www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Use of Internet 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 **Use of Internet 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 establishes a framework for the secure, effective, and appropriate use of Internet when conducting council business, or when representing the council.

1.3. This policy establishes the council's and user responsibilities for the Use of Internet.

2 SCOPE

2.1. The Use of Internet Policy ensures the Royal Borough of Windsor and Maidenhead implement the correct processes and procedures relating to the use of the internet.

2.2. The Use of Internet Policy aims to ensure that the integrity and security of the council's data and other resources remain protected.

2.3. The Royal Borough of Windsor and Maidenhead (the council) requires everyone using the internet when conducting council business to comply with this policy.

2.4. The purpose of this policy is to ensure the proper use the internet and make users aware of what the council deems as acceptable and unacceptable use of the internet.

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.

4.2.5. IT services ensure that privileged and systems administrator access is strictly controlled all applications we administer based upon a valid business justification and specific job requirements as approved by the user's line manager.

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 PURPOSE

6.1. The purpose of providing the internet service is primarily to give council employees and Councillors:

6.1.1. Access to information relevant to the council's business obligations.

6.1.2. The use of business applications and websites for council business.

6.1.3. The capability to post updates to council owned and/or maintained web sites.

6.1.4. The ability to purchase goods or services for the council electronically

7 RESPONSIBILITIES AND RISK

7.1. 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.

7.2. All use of the internet for council business must comply with the council's Use of Internet Policy and are under a general requirement to maintain confidentiality of information.

7.3. It is every user's responsibility to:

7.3.1. Assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.

7.3.2. Only use the council's internet facility within the terms described in this policy.

7.3.3. Understand this policy and comply with it, especially the limitations on internet use.

7.3.4. All users are responsible for the content and security of everything they send or receive on the Internet.

7.3.5. Report the misuse of the internet.

7.4. It is council managers and team leader's responsibility to ensure that the use of internet is:

7.4.1. Used appropriately and securely.

7.4.2. Within employees work time is relevant to and appropriate to the council's business and within the context of the user's responsibilities, and that personal internet use is limited.

7.4.3. Within an employee's own time is subject to the rules contained within this document.

7.5. When a manager suspects or has been made aware of the abuse of the use of the internet, a confidential email should be sent to the HR business partner team, explaining the concern and circumstances. Designated staff will investigate and provide evidence and audit trails of access to systems. IT services will comply with any legitimate requests from external authorised bodies.

7.6. IT services will investigate internet security breaches or incidents and provide advice. IT services (or authorised IT support services) will set up internet access rights for, and monitor internet use of, council internet facilities.

7.7. Audit and investigations service may be informed of investigations into suspected or actual breaches of this Use of Internet Policy. Advice will be provided to ensure the investigation is carried out appropriately and takes account of legal obligations.

7.8. The council will take all reasonable steps to ensure that all users are aware of policies, protocols, procedures, and legal obligations relating to the use of the internet. This will be done through training and staff communications at service and council-wide levels.

8 USE OF COUNCIL INTERNET ACCESS

8.1. When using the internet for council business users must identify themselves clearly.

8.2. Users must not send internet communications that hides their identity.

8.3. Council information must not be exported to non-council internet sites without written approval from the council manager responsible.

8.4. Users must be aware that messages sent or received via the internet may be lost or intercepted.

8.5. All users will send personal and sensitive information only to internet sites that are protected (i.e. with an Internet address starting 'https' and with a secure padlock symbol shown next to the https:// address).

8.6. If users think their computer has a virus infection, they will immediately unplug their computer from any IT networks and the internet. Any concerns, messages or warnings relating to viruses received when using council internet facilities must be referred to the council's IT service support desk, or to their approved IT support service.

8.7. Internet communications are not guaranteed to be safe.

8.8. Whilst doing work for the council, internet access may be used for the following:

8.8.1. Obtaining information or research.

8.8.2. Council electronic commerce (e.g. purchasing council equipment).

8.8.3. Communicating with residents and members of the public.

8.8.4. Professional networking and approved personal or professional development.

8.8.5. Appropriate use of social media networking sites for authorised business use only.

8.8.6. This list is not exhaustive and other exceptional authorised reasons may apply.

9 PERSONAL USE OF THE INTERNET

9.1. Access to the internet for personal use is generally confined to outside of normal working hours.

9.2. Personal use must still comply with this policy including its provisions regarding misuse.

9.3. Limited personal use of the internet during work time is permitted at the discretion of a council manager and provided it does not interfere with a user's work.

9.4. The purchase of personal goods or services is permitted using the council's internet facilities during non-work time.

