ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk Royal Borough of Windsor & Maidenhead

Security Policy

ELECTRONIC INFORMATION ASSET MANAGEMENT

Introduction and Policy Aim

The Royal Borough of Windsor and Maidenhead (the council) recognises the importance of its information assets, and the need to identify, track and protect them. This policy covers the protection of electronic information assets such as portable electronic devices and computers. It defines the requirements for the management of Council electronic assets. The aim is to establish professional good practice.

Policy Statement

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.

Electronic information assets must be accurately identified and published in an Information Asset Register. The register must define who is responsible for, and must protect, every asset. Those responsible are known as the information asset owners.

The council's Head of IT is responsible for definition of processes to manage electronic information assets, and their technical protection.

The council is committed to provide security training and communications to ensure everyone working for the council has the opportunity to understand their responsibilities. The stated preference is for online training and knowledge tests.

Not Covered by this Policy

Council mobile phones, which have different asset marking, asset register and support arrangements.
The management of non-electronic information assets, e.g. paper documents.
The management of software licences relating to electronic information assets.

Those Affected by the Policy

This policy applies to Councillors, employees of the council, contractors, agency staff, and others working in a similar capacity. It also applies to volunteers and partner organisations, and individuals who do work for the Council.

It does not cover work done by external consultants who independently use their own IT technology and information assets. Their Data Protection Act 1998 and information protection obligations must be stated in their contract for council work.

Roles and Responsibilities

1. Those affected by the policy – must ensure that electronic information assets allocated to them are protected. They must also inform the IT Service when such an asset previously allocated to them is transferred to another person.

2. Council Directors – are responsible for the security of information assets and are accountable for legal compliance, including to the Data Protection Act 1998.

3. Council Directors, Heads of Service, Service Leads and Managers - are accountable for the protection of data stored on electronic assets used by their

staff and others working for them. They must ensure that their staff return electronic information assets issued to them before they leave the council.

They must ensure employees and others working for them are aware of and in a position to comply with this policy.

4. The IT Service – is responsible for the procurement, technical security set-up and re-issue of council electronic information assets. Also for the maintenance of complete data about these assets and their owners.

   It is responsible for coordinating regular stocktakes of electronic information assets, and consequent follow-up investigations and actions.

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

Policy Compliance

If you are found to have breached this policy by not complying with its rules and responsibilities you may be subject to the council's disciplinary procedure or other action. If you are suspected of breaking the Law, you may be subject to prosecution.

If you do not understand the policy or how it applies to you, seek advice from your council manager, the IT Service, or from the Information Governance Team..

Applying the Policy

The rules that apply to electronic information asset management are defined below.

Obtaining a Council Information Asset

Rule 1 Electronic information assets must be ordered and obtained only through the IT Service and must not be ordered directly from manufacturers.

Identifying Council Information Assets

Rule 2 The IT Service must ensure that electronic information assets are identified by marking them either with an asset tag number or some other visible indication of council ownership

Owning an Information Asset

Rule 3 The person receiving a council electronic device (asset) must sign a security declaration when it is issued to them. The person issuing an electronic asset must ensure details about the person to whom it is issued are captured.

Transfer of an Electronic Asset

Rule 4 The IT Service must be informed by the asset owner (or their manager) when an electronic asset is going to be transferred to another person. The IT Service must ensure transfers are added to the Information Asset Register.

Rule 5 A new information asset owner must sign the appropriate security declaration before using the asset.

Rule 6 Every transfer of an asset from one person to another must be recorded in the appropriate Information Asset Register.

Information Asset Owner Leaves the Council

Rule 7 Electronic information assets must be returned to the council manager responsible prior to the person leaving.

Rule 8 The IT Service must check assets returned by council managers and either register a transfer of ownership or keep the asset in stock. The appropriate Information Asset Register must be updated.

Asset Destruction, Disposal or Re-issue

Rule 9 The IT Service must give every person returning an electronic information asset a receipt to confirm its return. The IT Service must check assets to decide whether they can be re-issued.

Rule 10 If the asset must be destroyed (or disposed of) IT must ensure that its data storage area is either physically destroyed, or that data storage areas are electronically destroyed in accordance with certified security standards.

Rule 11 The IT Service must keep accurate and up to date destruction and disposal records, and they must be made available for audit if required.

Electronic Asset Stocktakes and Checks

Rule 12 A full asset stocktake must be completed regularly.
Information asset owners must provide accurate and complete data about all of the assets they own when so requested.

Rule 13 A physical check of electronic information assets within the IT Data Centre must be completed regularly, and cross-checked with asset transfer records.

Policy Training

Online policy training and knowledge testing will be offered whenever possible.

Related Policies and Procedures

Information Handling Security Policy Storage of Information Policy
Use of Mobile Phones Policy

Legal Obligations

UK Data Protection Act

Related Documents and Sources

The Role of the Information Asset Owner, National Archives

Definitions

Electronic Information Asset – any electronic device capable of storing, processing or transmitting electronic information and therefore requiring information security protection. Also known as **Portable Electronic Devices (PEDs).** This includes, but is not limited to, desktop computers, portable computers and laptops, USB memory sticks, Internet smartphones, mobile telephones, CDs and DVDs, cameras, memory cards, dictaphones.
Information Asset Register – the published record of information assets owned by the Council.
Information Asset Owner – a named person assigned responsibility for the protection of an asset.