www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

Royal Borough Windsor & Maidenhead

Cyber 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. This cyber security policy ensures that the applicable and relevant security controls are set in line with the Royal Borough of Windsor and Maidenhead requirements.

1.2. The cyber security policy outlines the council's guidelines and provisions for preserving the security of council data and technology infrastructure.

1.3. The use of computing equipment, human errors, hacker attacks and system malfunctions make council information vulnerable to severe security breaches and could cause great financial damage and may risk the council's reputation.

1.4. To mitigate these security risks this policy outlines several security measures.

2. SCOPE

2.1. The aim of the cyber security policy is to prepare Royal Borough of Windsor and Maidenhead to ensure that the correct processes and procedures, roles and responsibilities are in place and followed for any council cyber threat or incident while we continue our normal business operations.

2.2. Security incidents include any incident that occurs by accident or deliberately that may impact communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data, or services in the council. This includes unauthorised access to, or the use, disclosure, modification, or destruction of data or services used or provided by the council.

3. APPLICABILITY

3.1. This policy applies to all council employees and RBWM Councilors. 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 people should have access to council assets, systems and networks. 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.

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. 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 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. The IT access security rules and procedures are defined by the council to ensure its IT facilities, systems and data are protected against unauthorised access.

6.2. All persons authorised to access council IT facilities, systems or data must comply with these rules and procedures. Further guidance on IT access is covered in the **IT Access Security Policy** which can be found on the council website and must be read in conjunction with this policy. The policy applies to any person accessing council IT facilities or electronic data in any format, on any device, and from any location.

7. NEW STARTERS

7.1. All new staff at the council, Councilors, contractors, temporary, agency staff and others working in a similar capacity and volunteers and partner councils who do work for the council that use or have access to systems and/or information and hardware will be screened and checked before employment.

8. TRAINING

8.1. All users will complete a mandatory security awareness training session yearly which covers:

- Security awareness.
- Identify sensitive information.
- Securely handle sensitive information.
- Identify suspicious and phishing e-mails.

9. CONFIDENTIAL DATA

9.1. Confidential data is private and valuable. A few common examples are:

- Unpublished financial information.
- Data of customers/partners/vendors.
- Patents, formulas, or new technologies.
- Customer lists (with personal detail).

9.2. All users are obliged to protect confidential data. In this policy, the council will give users instructions on how to avoid security breaches.

10. PRIVILEGED ACCESS RIGHTS

10.1. Allocating privileged access rights should be restricted and managed through an approval process.

10.2. Each entity in need of privileged access rights should be identified using their unique identity and approved before allowing them to execute privileged activities.

10.3. Privileged access rights should only be allocated to users whose job role requires these rights.

10.4. Approval of privileged access rights should only be granted after proper verification has been concluded by the CISO or security manager.

10.5. Privileged access rights should not last for more than 24 – 48 hours at most and can be renewed following the due process.

10.6. Logging and authentication for users granted privileged access rights should become stricter during the period they have it.

10.7. Constant monitoring and review of the users account with privileged access rights should be done by the Security Manager.

10.8. The identities with privileged access rights should not be assigned to more than one person.

11. NETWORK SEGREGATION

11.1. Network segregation should be implemented to separate sensitive data and networks in the council to control the traffic between them.

12. PROTECTION OF DEVICES

12.1. When staff use their electronic devices to access any council application accounts, they introduce security risk to our data. The council advise all staff to keep both their personal and council-issued electronic devices secured.

12.2. Users can do this if they:

12.2.1. Keep all devices password protected and locked while not in use.

12.2.2. Ensure they do not leave any device exposed or unattended.

12.2.3. Only log into council accounts and systems through secure and private networks.

12.3. IT Services will ensure the following are on all council computing devices:

12.3.1. Antivirus software with the latest digital signatures available for download when devices connect to the council network.

12.3.2. Apply security updates and patches of browsers and systems monthly or as soon as updates or patches are available.

12.4. Users must avoid accessing internal systems and accounts from another person's device or lending their own devices to others.

12.5. When users access the council's systems either with council-issued equipment or their own equipment they must follow instructions to protect their accounts and devices as covered in the **IT Access Security Policy** and **Electronic Information Asset Management Policy** which can be found on the council's website in the Information security section.

13. IDENTITY MANAGEMENT

13.1. To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

13.2. All council personnel must be assigned a unique identity linked to them for non-repudiation to be upheld.

13.3. All identities of authorised users accessing the council's systems and data should be recorded and retained for every action to uphold non-repudiation.

13.4. For cases of shared identity between users, it must only be used for council business or operational purposes, and only after approval has been given by the CISO or security manager.

13.5. Identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight.

13.6. When an employee or contractor's role changes or terminates their association with the council, the old identity should be properly disabled and deleted, and all associated access rights with the identity should be revoked in a timely fashion.

