STATEMENT

DEPARTMENT OF AGRICULTURE ENVIRONMENT AND RURAL AFFAIRS (DAERA)

Document Date: November 2020

Review Date: November 2022

Document information

Document details

Document name:	DAERA Records Management Policy Statement
Document version:	2.3
Document date:	02/11/2020
Document status:	Approved
Author:	[redacted]
Owner:	[redacted], DIM/DRO
HPRM reference:	AE1/20/1085083

Revision history

Version	Reason for change	Date	Comments
0.1	Initial document	01/07/2016	Creation of DAERA
1.0	Annual review	09/01/2019	Updated legislation
2.0	Annual review / ICO recommendations	02/11/2020	Include assurance including SIRO and SAG
2.1	Annual review / ICO recommendations	19/11/2020	Added Role of staff
2.2	Minor Update	08/03/2021	Refs to GDPR updated to UK GDPR
2.3	Annual Review	25/01/2022	Reviewed – no significant change

Distribution

Name	Position	Role	Date of Issue	Version
[redacted]	DIM/DRO	Owner	16/11/2020	2.0
[redacted]	DPO	Head of Branch	20/11/2020	2.1
[redacted]	SIRO	Head of Division	11/12/2020	2.1

Sign off

Approver:	[redacted]
Signature:	
Date approved:	17 December 2020

Contents **Page No**

RECORDS MANAGEMENT POLICY STATEMENT

Introduction

1. The Department of Agriculture, Environment and Rural Affairs (DAERA) holds a vast quantity of information in a variety of formats, including written and electronic formats, which has been created in the conduct of our business over the years. These records represent our corporate memory, providing historical evidence of our decisions and actions. They underpin our business by supporting our daily functions and operations, by contributing to policy formulation and decision-making and by acting as a reference store. They support consistency, continuity, efficiency and productivity, helping staff to execute business and deliver services in an equitable way.

2. Good records management reduces the risk of legal challenge or financial loss through control of content, storage and disposal; it maximises the achievement of best value for money in terms of human and spatial resources through greater coordination of information and storage systems. The Department is, therefore, dependent upon its records in order to operate efficiently and to account for its actions.

3. In publishing this Records Management Policy Statement the Department seeks to:
    - define a structure to ensure adequate records are maintained;
    - promote and develop best practice in records management throughout all the Department's business units by through the use of designated and structured maintenance, retention, and disposal system; and
    - assure value for money commensurate with legal, operational and information needs.

4. These things are critical as the Department continues with its restructuring of records management practices resulting from the introduction of RecordsNI as its officially designated Electronic Document Records Management System

(EDRMS) in 2007 – client then Tower Records Information Management (TRIM), then Hewlett Packard Records Management (HPRM) system, now Content Manager (CM) - while also ensuring that it remains in a position to meet legislative requirements relating to:

UK General Data Protection Regulation (UK GDPR): UK GDPR gives individuals more control over their personal data, and introduces more stringent measurable compliance requirements for organisations who process personal information.

Data Protection: The Data Protection Act (DPA) 2018 gives individuals the entitlement to have access to any personal information relating to themselves where this information is being held or processed by others. It must be provided within 1 calendar month of a written request. The Act, together with UK GDPR, also stipulates how personal data should be processed.

Freedom of Information: The Freedom of Information Act (FOIA) 2000 gives people the statutory right to information held by public authorities. Information must be provided within 20 working days of receipt of a written request. It was compliance with this legislation that required the Department to restructure its filing systems in order to improve the retrieval of information requested. The single official repository provided by RecordsNI supports this requirement.

Environmental Information: The Environmental Information Regulations (EIR) 2004 give people the right to information related to elements affecting the environment. Such requests may be written or oral and must be met within 20 working days.

5. While limited exemptions (FOIA & DPA) or exceptions (EIR) may apply under certain circumstances when dealing with requests for information under these pieces of legislation, these can often be overridden if the public interest is served better by disclosing the information. It is critical at all times that the Department's procedures for managing its records, both hard copy and electronic, enable the easy identification of all relevant documentation. This is beneficial also for the efficient conduct of the Department's business.

