www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Remote Working Security Policy

February 2025

“Together we are One Team, proud to deliver for the Royal Borough”.

Our ‘HERO’ Values:

Humility

• Embrace the diversity of colleagues, partners, and the people of the borough
• Seek and listen to the ideas of others
• Ask for help when you need it
• Take pride in your work

Empower

• Support each other to learn, grow and improve
• Focus on wellbeing – your own and your colleagues
• Celebrate success
• Take ownership, be accountable, focus on outcomes
• Learn lessons and innovate to change what isn’t working
• Use your professional expertise to make key decisions

Respect

• Be open, honest and transparent
• If you can’t do something, let people know
• Engage in a variety of ways
• Don’t sit in silence if something concerns you
• Consult with people on decisions which impact them
• Treat people with respect

One Team

• Deliver our vision together
• Break down internal silos – put the people of the borough first
• Don’t pass people around the system
• Understand how what you do relates to our vision
• Build good relationships and get to know other teams

CONTENTS

Frequently used acronyms

IT	Information Technology
RBWM	Royal Borough of Windsor & Maidenhead

1 PURPOSE

1.1 The purpose of this Remote Working Security 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 This policy defines the security rules and responsibilities that apply when doing council work outside of council offices at any time (also known as remote working).

1.3 This policy recognises the increased risk to personal information and its complements but does not replace the council's procedures and guidelines regarding protecting council information which are covered separately in the **Information Handling Policy** and should be read in conjunction with this policy.

2 SCOPE

2.1 This Remote Working Security Policy aims to ensure that the integrity and security of the council's data and other resources remain protected.

2.2 This policy aims to protect information and data from residents, service users, and the council. The policy applies to any type of remote working, covering both the remote use of computing devices and paper documents.

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

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.

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:

4.2.1. Users accessing council IT facilities must comply with all council policies and procedures.

4.2.2. Managers and Team Leaders must ensure their staff comply with this policy and provide advice to them.

4.2.3. 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**.

4.2.4. IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed. Administer, control and monitor access to IT facilities and systems.

4.2.5. 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. The IT Support 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 Management Team in advance.

5.3 Non-Compliance

5.3.1. Any action that constitutes a breach of this policy will be treated seriously and may result in disciplinary action being taken in accordance with RBWM's disciplinary policy and procedure or other measures that is deemed appropriate by RBWM.

5.3.2. In circumstances where it is believed that a criminal offence has been

committed the matter may be reported to the Police.

6 RESPONSIBILITIES AND RISK

6.1 All users have a responsibility for the safety and security of council systems and information. This applies to working in the office/work environment as well as working out of the office.

6.2 All users have a responsibility for the safety and security of council computing equipment and information and are expected to exercise reasonable care whilst it is in their possession as covered in the **Care of Council Owned Equipment Policy** which should be read in conjunction with this policy.

6.3 Periodic audit and monitoring of information (either soft or hard e.g., documents) with users working remotely should be audited and monitored by requesting for proof of possession regularly.

6.4 Directors, Heads of Service, Service Leads and Managers will approve requests for remote working, and ensure staff are trained and aware of the Remote Working Security Policy rules.

6.5 All remote workers will submit an **Amend Access Service Request Form** for authorisation from their line managers to use of facilities and information while working remotely.

6.6 Remote workers will not utilise any council electronic equipment, software, or documents outside of council offices without authorisation from their manager.

6.7 Remote workers will:

6.7.1. comply with this policy.

6.7.2. provide access to council equipment or information requested by the council or its agents after a security breach or concern.

6.8 IT Services is responsible for:

6.8.1. providing secure remote working hardware and software, and

6.8.2. providing advice, IT support, and monitoring compliance.

6.9 Any of these services may be delegated to an approved IT support service.

7 PHYSICAL SECURITY

7.1 Before removing documents from council offices users must get approval from their council manager.

7.2 No user will take documents out of council offices unless they will be

used.

7.3 Everyone needs 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.

7.4 Where possible make sure that council computing devices are kept separate from other council documents or notebooks when working remotely.

7.5 Make sure that physical security tokens and portable computer media are always kept physically separated from related computing equipment.

7.6 Protect council IT equipment and documents outside of council offices. When not in use it must be kept out of sight and locked away.

7.7 When staying in hotels or other accommodation keep council computing equipment and paper-based information protected. Use complimentary hotel security facilities if available.

7.8 Any theft or loss of council computing equipment or information must be reported to:

7.8.1. The police and ensure a Police Theft Report has been raised and a crime reference Number obtained, see the **Thames Valley Police website**.

7.8.2. The council's mobile phone provider using the 24x7 emergency number found on their website if the loss is involving a phone. (Failure to report a stolen mobile phone could result in significant charges from the council's telecoms provider).

7.8.3. The employee's manager.

7.8.4. The IT Service Desk if equipment and accounts need to be de-activated.

7.8.5. The Information Governance Team by submitting a security incident when any critical information or personal data is involved.

