www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Use of Email 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 Email 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 is to ensure the proper use the council's email system and make users aware of what the council deems as acceptable and unacceptable use of its email system.

1.3 The Use of Email Policy applies to all business functions and information of the email system and relevant people who support the system. This document sets out the council's policy for the protection of the confidentiality, integrity, and availability of the email system.

1.4 This policy establishes a framework for the secure, effective, and appropriate use of email when conducting council business, or when representing the council.

1.5 This policy establishes the council's and user responsibilities for the email system.

1.6 Compliance will reduce the risk of unauthorised loss or disclosure of information.

2 SCOPE

2.1 The use of email policy aims to ensure that the integrity and security of the council's data and other resources remain protected.

2.2 The Royal Borough of Windsor and Maidenhead (the council) requires everyone authorised to send emails when conducting council business to comply with this policy and follow email good practices.

2.3 In scope for this policy all email messages and attachments prepared and sent when conducting council business including:

2.3.1. all council email accounts

2.3.2. business, private, or personal email accounts

2.3.3. emails created using council electronic forms or websites.

2.4 The objective of this email policy is to ensure the security of the council's email system and the council will:

2.4.1. **Ensure Availability**

- Ensure that the email system is available for users.

2.4.2. **Preserve Integrity**

- Protect the email system from unauthorised or accidental modification ensuring the accuracy and completeness of the council's assets.

2.4.3. **Preserve Confidentiality**

- Protect assets against unauthorised disclosure.

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. 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 RESPONSIBILITIES

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 Senders of email on behalf of the council – must comply with the council's email policy and are under a general requirement to maintain confidentiality of information.

6.3 Managers and team leaders– must ensure members of staff or those doing work for the council comply with the policy.

6.4 The IT service will set up council email accounts and provide expertise during investigation or monitoring of council email account usage.

6.5 Audit and investigations service may be informed of investigations into suspected or actual breaches of this email policy. Advice will be provided to ensure investigation is carried out appropriately and takes account of legal obligations.

6.6 The infrastructure security manager will authorise exceptional access to email accounts.

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

6.8 When a manager suspects or has been made aware of the abuse of the council's email facilities, a confidential email should be sent to the HR business partner team explaining the concern and circumstances.

6.9 Designated staff will then investigate and provide evidence and audit trails of access to systems. The IT service will also comply with any such legitimate requests from external authorised bodies.

6.10 All email accounts maintained on our email systems are property of the Council.

7 LEGAL RISKS

7.1 Email is a business communication tool and users are obliged to use this tool in a responsible, effective, and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply.

7.2 It is important that users are aware of the legal risks of email:

7.2.1. If a user sends or forwards an email with any unfounded, insulting, offensive, harassing, racist, obscene, pornographic remarks or depictions, or does not comply with the council's Equality Policy, the user and the council can be held liable. Examples of inappropriate email content include (but are not limited to) the creation or transmission of:

- Any offensive, obscene, or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- Council personal or sensitive material that has not been authorised for release
- Material that infringes copyright, including intellectual property rights.
- Information that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Defamatory or other material which might bring the council into disrepute.

7.2.2. Any person who is unclear about the appropriateness of email content should consult their manager before sending it.

7.2.3. If a user unlawfully forwards confidential information, the user and the council can be held liable.

7.2.4. If a user sends or forwards an attachment that contains a virus, the user and the council can be held liable.

7.2.5. Email should not be used for permanent storage of documents and records that need to be retained for legal/statutory reasons.

8 ACCESS TO EMAIL SYSTEM

8.1 Employees wishing to use a council email account must submit a request for access by completing the appropriate **Request / Amend Access Form.** A line-manager or team leader must approve the request.

8.2 Users, or their line managers, must notify the IT service help desk of any change in status which may affect their right to use council IT facilities.

8.3 The **Request / Amend Access Process** extends from the initial registration of New Employee to the final de-registration of **Leavers** who no longer require access.

8.4 Authorised users of email for council business will:

8.4.1. be referred to this email policy from the staff handbook and so be informed about the provisions for monitoring and investigating email usage.

8.4.2. be issued with a council email address or addresses if required.

8.4.3. assist during investigations on information gathered about their use of a council email account into allegations or instances of email misuse.

9 ACCESS TO AN EMAIL ACCOUNT FOR BUSINESS PURPOSES

9.1 Access to another employee's email is normally forbidden unless the employee has given their consent (eg by setting delegated authority to access their emails).

9.2 If an email account needs to be accessed by another person for specific business purposes whilst they are absent, then a formal request must be made by submitting an **Exceptional Access to Another Email Account** request.

9.3 If approved, any such access must be completely necessary and carried out with full regard to the rights of the person being investigated.

10 EXCEPTIONAL EMAIL ACCESS

10.1 Obtaining access to another employee's email is normally forbidden unless it's for business purposes and the employee has given their consent (e.g. by setting delegated authority to access their emails) and by submitting an **Exceptional Access to Another Email Account** request.

10.2 If an email account needs to be accessed by another person for specific business purposes whilst they are absent, then a formal request must be made by submitting an **Exceptional Access to Another Email Account** request.

10.3 If approved any such access must be completely necessary and carried out with full regard to the rights of the person being investigated.

11 LEGAL REQUIREMENTS

11.1 The legal status of an email message is like other forms of written or electronic communication. Every email message sent to conduct, or support council business is an official communication from the council.

11.2 Whilst respecting the privacy of authorised email users, the council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act

2000, to monitor and audit the use of council email accounts. Interception or monitoring will be in accordance with the provisions of that Act.