6. As a public body the Department is also bound by The Public Records Act (NI) 1923 and The Disposal of Documents Order 1925 which lay down procedures both for the destruction of records deemed to have no long-term value, and for the preservation and transfer to the Public Records Office of Northern Ireland (PRONI) of any records selected for permanent preservation. While procedures for dealing with these factors have been in place for many years, the introduction of RecordsNI has greatly increased the volume and importance of electronic records in all of this and has provided a reliable means for the drafting, version control, sharing, storage, indexing, audit, searching, classification and disposal of all electronic documents held by the Department. Previously such records were generally unmanaged as they were spread across various servers, desktops, local drives, shared drives, storage devices etc…presenting a significant risk to Departments.

7. While RecordsNI has long now been the official repository for information held on official record used by the Department, and most manual files have now been closed, the Department continues to operate a manual system for those files with a security rating above "Official Sensitive" and specific legal documents. Existing procedures remain in place for the management of these and also the disposal of manual files that were created and closed historically (pre-RecordsNI).

8. This Policy Statement is intended to demonstrate the Department's commitment to the use of best practice in the creation, retrieval, storage, preservation and destruction of both paper and electronic records. It should be considered in conjunction with NICS and Departmental policies, procedures and guidance; ICO guidance; ISO 27001; and the Lord Chancellor's Code of Practice on Records Management under Section 46 of the FOIA. Extensive guidance covering the main procedural aspects of using RecordsNI is now available on the Data Protection and Information Management Branch (DPIMB) intranet site. This guidance is being added to and updated regularly.

Objectives

9. The objectives of this Records Management Policy are to inform staff of their responsibilities which will be met by complying with this policy:

    - Accountability: adequate records should be kept and maintained to account fully and transparently for all actions and decisions;
    - Quality: records should be accurate and complete, containing authentic and reliable information;
    - Accessibility: information should be easily identified and retrievable from records to facilitate work and to respond to requests for information from those with a legitimate right to access;
    - Security: records should be held in a robust format which remains readable for as long as the information is required. They should be secure from unauthorised or inadvertent alteration or erasure. Audit trails should be available to track updates including changes. Access and disclosure should be controlled and monitored;
    - Retention and Disposal: there should be documented retention and disposal procedures to ensure consistency across the Department. These should include provision for permanent preservation of archived records;
    - Training: all staff should be made aware of their record management responsibilities as a result of generic and / or specific training programmes and the provision of advice by managers; and
    - Performance Measurement: compliance with records management policies and procedures should be monitored regularly locally by managers and by DPIMB, and appropriate action taken promptly to improve standards; and
    - Breaches: policy breaches should be managed by line managers within business areas, who should report ongoing issues to the Departmental Information Manager (DIM). The DIM can decide whether the breach warrants informing the Data Protection Officer, the Security Assurance Group (SAG) or the Senior Information Risk Officer (SIRO) who have oversight of security and assurance of systems around the processing of information including personal data.

10. As the achievement of these objectives rests largely with Business Areas it is important that Business Area managers consider resource implications when developing business plans, as well as PPAs and PDPs.

Policy Statement

11. It has long been NICS and DAERA policy that the Department's official records are the electronic versions held in RecordsNI and that any hard-copy paper versions are to be regarded as working copies for ephemeral use only. Where this is not possible, e.g. due to security classification as outlined in paragraph 7, paper versions will continue to be the official records. DPIMB is committed to reducing any risk associated with records management and to this end NICS regularly tests the EDRMS RecordsNI and has ensured that appropriate contingency arrangements are in place. DPIMB will also carry out Compliance Assurance Checks within Business Areas.

12. The Department will take all possible steps to ensure compliance with current and possible future legislation in the area of information and records management. In order to do so it is necessary for all the Department's records to be authentic, reliable and accessible; additionally, they must support business functions and activities and be retained only for as long as they are of use. To achieve this, the Department has established and maintains both manual and electronic systems which facilitate appropriate management practices in the creation, retrieval, storage, preservation and destruction of its records. This is being done through:
    - use across the Department of a file plan organised on a functional, not an organisational, basis (as for all NICS Departments);
    - appropriate EDRMS training for all users;
    - development of clear policy guidance in the form of records management and EDRMS guidance;
    - dissemination throughout the Department of this guidance, and access via DPIMB intranet pages;

- where legitimately held, reorganisation of legacy manual filing systems so that they operate on a functional basis (responsibility of IAOs);
- regular review of records held and registering of all information assets on Electronic Information Asset Register (eIAR);
- operation of an Assembly approved Retention and Disposal Schedule for all departmental records;
- training of staff in business areas to promote a clear understanding of records management issues in order to develop the necessary expertise in records management generally and with specific reference to dealing with information requests;
- continual monitoring of responses to information requests; and
- regular reviews of policies and actions taken.

