www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Remote Working Security Policy

April 2023

“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

1	PURPOSE	4
2	SCOPE	4
3	APPLICABILITY	4
4	AUTHORISATION	4
5	POLICY COMPLIANCE	5
6	RESPONSIBILITIES AND RISK	6
7	PHYSICAL SECURITY	6
8	UNAUTHORISED ACCESS	7
9	STORAGE OF DATA AND USE OF EMAIL	8
10	PRINTING AND DOCUMENTATION	8
11	TECHNICAL SECURITY	9
12	REMOTE WORKING OUTSIDE OF THE UK	9
13	TEMPORARILY WORKING ABROAD - NOTICE	10
APPENDICES		12
RELATED STANDARDS, POLICIES AND PROCEDURES		12

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:

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

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

4.2.2. 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**.

4.2.3. 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.

4.2.4. 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

5.1.0. All users must comply with this policy.

5.1.1. 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.

5.1.2. 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

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

5.3 Non-Compliance

5.3.0. 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 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 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.

6.4 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.

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

6.6 Remote workers will:

6.6.0. comply with this policy.

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

6.7 IT Services is responsible for:

6.7.0. providing secure remote working hardware and software, and

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

6.8 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:

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

7.8.1. 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).

7.8.2. The employee's manager.

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

7.8.4. 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.

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

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

8.1.2. 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.

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

8.1.4. 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.

8.1.5. 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:

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

9.1.1. 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.

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

9.1.3. 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.

9.1.4. 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:

10.1.0. print information outside council offices unless absolutely necessary.

10.1.1. 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:

10.2.0. using a cross-cut shredder, or

10.2.1. 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 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.

11.4 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.

11.5 If a user's computing device is not connected the council's IT network within a 60-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.

11.6 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**.

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

12 REMOTE WORKING OUTSIDE OF THE UK

12.1 Remote workers must not take, nor access, personal and sensitive information outside of the UK.

12.2 The council will not generally approve a permanent arrangement for an employee to work abroad, as it would require the council to obtain specialist legal advice.

12.3 Only in exceptional circumstances would temporary work outside of the UK be considered (a minimum of 4 weeks and a maximum of 3 months).

12.4 The remote worker must provide a clear business case and authorisation must be obtained from all of the following:

12.4.0. The remote workers Director or Head of Service,

12.4.1. Human Resources (HR),

12.4.2. Data Protection Officer (DPO), and

12.4.3. IT Services

12.5 The remote worker must allow sufficient time for the request to be reviewed by each of the services and for the approval process to be completed.

12.6 The remote worker must complete **Appendix A** with their manager and Head of Service and forward a copy to dpo@rbwm.gov.uk and security@rbwm.gov.uk

12.7 Read the council's **Cyber Security Policy** and **Care of Council Owned Equipment Policy**.

12.8 In addition, a service request should be raised with IT Services at https://support.rbwm.gov.uk/

12.9 If the service request (12.8) is approved, the remote worker must book a face-to-face appointment with IT Services before leaving the UK to ensure that the laptop is updated with all the latest security patches and anti-virus definitions.

12.10 If all of the above (12.4 - 12.9) were completed, then the use of the remote access portal will be permitted from outside the UK.

12.11 While working from abroad there will be no access to any Microsoft 365 services (including Teams calls) or any systems using the VPN.

13 TEMPORARILY WORKING ABROAD - NOTICE

13.1 While working from abroad there will be no access to any Microsoft 365 services (including Teams calls) or any systems using the VPN.

13.2 The device is a council asset and should only be used for work purposes by the assigned user.

13.3 Any loss or damage should be reported immediately to your manager, who should report the loss to the IT security team via the Security Incident Reporting Form and an email to security@rbwm.gov.uk.

13.4 The security of the device is the responsibility of the user. Any damage or loss will be reclaimed from the business area or user directly.

13.5 Be aware that you may incur additional charges for using a mobile device abroad. Tariffs vary depending on location, and you will be accountable for any additional expenses.

13.6 Any Wi-Fi connection used should be residential broadband and secured by a suitable passcode. Where possible, disable the online backup of photographs and messages, operating system upgrades, and application updates to minimise data usage on mobile devices.

13.7 The risk of malicious software is more prevalent when using Wi-Fi hotspots. Connecting to hotel or café Wi-Fi hotspots is not advised, as they can be prone to 'man-in-the-middle' attacks.

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	**26/04/2023**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/04/2024**		