Radioactive Waste Management

RWP104 Information Governance Policy

Rev	Date	Description	Owner	Approvers
1	October 2018	New format introduced, combined RWP103 and RWP104 into one policy document (RWP104). Introduction of IP.	P Welch	RWM Board
0	3 June 2015	First issue of policy	H Harding	RWM Board

Radioactive Waste Management

Foreword

In fulfilling its mission RWM holds and processes a wide range of information, spanning publicly available information, sensitive nuclear information and personal data. RWM needs to handle this information in ways that ensure its:

- **Confidentiality**: ensuring information is not made available or disclosed to unauthorised entities;
- **Integrity**: ensuring information is suitably accurate;
- **Availability**: ensuring information is accessible when and how it is needed.

Implementing this Policy will help achieve these aims; protect against threats such as cyber attack, theft, misuse and loss of information; and contribute to the efficient delivery of our mission by making informational readily available to those who need it and supporting innovation and organisational learning. Achieving our mission will span many decades and we need to recognise the particular challenges this presents for effective information governance.

Professor Malcolm Morley, Chairman

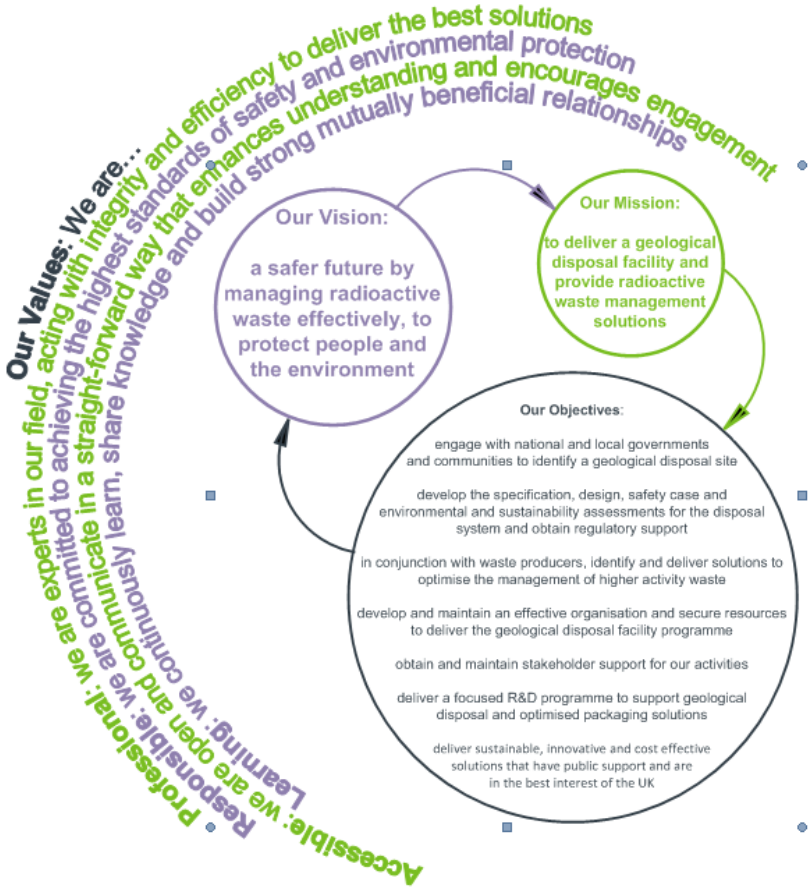
Signed:

Date:

Bruce McKirdy, Managing Director

Signed:

Date:



Radioactive Waste Management

Information Governance Introduction

RWM's Information Governance Policy sets out how RWM will discharge its responsibilities for the management of the information it holds and uses. The policy also reflects the expectations of Her Majesty's Government (HMG) and the Nuclear Decommissioning Authority (NDA). It incorporates requirements placed upon us by the HMG Security Policy Framework and relevant NDA policies.

The policy covers Data, Information, Knowledge and Records:

- **Data**: set of discrete, objective facts about an event;
- **Information**: evaluated, validated, or useful data;
- **Knowledge**: possessed by people, it is the effective combination of information and insight or experience;
- **Records**: information created, received and maintained as evidence and information by an organisation or person in pursuit of legal obligations or in the transaction of business.