11.3 Email and attachments may need to be disclosed under the UK Data Protection Act, the Freedom of Information Act or Environmental Information Regulations.

11.4 Only approved email accounts may be used to conduct council business.

11.5 All emails sent on behalf of the council must be clearly identified and contain the sender's name. They must never be sent anonymously.

11.6 The following rules are required by law and are to be strictly adhered to:

11.6.1. It is strictly prohibited to send or forward emails containing unfounded, insulting, offensive, harassing, racist, pornographic remarks or depictions, or does not comply with the council's Equality Policy. If you receive an email of this nature, you must promptly notify your line manager.

11.6.2. Do not forward a confidential message without acquiring permission from the sender first.

11.6.3. Do not send unsolicited email messages.

11.6.4. Do not forge or attempt to forge email messages.

11.6.5. Do not send email messages using another person's email account.

11.6.6. Do not breach copyright or licensing laws when composing or forwarding emails and email attachments.

12 UNSOLICITED EMAILS

12.1 If any phishing emails, junk emails, 'spam' or unsolicited emails are received they must be deleted without reading them.

12.2 The recipient must not reply to these emails, nor open any attachments; nor click on any hypertext links within the email.

12.3 Those using email when conducting council business must take precautions to reduce the risk of virus and malware infection.

12.4 Computer viruses are easily transmitted via email and from websites and internet downloads.

12.5 All users must take these security precautions to reduce the risks:

12.5.1. Ensure your computing devices receive the latest anti-virus updates.

12.5.2. Do not send email file attachments which are known to be infected with a virus.

12.5.3. Do not download data or programs of any nature from unknown sources.

12.5.4. Report concerns about suspect emails or attachments, or suspected virus attacks, to the council's IT service support desk or approved IT support provider.

13 PERSONAL USE

13.1 The council's email system is meant for business use only. Council email accounts must not be used to conduct personal business or to run a private business.

13.2 In exceptional circumstances, the Council may authorise the use of email for personal use, however the following guidelines will be adhered to:

13.2.1. Personal use of email should not interfere with work.

13.2.2. Personal emails must also adhere to the guidelines in this policy.

13.2.3. Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly.

13.2.4. The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.

13.3 Emails sent when conducting council business become part of the council's corporate record, even if sent from private business or personal email accounts.

13.4 In exceptional circumstances the use of private business or personal email accounts for council business may be authorised and a security declaration signed to acknowledge the increased risk and agreement to take additional precautions.

13.5 All users sending emails (of whatever sort) whilst conducting council business must acknowledge their legal responsibilities.

13.6 Any user using their personal email account for council business must acknowledge their Data Protection Act and Freedom of Information obligations.

14 SENSITIVE PERSONAL INFORMATION

14.1 The council encrypts data between council email accounts to approved standards.

14.2 The council's email system can be used for sending sensitive personal information internally.

14.3 Information sent from a council email account to email accounts that are not part of the council's email are not encrypted.

14.4 Personal and sensitive information should not be sent unless protected by encryption or some other means, e.g. by using an encrypted email service, or by alternative protection.

15 SYSTEM MONITORING

15.1 All email traffic is monitored for viruses. All email traffic (incoming and outgoing) is logged automatically. The logs do not include email content. These logs are audited periodically.

15.2 The content of emails is not routinely monitored. However, the council reserves the right to retain message content as required to meet legal and statutory obligations.

15.3 If there is evidence that users not adhering to the guidelines set out in this policy, any breach 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.

16 MONITORING OF COUNCIL EMAIL ACCOUNTS

16.1 Council email accounts are monitored and recorded centrally. This is carried out under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

16.2 All incoming and outgoing email traffic across the council IT network may be monitored by authorised staff in IT services, or audit and investigations, in order to:

16.2.1. Manage council email services and ensure efficient email performance.

16.2.2. Ensure that users act only in accordance with policies and procedures.

16.2.3. Prevent and detect any crime.

16.2.4. Investigate or detect unauthorised use of email.

16.2.5. Determining if emails relate to a private business or are of a private nature.

17 MONITORING BUSINESS, PRIVATE OR PERSONAL EMAIL ACCOUNTS

17.1 Personal email accounts should not be used for conducting council business.

17.2 The council does not directly monitor these personal accounts but may request access to these emails when it is suspected to provide a record of council business. The council may also be required to respond to Freedom of Information requests.

17.3 Note however that these accounts may be monitored by the law enforcement agencies in appropriate circumstances.

18 INSTANCES OF EMAIL MISUSE

18.1 When a manager suspects or has been made aware of the abuse of the council's email facilities, a confidential email should be sent to the HR business partner team explaining the concern and circumstances.

18.2 IT services or designated persons investigating the abuse of the council's email facilities may access the suspected users email account to gather evidence. IT services will also comply with any such legitimate requests from external authorised bodies.

18.3 In more serious situations where an allegation has been made or suspected serious breach of the policy has occurred then a formal request must be made to the council's Senior Information Risk Officer, by submitting an **Exceptional Access to Another Email Account** request.

18.4 The head of audit and investigations must be informed of any suspected or actual breaches of email policy before any subsequent investigation begins to ensure that it is carried out in accordance with good practice.

Document Name	**Use of email policy**		
Document Author	**Infrastructure security manager**		
Document owner	**Head of HR, corporate projects and IT services**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**21/11/2012**	**Security manager**
	Version 2	**25/10/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		