www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Electronic Information Asset Management Policy

June 2020

“Building a borough for everyone – where residents and businesses grow, with opportunities for all”

Our vision is underpinned by six priorities:

Healthy, skilled and independent residents
Growing economy, affordable housing
Safe and vibrant communities
Attractive and well-connected borough
An excellent customer experience
Well-managed resources delivering value for money

CONTENTS

Frequently used acronyms

IT	Information Technology
RBWM	Royal Borough of Windsor & Maidenhead
EIA	Electronic information assets
IA	Information Assets
IAO	Information Asset Officer
PA	Physical Assets
SA	Software Assets
PED	Portable Electronic Devices

1 PURPOSE

1.1 The purpose of this Electronic Information Asset Management Policy is to ensure that the applicable and relevant security controls are set in place in line with the Royal Borough of Windsor and Maidenhead requirements.

1.2 The Royal Borough of Windsor and Maidenhead (the council) recognises the importance of its Electronic Information Assets (EIA), and the need to identify, track and protect them.

2 SCOPE

2.1 This policy covers the protection of all Electronic Information Assets which includes Information Assets (IA), Software Assets (SA), Physical Assets (PA) or Portable Electronic Devices (PED).

2.2 All council Electronic Information Assets must be identified, tracked, and protected. They must be assigned to named individuals who must be made aware of their responsibility to protect these assets and the information stored on them.

2.3 Electronic Information Assets must be accurately identified and published in the Information Asset Register (IAR). The register must define the responsible Asset Owners (AO) for every asset.

2.4 The council's Head of HR, Corporate Projects and IT is responsible for the definition of processes to manage Electronic Information Assets, and for the technical protection of Electronic Information Assets.

2.5 The council is committed to provide training and communications to ensure everyone working for the council understands their security responsibilities.

2.6 This policy does not cover the management of non-electronic information assets (e.g. paper documents) and the management of software licences relating to Electronic Information Assets.

3 APPLICABILITY

3.1 This policy applies to all council employees and RBWM Councillors. This policy also applies to contractors, temporary, agency staff, partners and others working in a similar capacity that can access, manage, or process Information Assets of the council. They are also accountable for understanding and adhering to the guidance contained in this policy and any applicable supporting policies and procedures. All applicable persons listed above are referred to as 'users' in this policy.

3.2 This policy does not cover work undertaken by external consultants who independently use their own IT technology and Electronic Information Assets. Their Data Protection Act 2018 and information protection obligations must be stated in their contract for council work.

4 AUTHORISATION

4.1 Only authorised persons should have access to council assets and systems or accessing the council IT or mobile network. Any user that deliberately or inadvertently accesses the council IT or mobile network or systems unauthorised, will be in breach of this policy.

4.2 For any council business:

- Users accessing council IT facilities must comply with all council policies and procedures.
- Managers and Team Leaders must ensure their staff comply with this policy and provide advice to them.
- Managers and Team Leaders must ensure security incidents are raised in response to IT access security concerns or security breaches as covered in the Reporting security incidents policy.
- IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed.
- IT Services ensure that privileged and systems administrator access is strictly controlled for all applications they administer based upon a valid business justification and specific job requirements as approved by the user's line managers.

5 POLICY COMPLIANCE

5.1 **Compliance Measurement**

5.1.1. All users must comply with this policy.

5.1.2. IT Services will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.3. If you do not understand the implications of this policy, how it may apply to you, or your security responsibilities when working with the council, please seek advice in advance from your line-manager or contact the council's Data Protection Officer at **dpo@rbwm.gov.uk**.

5.2 **Exceptions**

5.2.1. Any exception to the policy must be approved by the IT Senior Management Team in advance.

5.3 **Non-Compliance**

5.3.1. Any breach of this policy may be subject to disciplinary action under the council’s disciplinary procedures, up to and including dismissal. In circumstances where it is believed that a criminal offence has been committed the matter may be reported to the Police.

6 ROLES AND RESPONSIBILITIES

6.1. Users must ensure that Electronic Information Assets allocated to them are protected. They must also ensure that all assets allocated to them are returned to IT Services when such assets are not required for council business or when they leave the council.

6.2. Council Directors are responsible for the security of Electronic Information Assets and are accountable for legal compliance, including the Data Protection Act 2018.

6.3. Council Directors, Heads of Service, Service Leads and Managers are accountable for the protection of data stored on Electronic Information Assets used by their teams and others working for them. They must ensure that their users complete the leavers form and return all PA issued to them to the Information Asset Officer (IAO) before they leave the council. They must ensure employees and other users working for them have read and adhere to all policies.

6.4. IT Services are responsible for the procurement, technical security set-up and re-issue of all council Electronic Information Assets.

6.5. The Information Asset Officer is responsible for the registration and update of asset detail and responsible owners' (Asset Owners) detail in the Information Asset Register.

6.6. The Information Asset Officer is responsible for coordinating regular stocktakes of Electronic Information Assets, and consequent follow-up investigations and actions.

6.7. The Information Governance Team is responsible for monitoring policy compliance, e.g. spot checks that leavers have returned their electronic devices.