13.7. No council personnel should have more than one identity assigned to them at any time.

13.8. Inventory of all identity authentication should be kept.

13.9. Management of each identity authorisation should be kept.

14. E-MAIL

14.1. Emails often host scams (phishing) and malicious software (worms).

14.2. To avoid virus infection or data theft, the council instruct all staff to:

14.2.1. Do not open attachments and clicking on links from unknown senders.

14.2.2. Do not open attachments and clicking on links from external senders unless it was an expected email.

14.2.3. Be very suspicious of clickbait titles (e.g., offering prizes, advice.)

14.2.4. Check email and names of people they received a message from to ensure they are legitimate.

14.2.5. Look for inconsistencies or signs (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

14.2.6. Any suspicious email will be referred to security@rbwm.gov.uk.

14.3. The policy for use of email is covered in **Use of Email Policy** and should be read in conjunction with this policy.

15. PASSWORD MANAGEMENT

15.1. Password leaks are dangerous since they can compromise the entire RBWM infrastructure.

15.2. Not only should passwords be secure, to prevent passwords to be easily hacked, but they should also remain secret.

15.3. Passwords are a line of defense for IT systems and, together with personal user identifiers and IT access codes, protect against unauthorised access.

15.4. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computing devices and systems and can compromise the council's entire infrastructure.

15.5. Username / user identifiers and passwords are covered in a separate policy Password Policy with further guidance on user identifiers and passwords and should be read in conjunction with this policy.

16. CLEAR DESK AND CLEAR SCREEN

16.1. Please refer to the Clear Desk Policy

17. DATA TRANSFERS

17.1. The Transferring data introduces security risks.

17.2. All users will:

17.2.1. Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless necessary. When mass transfer of such data is required, IT services must be informed.

17.2.2. Only share confidential data over the council network and not over public Wi- Fi or private connection.

17.2.3. Ensure that the recipients of the data are authorised people or organisations and have adequate security policies to handle council data.

17.2.4. Report suspicious emails, scams or phishing emails, privacy breaches and hacking attempts to security@rbwm.gov.uk.

17.3. IT services are responsible for advising staff on how to detect scam emails. The council encourage users to contact the team with any questions or concerns.

18. MONITORING ACTIVITIES

18.1. A centralized monitoring system should be set up using SIEM tools, IDS, IPS, EDR and XDR tools.

18.2. Event logs from the firewall, web filters, IPS, IDS and DLP tools should be closely monitored, and including the following:

18.2.1. All outbound and inbound network, system and application traffic should be closely monitored for abnormalities.

18.2.2. Every access to systems, servers, networking equipment, monitoring system, critical applications should be monitored.

18.2.3. Extra effort should be used in close monitoring of all sensitive information and/or admin level system and configuration files.

18.2.4. Any code being executed on the endpoint or network should be authorised and a non-compromise check thoroughly executed.

18.2.5. The usage of system resources including CPU, disk space, memory, bandwidth, etc., should be monitored.

19. ADDITIONAL SECURITY MEASURES

19.1. To reduce the likelihood of security breaches, all users will:

19.1.1. Turn off their screens and lock their devices when leaving their workspace.

19.1.2. Change all account passwords immediately when a device is stolen.

19.1.3. Report a perceived threat or possible security weakness in IT systems.

19.1.4. Refrain from downloading suspicious, unauthorised or illegal software on their council devices.

19.1.5. Avoid accessing suspicious websites.

19.2. All users will comply with the **IT Access Security Policy**, **Care of Council**

Owned Equipment Policy, **Use of Email Policy** and **Use Internet Policy** which can be found on the council's website in the Information security section.

19.3. IT Services will:

19.3.1. Install firewalls, anti-malware software and access authentication systems.

19.3.2. Arrange for security training for all staff.

19.3.3. Inform staff regularly about new scam emails or viruses and ways to combat them.

19.3.4. Investigate all security breaches thoroughly.

19.3.5. Follow this policy provisions as other staff do.

19.4. The council will implement physical and digital shields to protect information and systems.

20. REMOTE WORKING

20.1. All users working remotely must comply with this Cyber Security Policy.

20.2. Most employees working remotely will still access the council's network and systems and must ensure their private/home network is secure.

20.3. Guidelines and instructions for staff working remotely are covered in the Remote Working Security Policy and must be read in conjunction with this policy.

21. SECURITY INCIDENT

21.1. All employees must ensure a security incident is raised in response to IT security concerns or security breaches as covered in the **Reporting Security Incidents Policy** which can be found on the council's website in the Information security section.

21.2. Each security incident raised by the employees should be assessed by the help desk or the security manager to ensure effective categorization and prioritization of each incident raised.

22. RELATED POLICIES AND PROCEDURES

- Reporting Security Incidents Policy
- Remote Working Security Policy
- IT Access Security Policy
- Care of Council Owned Equipment Policy
- Use of Email Policy
- Use Internet Policy
- Care of Council Owned Equipment Policy

Document Name	**Cyber Security 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	**25/06/2020**	**Infrastructure security manager**
	Version 2	**21/07/2022**	**Infrastructure security manager**
	Version 3	**07/02/2025**	**Infrastructure security manager**
	Version 4		
Circulation Restrictions			
Review Date	**01/03/2026**		