RWM creates **Intellectual Property (IP)** which is owned by the NDA. RWM uses that IP under license from the NDA and manages it on the NDA's behalf.

Information Governance Goals

- **Data, Information, Knowledge** and **Records** (described collectively in this policy as **"information"**) are managed to support delivery of RWM's mission and objectives.
- Business processes are developed to realise **opportunities to create, manage and store** information so that its **provenance and integrity** is maintained and the information is available and accessible when needed.
- **Information risks** are identified and managed. Risks will be reviewed periodically to identify improvements in the management of information.
- Information is periodically reviewed to check that it is **still required** and remains **fit for purpose**, recognising the long-term nature of RWM's mission.
- A **learning culture** is promoted and **training and awareness raising** delivered as part of an integrated approach to meeting this and other policies.
- **Waste package records** requirements are **specified** for those wastes intended for geological disposal or management in accordance with Scottish Higher Activity Waste Policy.

Radioactive Waste Management

Information Governance Policy

To realise our goals we will:

- **Appoint roles** that have responsibilities delegated from our Managing Director:
  - **The Senior Information Risk Owner (SIRO)** will be a member of our Board with a focus on **strategic information risks** to the delivery of our Mission.
  - An **Information Governance Officer (IGO)** will be a member of our senior leadership team responsible for **information Governance matters** within RWM.
  - **Information Asset Owners** will be at Functional Lead level and are responsible for **information within their area of responsibility**.
  - **Data Protection Officer** is consulted on all matters relating to the handling and storing of **personal data**.
- **Proactively manage our information and knowledge** so that it remains **accessible** to the systems, processes and people that need it and for as long as it is needed to perform activities to deliver our long-term mission:
  - Maintain an **information asset register** and **manage risks and identify opportunities** to achieve effective information management.
  - Understand the **scope, content and volume** of retained information and apply appropriate **retention periods** so that information is only kept for as long as it is needed.
  - Plan the management of **new information** and **identify opportunities to create and effectively manage** information early in process design.
  - **Store and maintain** information in such a way that its **physical integrity** is preserved. Approved media and format must be used for storing information so that integrity is maintained and information is accessible when needed, until a decision is made that it should be destroyed.
  - Create and maintain **Vital Records** (information relating to radioactive materials, their quantity, characteristics, properties, location and containment), so that their content is **accurate and reliable**.
  - Collect and use **personal data fairly and transparently** in line with data protection legislation.
  - **Anonymise or redact personal information** where appropriate.

Radioactive Waste Management

- Have **metadata** for all new information that meets **agreed standards**.
- **Store** information in **appropriate locations** depending on its age, retention period, storage media type and access requirements.
- Apply **appropriate and approved controls** to the **migration** of information.
- **Safeguard information** (including its metadata), especially where **storage media is changed**.
- **Control,** via an approved process, the **formal handover of information** and **transfer of responsibility** for its ongoing management.

- Work with **waste producers** to encourage preparation and **retention of necessary Vital Records** relevant to the disposal of waste.

- **Proactively manage our information and knowledge** so that it remains **secure**:
  - **Classify** all information in accordance with the **Government Classification Scheme**. All staff and contractors will have the security clearance appropriate for the information they will be required to have access to.
  - Apply the **"Need to Know" principle**; which requires that knowledge or possession of classified information must be strictly limited to those members of staff, or trusted third parties, who have the appropriate security clearance and a clear justification for access.
  - Work with the NDA as our main Information and Communications Technology providers to protect information from cyber-attack and theft.

- **Benchmark** current **information and knowledge management practice** using appropriate assessment and assurance models and use third party assurance to **appropriate standards** to contribute to continuous improvement.
  - Participate in **Communities of Practice** relevant to information and knowledge management to encourage sharing of information and knowledge and learning from others.
  - Regularly **test the effectiveness of security measures** (including those in place for the protection of personal data) and implement improvements as appropriate.