7 INFORMATION ASSET CONTROLS

7.1. Electronic Information Assets must be accounted for to maintain the appropriate level of protection.

7.2. Ownership of each Information Asset will be linked to the asset owner and recorded in the Information Asset Register.

7.3. Asset Owners will follow the requirements of the **Care of Council Owned Equipment Policy** with further guidance on asset management and should be read in conjunction with this policy.

7.4. The Information Asset Officer will provide reports to the Royal Borough of Windsor and Maidenhead Senior Information Risk Owner (SIRO), annually on assurance and usage of council Electronic Information Assets.

7.5. Electronic Information Assets must be ordered and obtained only through IT Services.

7.6. IT Services must ensure the asset owner completes, signs, and dates the **Care of Council Owned Equipment Issue Record Form** accepting responsibility for the Information Asset until it is handed back or replaced.

7.7. The Information Asset Officer must update the Information Asset Register with all the detail of the captured in the **Care of Council Owned Equipment Issue Record Form**.

7.8. Electronic Information Assets fall into 3 categories:

- IA - Information Assets (databases and data files, system documentation, user manuals, training manuals etc)
- SA - Software Assets (application software, system software, development tools etc)
- PA - Physical Assets (computer equipment, communications equipment, magnetic media, mobile phones, documentation, etc)

7.9. Only authorised or officially purchased and properly licensed SA will be used on any PA accessing the council's network and systems. The terms and conditions of the license must be adhered to.

7.10. Only approved SA installed by IT Services will be used for council business.

8 ASSET IDENTIFICATION AND REGISTER

8.1. All council Electronic Information Assets will be recorded and maintained by the Information Asset Officer in the Information Asset Register.

8.2. The Information Asset Officer must ensure that all physical assets are identified by marking them with a council asset tag number.

8.3. Each register will include the below information:

- Asset make and model
- Product number
- Asset tag number or phone number
- A unique serial number (Not for phones)
- SIM number
- IMEI number
- Asset owner (AO)
- Directorate
- Service Area
- Support/Warranty Information
- Category of asset
- Classification of asset
- Final disposal details
- IT issuer name

- Date of Transfer.

9 INFORMATION ASSET TRANSFER

9.1. The Asset Owner (or their manager) must hand all physical assets back to the Information Asset Officer when these assets are no longer required or used.

9.2. The transfer of physical assets from the Asset Owner to another Asset Owner are not allowed.

9.3. The status of physical assets handed back to the Information Asset Officer will be updated in the Information Asset Register.

9.4. IT Services or the Information Asset Officer will acknowledge receipt of a physical asset by completing **The Return of Council Portable Electronic Devices form**.

9.5. The Information Asset Officer will hand the physical assets to IT Services for a complete software rebuild and update.

9.6. A new asset owner must complete and sign the **Care of Council Owned Equipment Issue Record Form** when any physical assets are issued to them.

9.7. The Information Asset Officer will ensure the detail of the Electronic Information Assets and the new asset owner is captured in the Information Asset Register.

10 LEAVERS PROCESS

10.1. Physical assets must be returned to the Information Asset Officer by the asset owner or their manager prior to the person leaving the council.

10.2. The Information Asset Officer must update the Information Asset Register with receipt of asset from asset owner or their manager.

10.3. IT Services or the Information Asset Officer will acknowledge receipt of a physical asset from the Asset Owners by completing **The Return of Council Portable Electronic Devices form**.

10.4. The Information Asset Officer will hand the physical asset to IT Services for a complete software rebuild and update.

10.5. IT Services will keep the physical asset in stock until the Information Asset Officer transfers it to a new asset owner.

11 ASSET DESTRUCTION, DISPOSAL OR RE-ISSUE

11.1. The IT service will complete a software rebuild and update and check if a physical asset is still fit for purpose before it can be re-issued.

11.2. IT services will ensure that for all physical asset that must be destroyed (or disposed of), the storage area is either physically destroyed, or that data storage areas are electronically destroyed in accordance with certified security standards.

11.3. IT services will keep accurate and up to date destruction and disposal records, and these records will be made available for audit inspections if required.

11.4. The Information Asset Officer will include the following for all asset destruction or disposal:

- Date, time, method, and company or personnel responsible for the disposal of the asset will be recorded in the Information Asset Register.

11.5. This will ensure that assets are identified and managed all the way through to their final disposal.

12 INFORMATION ASSET STOCKTAKES AND CHECKS

12.1. A full Information Asset stocktake must be completed yearly by the Information Asset Officer.

12.2. The Information Asset Officer must provide accurate and complete information about all the councils' Electronic Information Assets.

12.3. A physical check of all Electronic Information Assets must be completed regularly by the Information Asset Officer and cross-checked with the Information Asset Register.

12.4. All council Electronic Information Assets that involve council data/information will be disposed of in accordance with the requirements of Government Guidance for the type of asset.

Document Name	**Electronic Information Asset Management Policy**		
Document Author	**Security manager**		
Document owner	**Head of HR, Corporate Projects and IT**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**15/12/2014**	**Security manager**
	Version 2	**19/09/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		