www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Care of Council Owned Equipment 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

1 PURPOSE

1.1 The purpose of this Care of Council Owned Equipment 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 Many employees are issued with items of equipment owned by the council for use as part of their day to day responsibilities. This will include computer devices and portable computer devices, collectively known as computing equipment. This computing equipment helps staff in the performance of their duties within council buildings, as well as out of the office on council business and working at home.

1.3 Most computer equipment is valuable and highly desirable to thieves. The council works closely with the local Police to reduce the level of theft of such items in the borough. This policy sets out the expectations of the council in relation to the care of council owned equipment and the responsibilities of staff.

2 SCOPE

2.1 This Care of Council Owned Equipment Policy ensures the Royal Borough of Windsor and Maidenhead implement the correct processes and procedures relating to the care and responsibility of council equipment. This policy is aimed at all users who are authorised to use computing equipment ensuring they are aware of the security risks relating to computing equipment and comply with the council's confidentiality and security standards.

2.2 This policy covers the use of all council owned equipment including computing equipment such as portable electronic devices, purchased, or authorised by the council. Portable electronic devices - includes laptops, notebooks, tablet computers, PDA's and Smartphone's e.g. iPhones, Windows phones etc.

2.3 The principles set out in this policy also cover any council owned non-IT equipment issued by service areas.

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 are referred to as 'users' in this policy.

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 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 SECURITY MEASURES

6.1 To reduce the risk of loss of computing equipment or data and unauthorised access to council computing equipment the following measures are in place:

- An asset control form is completed for each computing device provided to a user; and this user is listed in the asset register as the nominated Asset Owner.
- The completed asset control form will be signed and dated by the Asset Owner.
- All computing equipment is security marked with a council asset label.
- Encryption is applied to all computing equipment.
- Password protected screensavers are installed on laptops.
- Anti-virus software is installed on computing devices and is automatically updated.
- Regular backups are taken of the data stored on the council's shared network drives
- No data should be stored on mobile computing equipment.
- Disposal and re-issue of computing equipment is recorded in the asset register.
- Always wear your identity badge when you are on council business or in council buildings.
- Escort anyone in council buildings without an identity badge to reception.
- Escort visitors around the building whenever possible.

7 RESPONSIBILITIES AND RISK

7.1 Users have a responsibility for the safety and security of council equipment and are expected to exercise reasonable care with council equipment whilst it is in their possession. This applies to working in the office environment as well as working out of the office.

7.2 Users need to be security conscious and follow common-sense rules with further guidance on asset management as covered in the **Electronic Information - Asset Management Policy** which should be read in conjunction with this policy and can be found on the council's web site.

7.3 **Users must:**

- Store computing equipment securely when not in use on and off site.
- Exercise reasonable care with council equipment whilst it is in their possession.
- Store all Council data on the council's cloud storage (RBWM OneDrive) or network drive unless there is no alternative.
- Obtain authorisation from Heads of Service and IT Services before any data is stored locally on a computing device.
- Protect files containing personal or confidential data adequately e.g. encrypted and password protected.
- Obtain authorisation before they remove computing equipment from the premises.
- Be aware that software and any data files created by them on council computing equipment are the property of the council.
- Immediately report any stolen council computing equipment to the police and your line manager - Police Theft Report has been raised, see the **Thames Valley Police** website and comply with the **Reporting Security Incidents Policy**.
- Be aware that the security of their mobile computing equipment is their responsibility.
- Ensure that computing equipment is only used by council employees and authorised users for council business.
- Ensure that computing equipment is returned to the council when they leave employment at the council (A final salary deduction may be made if equipment is not returned).

7.4 **Users must not:**

- Disable the virus protection software or bypass any other security measures put in place by the council.
- Store personal information on computing equipment unless the equipment is protected with encryption, and it is necessary to do so.
- Remove any council personal information off site without authorisation.

- Use any removable media e.g. USB/memory sticks, DVD/CDs etc.
- Use mobile computing equipment outside the council premises without authorisation.
- Use their own mobile computing equipment for any council business unless authorised to do so.
- Allow the use of computing equipment in their charge to be used by unauthorised persons/friends/relatives.
- Leave computing equipment in unattended offices or places where anyone can easily steal them.
- Leave computing equipment visible in the car when traveling between locations.
- Leave computing equipment in an unattended car.
- Leave computing equipment unattended in a public place e.g. hotel rooms, train luggage racks.
- Install unauthorised software.
- Download unauthorised software / data from the internet.
- Delay in reporting lost or stolen equipment.
- Leave security doors/fire doors or windows open when the office is empty or at the end of the day.

8 INSURANCE CLAIMS

8.1 The council has limited insurance cover for portable equipment such as laptops, whilst on council premises. Claims for theft can only be made where there is evidence of a forcible entry or exit. An excess fee applies (refer to the Insurance & Risk team).

8.2 If computing equipment is stolen from a user's home or vehicle, it may be possible for a claim to be made under the user's household contents or vehicle insurance policy. All users should check the wording of their insurance policies to clarify whether such work equipment would be covered in the event of loss or damage.

8.3 In the event of theft or damage to computing equipment resulting directly from a user's recklessness or gross carelessness with regard to their responsibilities outlined in this policy, the matter may be investigated under the council's Disciplinary procedure and if appropriate, disciplinary action may be taken. In cases where recklessness or gross carelessness is proven the council reserves

the right to ask users to pay a reasonable contribution towards the repair or replacement of the item.

8.4 Managers are responsible for ensuring that users issued with valuable equipment complete the **Care of council owned equipment issue record form**

8.5 Following a theft of council equipment or assets from either themselves, or their users, managers must ensure a Police Theft Report has been raised, see the **Thames Valley Police** website**.**

Document Name	**Care for Council Owned Equipment Policy**		
Document Author	**Infrastructure security manager**		
Document owner	**Head of HR, Corporate Projects and IT**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**01/02/2004**	**Security manager**
	Version 2	**01/02/2016**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		