13. This Policy Statement covers all recorded information, in any form, created or received and maintained by the Department or any member of staff in the transaction of business or conduct of affairs and retained as evidence of these activities. Information therefore includes anything handwritten or typed, emails, text messages sent and received from DAERA business mobile phones and other electronic records, films, photographs or slides, computer disks, microfilms or microfiches, audio and video material, imagery, maps, plans, drawings and all documentary material held under any other format by the Department.

14. It is envisaged that ongoing adherence to this Policy Statement will assist the Department in meeting legislative requirements while also enabling it to:
    - access records efficiently when they are required for internal work or management purposes;
    - comply with best practice;
    - make efficient use of staff time;
    - make efficient use of space and storage facilities for both manual and electronic systems;
    - have improved control over records; and
    - keep costs to a minimum.

15. Under this Policy Statement, which was originally endorsed by the Departmental Board, and any subsequent significant revisions endorsed by Top Management Team, overall responsibility for the management of Departmental systems of information and records rests with the Grade 3 Heads of Groups. However, in the case of the Department, many of the functions are devolved in the first place to the Departmental Information Manager (DIM), and secondly, to G7 / Heads of Branches (who will also be Information Asset Owners) acting with the support of local Information Managers (line managers), Day-to-day Administrators and Power Users who are expected to coordinate the day-to-day implementation of the Records Management Policy in their respective business units. Staff in DPIMB have an administration and coordination role and are available to advise on the day-to-day issues surrounding records management. All staff in business units, including Agencies, who have information management responsibilities – most, if not all, do - should have these clearly inserted into any job descriptions, Personal Performance Agreements (PPAs), and Personal Development Plans (PDPs) where any training or development is required. This will apply to most staff and line managers should thereby ensure that all such staff receive the appropriate training in records management from induction and on an ongoing basis.

16. The Department will audit its records management procedures regularly to ensure continued compliance with this Policy Statement which, itself, will be reviewed annually by DPIMB.

17. Line managers and business managers must take appropriate measures to ensure that staff comply with records management policies and procedures. Monitoring checks should therefore be completed by line managers to ensure that staff not only keep appropriate records in the first place, but that they properly manage and securely store electronic records and (exceptionally) hard copy records in accordance with policy. DPIMB may conduct random monthly checks to monitor EDRMS usage and the management of records within the EDRMS, and may highlight to staff / line managers were it appears that records management procedures are not being properly followed. DPIMB will keep an audit trail of these checks. Any significant policy breaches will be reported to the

Departmental Information Manager, and may be reported to the Data Protection Officer and / or Security Assurance Group who oversee the security and assurance of all DAERA information and records management systems.

Implementation of Records Management Policy

18. The Department's Records Management Policy Statement originates from a DARD document introduced in May 2004 and since then a lot of work has been done by both what is now DPIMB and business areas to improve upon the standard of records management across the current Department, and must continue.

19. Since the original Policy Statement was introduced in May 2004, there have been significant organisational changes including restructuring of NICS Departments in 2016, and a number of projects including EDRMS upgrades and the NICS Legacy Project to deal with information held on shares, nevertheless huge progress has been made in optimising compliance across the Department.

20. Business Areas should have all information assets registered on the Electronic Information Asset Register (eIAR), and all conventional records should be held in RecordsNI, the designated EDRMS repository. Heads of Branches as Information Asset Owners (IAOs) are also responsible for any data and information held in line-of-business systems, databases, legacy files including off-site storage, and any other location where information may be held regardless of media. More information provided under "Roles".

