ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk Royal Borough of Windsor & Maidenhead

SECURITY POLICY

USE OF EMAIL

Introduction

This policy establishes a framework for the secure, effective and appropriate use of email when conducting council business, or when representing the council. Compliance will reduce the risk of unauthorised loss or disclosure of information.

Policy Statement

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.

Users of email when working for the council must comply with their responsibilities under Data Protection Act legislation to maintain the confidentiality of personal data.

Scope of Policy

All email messages and attachments prepared and sent when conducting council business including:

a) Council email accounts, i.e. those that end in @rbwm.gov.uk @rbwm.org or @rbwm.gcsx.gov.uk
b) business, private or personal email accounts
c) emails created using council electronic forms or websites.

Not covered by this Policy

Instant messaging, SMS text and other communications, e.g. Twitter, WhatsApp, Skype. These are covered by the Social Media Policy.

Those Affected by the Policy

This policy applies to anyone performing council duties or providing services. This includes Councillors; employees: other organisations conducting council business; agency workers; contractual third parties and agents of the council.

Roles and Responsibilities

1. 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.
2. Council Managers and Team Leaders– must ensure members of staff or those doing work for the council comply with the policy.
3. The IT Service – will set up council email accounts and provide expertise during investigation or monitoring of council email account usage.
4. 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.
5. Senior Information Risk Officer – authorise exceptional access to email accounts.

Policy Compliance

This policy must be complied with. Inappropriate or unauthorised use of email when conducting council business or representing the council will be regarded as a serious disciplinary or contractual issue. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand this policy, or how it may apply to you, get advice from your council manager, the council's Data Protection Officer, or the Information Governance Team.

Applying the Policy

Rule 1 Only approved email accounts may be used to conduct council business. All emails sent on behalf of the council must be clearly identified and contain the sender's name. They must never be sent anonymously.

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

Rule 1b Council email accounts must not be used to conduct personal business or to run a private business.

Rule 2 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.

Rule 3 All those sending emails (of whatever sort) whilst conducting council business must acknowledge their legal responsibilities.

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

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

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.

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

Rule 4 Personal and sensitive information should not be sent unless protected by encryption or some other means, e.g. by using GCSx email, an encrypted email service, or by alternative protection.

The reason is that emails sent over the Internet are at higher risk of interception or loss.

Rule 5 Authorised users of email for council business have these rights:

a) To be issued with the email policy and so be informed about the provisions for monitoring and investigating email usage.
b) To be issued with a council email address or addresses if required
c) To obtain a copy of any information gathered about their use of a council email account during investigations into allegations or instances of email misuse.

Rule 6 Under no circumstances should users communicate material which might be deemed inappropriate or offensive using email.

Any person who is unclear about the appropriateness of email content should consult the council manager who is responsible for their work before sending it.

This includes information that is illegal, defamatory, obscene, or does not comply with the council's Comprehensive Equality Policy.

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.

Rule 7 If any junk email, 'spam' or unsolicited emails are received they must be deleted without reading them. The recipient must not reply to these emails; nor open any attachments; nor click on any hypertext links within the email.

Rule 8 All GCSx encrypted emails must have a security marking in accordance with the Government's Security Policy Framework.

Every GCSx email sent must contain a security classification at the start of the email subject line to define how it must be protected.

Rule 9 Email should not be used for permanent storage of documents and records that need to be retained for legal/statutory reasons.

Rule 10 Those using email when conducting council business must take precautions to reduce the risk of virus and malware infection.

Computer viruses are easily transmitted via email and from websites and internet downloads. You must take these security precautions to reduce the risks:

- Ensure you have a reputable virus checker running on your computer and that it receives the latest anti-virus updates immediately.
- Do not send email file attachments which are known to be infected with a virus.
- Do not download data or programs of any nature from unknown sources.
- Report concerns about suspect emails or attachments, or suspected virus attacks, to the council's IT Service Desk or approved IT support provider.

Applying the Policy – Monitoring of Council Email Accounts

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

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:

- Manage council email services and ensure efficient email performance.
- Ensure that users act only in accordance with policies and procedures.
- Prevent and detect any crime.
- Investigate or detect unauthorised use of email.
- Determining if emails relate to a private business or are of a private nature.

Applying the Policy – Monitoring Business, Private or Personal Email Accounts
The council does not directly monitor these accounts, but may request access to these emails because they provide a record of council business. They may also be required to respond to Freedom of Information requests.
Note however that these accounts may be monitored by the law enforcement agencies in appropriate circumstances.

Applying the Policy – Exceptional Email Access
Procedure 1 Report a Concern about Email Use
Where a manager suspects that the email facilities are being abused, a confidential email should be sent to the Head of IT explaining the concern and circumstances. Designated staff can 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.

Procedure 2 Obtain Access to an Email Account for Business Purposes
Access to another employee's email is normally forbidden unless the employee has given their consent (e.g. by setting delegated authority to access their emails).

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 Email Access Request.

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

Procedure 3 Investigate Allegations or Instances of Email Misuse
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, using the Exceptional Email Access Request process. 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.

Procedure 4 How to Request a Council Email Account
Members of staff who require access to email will normally be issued with a council email account when they start work. If access to other email accounts is required, it can be obtained by completing an e-form. The set-up procedures are:
1. To request access to a shared operational email account, the line manager must submit an IT Access Request e-form
2. To request a new GCSx encrypted email account a GCSx email request e-form must be submitted.

Related Policies and Other Documents
Social Media Policy Storage of Information Policy
Retention and Disposal Policy

Related Legal and Regulatory Obligations
UK Data Protection Act
Information Commissioner guidance on FOI access to private email accounts
Government Security Policy Framework

Definitions

Council email accounts – email accounts allocated and set up by the council, i.e. those that end in @rbwm.gov.uk @rbwm.org or @rbwm.gcsx.gov.uk.

GCSx email – a higher security email account that is protected and can send or receive emails from the central Government IT network.

Personal business - any activity that is social or personal and not related to council business

Private business – any activity pertaining to the running of a private business, whether for profit or not for profit.