9.5. For any online purchase of personal goods or services using the council's internet service the user will be responsible for ensuring that the information provided, clearly shows that the transaction is being entered by themselves personally and not on behalf of the council.

9.6. The council is not responsible for any personal transactions entered into and users must accept responsibility for, and keep the council protected against any claims, damages, losses or the like which might arise from online transactions using the council's internet facilities.

9.7. All personal goods and services purchased should be delivered to a home or other private address and not delivered to council property.

9.8. All personal usage must be in accordance with this policy. Your computer used for council business and any data held on it may be accessed at any time by the council to ensure compliance with all its statutory, regulatory, and internal policy requirements.

9.9. If users are in any doubt about how they may make personal use of the council's internet service, they should consult their manager.

10 INAPPROPRIATE INTERNET USAGE

10.1. Except where it is strictly and necessarily required for council business and authorised by management, users will not use the council's internet for the following:

10.1.1. Create, download, upload, display, or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene, or offensive.

10.1.2. Use foul or offensive language or make defamatory or derogatory remarks.

10.1.3. Represent personal opinions as those of the council or impersonate or misrepresent others.

10.1.4. Run a private business.

10.1.5. Subscribe to, enter, or use peer-to-peer networks or install software that allows illegal sharing of music, video or image files.

10.1.6. Subscribe to, enter, or utilise real time chat facilities such as chat rooms.

10.1.7. Subscribe to, enter, or utilise online gaming or betting sites.

10.1.8. Subscribe to or enter "money making" sites or use "money making" programs.

10.1.9. Access to "unsuitable" material.

10.2. The list in 10.1 is neither exclusive nor exhaustive.

10.3. Access to inappropriate internet sites or unsuitable material is prohibited and the consequence of accessing these sites and material can have serious security impact on our IT infrastructure.

10.4. Members of the public, and others doing council work, using council internet facilities are protected by having access to certain categories of webs content blocked.

10.5. Access to the following categories of web content are currently blocked:

10.5.1. Illegal.

10.5.2. Pornographic.

10.5.3. Violence.

10.5.4. Hate and discrimination.

10.5.5. Offensive.

10.5.6. Weapons.

10.5.7. Hacking.

10.5.8. Web chat.

10.5.9. Gambling.

10.5.10. Dating.

10.5.11. Radio stations.

10.5.12. Games.

10.6. Blocked categories are not restricted to the list in 10.5.

10.7. If a user unintentionally accessed an inappropriate internet site or unsuitable material it must be reported to **security@rbwm.gov.uk**.

10.8. To gain access to any blocked categories of information using council internet facilities, requires authorisation from the user's manager by completing the **Exceptional Internet Access Form**.

11 DOWNLOAD SOFTWARE OR DATA

11.1. Users must not download software without authorisation from IT services.

11.2. Internet downloading is only permitted in controlled circumstances as the internet is a primary source of virus infection.

11.3. When authorised to download software or data these downloads should only be done through secure website.

11.4. If software needs to be downloaded from the Internet onto council IT equipment, please submit an **IT Access Request Form**.

11.5. Users should avoid infringement of copyright when downloading software.

11.6. If in doubt check with IT services support desk before any software or data is downloaded through the internet.

12 SECURITY AND MONITORING

12.1. Internet access and security using council internet facilities will be monitored.

12.2. The council has a responsibility to ensure that use of its internet facilities complies with legislation and statutory guidance.

12.3. All access is recorded, logged, and may be used for the purposes of:

12.3.1. Monitoring total usage to ensure business use is not impacted by lack of capacity,

12.3.2. Monitoring access to websites and appropriate usage.

12.4. All computing devices and any data held on it are the council's property and may be accessed at any time by IT support to ensure compliance with all the council's statutory, regulatory, and internal policy requirements.

12.5. Users are provided with a network username and password for secure access and it is their responsibility to protect their login detail. Users will be held responsible for any internet activity during their login session.

12.6. All access is recorded, logged, and reviewed for the purposes of monitoring total usage to ensure business use is not impacted by lack of capacity and ensuing only appropriate use is made of the facility.

12.7. The internet filtering system monitors and records all access for reports that can be produced for IT management and auditors.

13 MISUSE OF THE INTERNET

13.1. All users are responsible to report council internet misuse or any council internet usage that conflicts with this policy or with the **Equal Opportunities policy**.

13.2. Users must report any misuse or policy conflict to their council manager and submit a council **Security Incident Report** as soon as possible. This is covered in more detail in the **Reporting Security Incidents Policy** which can be found on the council's web site.

Document Name	**Use of Internet 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	**21/11/2012**	**Security manager**
	Version 2	**20/10/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		