21. DPIMB can facilitate the provision of storage facilities only in exceptional circumstances and arrange with PRONI for one-off disposals of records where appropriate. IAOs are responsible for the annual review and disposal of any manual records held in accordance with agreed disposal schedules, including the transfer of those records to PRONI where they have been selected for permanent preservation. These procedures will continue for all manual records referred to in paragraph 7.

22. Electronic record keeping is accepted as the main means of record keeping in the Department and wider NICS. Where paper records are received or created these should be scanned and saved to the RecordsNI EDRMS and the paper copies destroyed appropriately.

23. Records saved to the RecordsNI EDRMS should be saved according to the classification and sub-classification structure agreed by NICS on a functional rather than organisational basis. Top level classifications will be similar for all NICS Departments for corporate functions, i.e. functions all Departments have in common such as “Accommodation & Services”, “Financial Management” etc…Operational functions vary between Departments and so top level classifications will vary between departments for operational records, e.g. only DAERA has “Agriculture, Food & Science”, “Animal & Veterinary Public Health”, “Rural Services” etc…

24. Where necessary corresponding paper and electronic records can be cross-referenced as hybrid files. The EDRMS captures active audit events for all records, facilitates restricting records where necessary and facilitates review and disposal of electronic records similar to that in place for manual records. For disposal purposes all EDRMS book level classifications should have “triggers” in place based on the Departmental Retention and Disposal Schedule approved by the NI Assembly.

25. Work to ensure continued compliance with this Policy Statement will be required from DPIMB, senior management and Business Units. This will include:
    - Business Units to ensure records management training at the earliest opportunity for new staff and anyone returning from long term absence who has not already been trained;
    - Business Units (IAOs, Line Managers, Day-to-day Administrators, Power Users) to ensure compliance with Records Management policies and procedures, including RecordsNI guidance, through appropriate monitoring and checks;

- Managers to ensure that records management continues to be included in Business Plans and Personal Performance Agreements (PPAs), and also Personal Development Plans (PDPs) if training or development needed;
- Business Units to carry out a review of all manual (at least annually) and electronic (at least quarterly) records that have reached their review date and follow appropriate disposal procedures;
- DPIMB and Business Units to ensure the temporary retention ("hold") of records due for destruction which are the subject of any ongoing legal action, information access request or any complaint or appeal following the non-disclosure of information: such temporary retention will continue until the action, complaint or appeal has been resolved;
- DPIMB will monitor compliance with legislative deadlines with respect to requests for information under the Data Protection Act 2018, General Data Protection Regulation, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004;

26. The NICS has made a significant investment in its EDRMS and Business Areas have devoted considerable resource to populating and maintaining it. While it may not be perfect, RecordsNI provides a more focused and efficient approach to the management of records than previous practices and it is important that staff continue to use and maintain the system as intended to ensure that the Department continues to realise the savings and business benefits that the system has delivered. This is particularly important given that many Business Units often find meeting the legislative requirements of dealing with information access requests challenging – which can be supported if records are properly saved and titled.

27. Taking account of these factors it is important that Business Units should allocate sufficient resources to Records Management and not view it as a competing priority. Good records management practice is not a competing priority, rather it underpins almost everything the Department does including its highest priorities. This should be reflected in Business Plans being signed off by senior management.

28. While DPIMB takes the lead in the implementation of all records management issues it is largely up to Business Units to ensure that the Records Management Policy is fully adhered to throughout the Department on an ongoing basis. Staff in the Records Management Section of DPIMB are available to provide advice at all times. Contact details for Records Management staff and a range of useful guidance documents are available on the Records Management intranet pages.

Roles – all staff

29. DAERA's Senior Information Risk Owner (SIRO) is accountable to the Accounting Officer (the Permanent Secretary), is familiar with information risks, and leads the Department's response to those risks. The SIRO is the focus for the management of information risk at Board level and chairs the Security Assurance Group. The SIRO is named and trained on appointment, takes the lead in the department's strategic approach for managing the organisations information risks, including maintaining an information risk register.

30. The Security Assurance Group's remit includes oversight of the security and assurance of information and record management by DAERA and any significant policy breaches will be reported to this group by the Departmental Information Manager (DIM) or Departmental Information Assurance Officer (DIAO). This may include incidents other than those reported by staff using the "big red button" incident-reporting tool found on the front page of the "DAERA Security Centre" (intranet).