8 UNAUTHORISED ACCESS

8.1 Remote workers are responsible for preventing unauthorised access to council equipment or information, whether electronically or on paper.

8.1.1. No family members or other unauthorised persons may be given access to council IT equipment, information, or documents.

8.1.2. Remote workers will accept responsibility for any access they have made to council IT services.

8.1.3. All users will protect their council logon user identifiers, passwords, access tokens, or other access mechanisms. Never share or disclose their council user identifier and password with anyone else.

8.1.4. Only in exceptional situations a shared (generic) user account may be authorised by the IT Service, on receipt of the appropriate authorisation request.

8.1.5. Access to council computing devices and systems are covered in detail in a separate policy, **IT Access Security Policy,** and should be read in conjunction with this policy.

8.1.6. Switch off or log off any IT equipment used remotely when it is not in use or left unattended.

9 STORAGE OF DATA AND USE OF EMAIL

9.1 Unless authorised by IT Service for reasons arising from exceptional circumstances, then:

9.1.1. All Council data must be stored on the council's cloud storage areas or network drives.

9.1.2. Management and IT Services authorisation must be obtained before any data is stored externally, e.g., stored on the Internet, on a portable electronic device, or on a local computer.

9.1.3. Council data must not be emailed to an external personal or business email address, unless there are exceptional circumstances.

9.1.4. Personal or sensitive data stored on a computing device outside the council's IT network must be encrypted and access to it protected by a strong password.

9.1.5. Remote workers must accept responsibility for use of any email accounts they have used to conduct council business.

10 PRINTING AND DOCUMENTATION

10.1 Remote workers will not:

10.1.1. print information outside council offices unless absolutely necessary.

10.1.2. leave printed council information where it can be read by others.

10.2 Paper documents containing personal or sensitive data must be disposed of by either:

10.2.1. using a cross-cut shredder, or

10.2.2. returning them to the office and using the council's confidential wastepaper disposal service.

11 TECHNICAL SECURITY

11.1 All users will use a fast, reliable home broadband connection that is set up securely to access the council IT network remotely and follow the **NCSC guidance for secure home working.**

11.2 Non-council computing equipment used for remote working will be protected by reputable anti-virus software receiving regular anti-virus definition updates.

11.3 All computing equipment should have device location tracking and remote access wipe capabilities enabled in case of theft.

11.4 Device screen locks after a period of inactivity must be enabled on all remote workers computing devices and there should be adherence to the Clean Desk and Clear Screen section of the Cyber Security Policy.

11.5 Periodic backup (Daily or weekly) of data on computing equipment for remote working must be done to avoid loss of the council's data.

11.6 Remote workers must not install or update any hardware, software or make other changes to council computing equipment. These changes will only be carried out by IT Services or authorised support staff.

11.7 If an incident of theft should occur while working remotely, the remote worker should ensure the incident is reported to the IT service desk in a timely manner to action a remote wipe of the council's information where applicable.

11.8 Remote workers will connect council computing equipment to the council's IT network monthly to ensure the acceptance of regular policy updates and to synchronise password changes.

11.9 If a user's computing device is not connected the council's IT network within a 28-day period, the connection is disabled. It will not be possible to connect it to the council's IT network without a support request being raised.

11.10 Access rights to remote work capabilities should be revoked and return of remote equipment should be made immediately to the Council upon termination of remote working activities.

11.11 If any user suspects a virus infection on council computing equipment,

they must switch-off the device and report it as soon as possible to the IT Service Desk. The user must also inform their manager and follow guidance in the **Reporting Security Incidents Policy**.

11.12 Failure to report a virus will be considered a serious breach of this policy.

12 REMOTE WORKING OUTSIDE OF THE UK

12.1 Any council IT network, system or mobile network accessed from outside the United Kingdom have significantly higher security risks.

12.2 Written authorisation must be obtained by the employee from their Line Manager, IT Security and the DPO.

12.3 Once approved to use our devices from outside the UK the user will be required to book an IT appointment to check devices for the latest updates. This appointment must be completed within the 2 weeks prior to leaving the UK to ensure devices have the latest updates.

12.4 Additional charges may be incurred, and service restrictions imposed.

12.5 Council personal data or sensitive information must not be accessed from outside the United Kingdom.

APPENDICES

RELATED STANDARDS, POLICIES AND PROCEDURES

- IT Access Security Policy
- Electronic Information - Asset Management Policy
- Reporting Security Incidents Policy
- Information Handling Policy
- Care of Council Owned Equipment Policy
- Terms and Conditions of Employment – this states that employees are required to follow the council's policies, procedures, and guidelines, including those for security.
- UK Data Protection Act 2018
- Information Security Management Standard ISO/IEC 27001:2013
- NIST SP800-63.3 standards.

Document Name	**Remote Working Security 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	**21/11/2012**	**Security manager**
	Version 2	**20/10/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
	Version 4	**06/06/2023**	**Infrastructure security manager**
	Version 5	**02/02/2025**	**Infrastructure security manager**
Circulation Restrictions			
Review Date	**01/03/2026**		