Member Internet & Email Acceptable Use Policy

By providing Members with access to IT systems, Rossendale Borough Council (RBC) has a number of responsibilities to ensure the protection of our commercial interests and reputation, as well as safeguarding Members against the possibility of misuse and infringement of their personal privacy. As an RBC Member and user of the corporate IT systems, Members also have a legal responsibility to understand and comply with the requirements that RBC have put in place around IT access.

In providing clear guidance and instructions, Members and the organisation are provided with protection against abuse. This document outlines and explains the responsibilities of Members and the implications of misuse, taking into account personal privacy, General Data Protection Regulation, Data Protection Act 2018, system monitoring and the cost of system misuse. Please take time to read and understand this policy.

Chief Executive

Summary

To promote improved system awareness, to encourage innovation and develop a culture where IT systems are a useful and integral part of our daily lives, Internet and e-mail access has been provided to many people within RBC. Members with Internet and/or e-mail access must understand the activities that are permissible and those activities which are not allowed and therefore potentially subject to disciplinary action.

Where Members fail to comply with the instructions identified in this policy will be subject to disciplinary action and serious breaches will be considered as gross misconduct and could lead to referral to standards.

Members should ensure they fully understand this policy and their responsibilities. Where further clarification is required, Members are advised to speak to Democratic Services.

Please ensure all RBC equipment is secure and locked whenever not in use.

RBC E-Mail Services

RBC tolerates limited personal use of its corporate email facility, provided non-business related e-mails are kept short, and there is no interference with the Members day to day roles and responsibilities. Please remember that's emails could be the subject of litigation and court action. They could been be seen by others and could form part of a data subject access request.

Email access is provided by RBC as a privilege. Any abuse or misuse of this facility could result in the termination of these services. This decision will be made and communicated by respective Group Leader & Chief Executive where appropriate.

The following activities are prohibited at all times:-

- Creating, sending or forwarding e-mail that includes profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially or sexually), offensive, subversive, violent or other illegal material.
- Creating or forwarding any e-mail that:
  - is a chain letter
  - contains jokes or other inappropriate material
  - is for personal gain or profit
  - represents a personal opinion as being that of RBC
- Forwarding any non-business related e-mail attachments received from an external source.
- Forwarding confidential or sensitive RBC information to a personal or Web Mail account.
- All PSN emails should be sent using via the Egress secure email system.
- If you receive an email from someone, you do not know or if it from a suspicious email address, do not open it as it could contain a virus – Inform Democratic Services & IT.

The above list is not exhaustive by any accounts.

Downloading and Using Information

While RBC tolerates limited personal use of its IT facilities, Members should use them responsibly, and be mindful that network, server and printing facilities at our locations have been sized for business use only. Members must also be aware that information found on the Internet may be copyrighted and therefore be legally protected from copying or distribution.

The following activities are prohibited at all times:-

- Downloading or copying copyrighted information, including materials such as music, films and computer software.
- Copying software without authorisation or where this breaches license agreements or import or export regulations.
- Downloading and/or saving inappropriate or illegal material from websites onto the network, hard or temporary drives/disks. This includes removable storage devices.
- Encrypting or password protecting information held within the RBC network (including the e-mail system) with non-standard and unsupported encryption tools and products.
- Using e-mail services within RBC to circulate downloaded information that is illegal, inappropriate or not business related.

Rossendale
BOROUGH COUNCIL

Internet Access Using RBC Facilities

Internet access is provided by RBC as a privilege. Any abuse or misuse of this facility could result in the termination of these services. This decision will be by respective Group Leader & Chief Executive where appropriate.

The following activities are prohibited at all times:-

- Accessing/viewing, printing or downloading any profane, obscene, indecent, pornographic, defamatory, inflammatory, threatening, discriminatory, harassing (racially or sexually), offensive, subversive, violent or other illegal material.
- Using Internet-based services to share copyrighted materials, such as music, films and computer software.
- Downloading or playing online computer games.
- Online gambling or making financial transactions.
- Accessing/using Instant Messaging services.
- Accessing or posting content to online chat rooms or bulletin boards.
- Soliciting for, or pursuing personal gain or profit.
- Circumventing RBC security controls to access unauthorised Internet or e-mail services.
- Accessing Web Mail services.
- Any illegal activities.
- Accessing any social message unless you are an approved social media user.

The above list is not exhaustive by any accounts. RBC will not be held liable for any fraudulent use of credit card information that a Member submits over the Internet.

RBC may decide to block access to certain websites it considers high risk or inappropriate.

Monitoring of System Usage

Monitoring and investigation processes have been established within RBC to ensure compliance with this policy. These processes protect the commercial interests and reputation of RBC and also safeguard Members against potential misuse and their rights to personal privacy.

In monitoring Internet access, RBC can identify the length of time the Internet is accessed, the content and websites accessed and what information is downloaded. The aim of monitoring is to identify possible areas of misuse.

Monitoring of other system usage will be managed through normal managerial control during the normal working day. Therefore, there will be no direct system monitoring of activity. However, respective Group Leader in conjunction with Chief Executive can request individual system investigations where they suspect possible system misuse. Investigations may include analysis of Internet use, access to individual e-mail addresses and or saved network information. All Email activity may be monitored.

Business Use

The data generated and stored within RBC's network and systems includes customer, employee and commercially sensitive information and understand that our systems contain information protected by GDPR, DPA 2018.

To ensure RBC complies with legal and regulatory requirements, Members must ensure that:-

- RBC information and data is treated as confidential or sensitive.
- Employee or customer related data held electronically is stored and retained in a secure and appropriate manner.
- Document retention and storage mechanisms, should be used where these are available.
- Comments posted by email or to any other system will not necessarily be considered as formal statements issued by, or the official position of, the Council and should not be phrased as such.
- The confidentiality or sensitivity of customer, employee or business related information is not jeopardised by it being included in e-mail communication.

Remote Access

Members using remote access to RBC managed IT services (including Internet and e-mail) must adhere to the requirements outlined in this, and other relevant policy documents. To minimise the risk of inappropriate use, monitoring and investigation processes will also apply to the remote access service.

System Security

All Members are individually responsible for the security of all of their respective RBC equipment including computers, smartphone, usb sticks, etc and including the information, reports and any data they hold.

Any System passwords must not be shared with colleagues, friends or family members.

Member Agreement

I have received a copy of Rossendale Borough Council's Corporate Policy Guideline on Internet and email acceptable use. I agree to abide by all the terms and conditions set out in the above policy.

Print Name: .....

Signed ..... Date .....