31. The Departmental Information Manager (DIM) leads on information and records management and is appointed by the Accounting Officer (Permanent Secretary). The role of a DIM is to ensure the department is compliant with Records Management best practice and relevant legislation including the Public Records Act (NI), UK GDPR, Data Protection Act, Freedom of Information Act, and Environmental Information Regulations. The DIM works closely with the Data Protection Officer (DPO) on matters concerning personal data and with colleagues across the department to support compliance with legislation. Also to

reduce risk of maladministration should the Department not properly keep record of key decisions made, including the rationale for decision-making, in accordance with Lord Chancellor’s Code of Practice on the management of records issued under Section 46 of the Freedom of Information Act and also the Northern Ireland Public Service Ombudsman's' Principles of Good Administration.

32. The Data Protection Officer (DPO) is appointed under UK GDPR to monitor internal compliance, inform and advise on data protection obligations. The DPO is independent, an expert in data protection, and reports to the highest management level. DPOs can assist IAOs demonstrate compliance and are part of the enhanced focus on accountability with responsibility for ensuring the Department adheres fully with the requirements set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.

33. The Departmental Information Assurance Officer (DIAO) is responsible for policy related to information assurance, advice on information assurance, oversight of the eIAR, incident management (data breach, information loss), supporting IAOs, and leading on Assurance Checks around compliance.

34. Information Asset Owners (IAOs) – in DAERA these are generally Heads of Branches (Grade 7) - are accountable to the SIRO. IAOs are senior officials whose business areas use one or more registered information asset. Their role is to ensure that information (particularly any personal data) they are responsible for is protected appropriately; and also that where information is shared that the proper confidentiality, integrity and availability safeguards apply, for example they should know what information their business areas hold, why they hold it, what it is used for, where it is held, for how long, who has access to it, ensure it is available for all necessary purposes, and when/how it will be disposed of.

35. IAOs are responsible for ensuring all information assets are properly registered on the eIAR and that the eIAR is kept up to date. They are expected to provide assurance on a regular basis that any information assets they are responsible for are being managed in accordance with all policies, procedures and legislative requirements. One example of this will be via annual Stewardship Statements, another will be through any audits or compliance Assurance Checks.

36. Line Managers – line managers are also local information managers and are responsible for ensuring their staff manage records in accordance with policies and procedures. This is whether they themselves have a designated role or not, such as Day-to-day Administrator or Power User for local administration of records held in RecordsNI. Line Managers should ensure records management responsibilities are included not only in their own but in staff's PPAs and where appropriate PDPs.

37. All staff – all staff have their role to play and all are responsible for ensuring the records they manage are managed in accordance with NICS and DAERA Policies and Procedures. All staff should ensure they have records management responsibilities includes in their PPAs. This is whether they themselves have a designated role or not, such as Day-to-day Administrator or Power User for local administration of records held in RecordsNI. All staff should ensure records management responsibilities are included their PPAs and where they feel they need more training or development that this is reflected in their PDPs.

For more information including contacts:
Data Protection and Information Management Branch
Records Management

Annex A – Glossary of acronyms

These are acronyms that not only feature in this document but are also used and commonly referred to elsewhere.

Systems:

EDRMS	- Electronic Document Record Management System (Records NI)
TRIM	- Tower Records & Information Manager (now Content Manager)
HPRM	- Hewlett Packard Records Manager (now Content Manager)
CM	- Content Manager (current EDRMS)
eIAR	- Electronic Information Asset Register

Legislation:

FOIA	- Freedom of Information Act
EIR	- Environmental Information Regulations
DPA	- Data Protection Act
UK GDPR	- UK General Data Protection Regulation

Designated Roles:

SIRO	- Senior Information Risk Owner
DPO	- Data Protection Officer
DIM	- Departmental Information Manager
DRO	- Departmental Record Officer
DIAO	- Departmental Information Assurance Officer
IAO	- Information Asset Owner

Authorities / Branches / Groups:

DPIMB	- Data Protection & Information Management Branch
SAG	- Security Assurance Group
PRONI	- Public Records Office Northern Ireland

Other:

PPA	- Personal Performance Agreement
PDP	- Personal Development Plan