Rossendale BOROUGH COUNCIL

Subject:	Adoption of RBC Members' Social Media Policy, Internet & Email Acceptable Use Policy & Mobile Phone Policy	Status:	For Publication		
Report to:	Cabinet	Date:	3rd July 2019		
Report of:	Andrew Buckle	Portfolio Holder:	Resources		
Key Decision:	☒ Forward Plan ☒	General Exception ☐		Special Urgency ☐	
Equality Impact Assessment:		Required:	**Yes**	Attached:	**Yes**
Biodiversity Impact Assessment		Required:	**No**	Attached:	**No**
Contact Officer:	Andrew Buckle	Telephone:	**07854026590**		
Email:	**andrewbuckle@rossendalebc.gov.uk**				

1.	**RECOMMENDATIONS**
1.1	The Cabinet approve the RBC Members' Social Media, revised Internet & Email Acceptable Use and Mobile Phone Policies.
1.2	All future minor amendments to the RBC Members Social Media, Internet & Email Acceptable Use and Mobile Phone Policies are to be delegated to the Head of Customer Services & ICT Officer in consultation with the Portfolio Holder.

2. PURPOSE OF REPORT

2.1 The General Data Protection Regulation (GDPR) EU 2016/679 and Data Protection Act were implemented in 2018. In-order to ensure compliance with the new and revised legislation, Council policies around Social Media, Email & Internet Acceptable Use and Mobile Phone policies have to be amended to meet the new criteria imposed with the legislation.

3. CORPORATE PRIORITIES

3.1 The matters discussed in this report impact directly on the following corporate priority:

- **A proud, healthy and vibrant Rossendale:** our priority is to ensure that we are creating and maintaining a healthy and vibrant place for people to live and visit.
- **A clean and green Rossendale:** our priority is to keep Rossendale clean and green for all of Rossendale's residents and visitors, and to take available opportunities to recycle and use energy from renewable sources more efficiently.
- **A connected and successful Rossendale that welcomes sustainable growth:** our priority is to ensure that we are well connected to our residents, key partners and stakeholders. We want to make the most of every pound we spend and we are always looking for new and innovative ways to make the resources we do have, work harder for us.

4. RISK ASSESSMENT IMPLICATIONS

4.1 Failure to adopt the new and revised policies could result in the following:

Non-compliance with the GDPR and DPA 2018 resulting in a Data breach and loss of personal data.

Loss of reputation and a potential fine following Data breach.

Increased costs with misuse of RBC mobile phones.

5. BACKGROUND AND OPTIONS

5.1 The GDPR EU 2016/679 and DPA were implemented in 2018. The new GDPR and revised DPA Acts increase the responsibility of organisations when managing, storing and disclosing personal data. As well as introducing a financial penalty for instances of non-conformance resulting in Data breaches.

The legislation is mandatory and the Council has completed a considerable amount of work complying with the new legislation. This has included all service areas performing Information audits, Privacy Statements have been developed both from respective service areas and corporately.

5.2 The revised policies incorporate best practise and provide useful advice and guidance to Members around ensuring that both the requirements of GDPR and DPA are met.

As well as ensuring that the organisation has in place the necessary Protective Measures, which have been reviewed and approved by the Council as appropriate to protect against a Data Loss Event having taken account of the:
(i) nature of the data to be protected;
(ii) harm that might result from a Data Loss Event;
(iii) state of technological development; and
(iv) cost of implementing any measures;

5.3 Rossendale will apply organisational and technical controls such as network and system specific security, physical security, user access privileges, user passwords including but not limited to the following to ensure that:

Irrespective of whether Personal Data is at rest or in transit, the controls deployed are appropriate to the harm, which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage taking account of the nature and sensitivity of Personal Data.

Physical measures provide effective protection for information, systems and services from unauthorised access, theft, interference or damage.

Procedures are in place to identify and resolve software and system faults and failures, including the identification of malicious software.

Access to Personal Data is role based for legitimate business purposes in accordance with the "need to know" principle and that user permissions are controlled, granted, and removed in line with job responsibilities.
Sufficiently complex password controls are implemented for all authorised personnel with role based access to Personal Data.

Passwords, usernames and access codes are not disclosed to any other person (whether employed by the Provider or not) and that all passwords and security codes are kept securely.

COMMENTS FROM STATUTORY OFFICERS:
6. SECTION 151 OFFICER
6.1 There are no financial implications.

7. MONITORING OFFICER
7.1 All legal implications are covered in the body of the report.

8. POLICY IMPLICATIONS AND CONSULTATION CARRIED OUT

8.1 The policies ensures the Council meets its responsibilities under GDPR EU 2016/679 and the DPA 2018 and complies with the Equality Act 2010.

8.2 The policy was reviewed by the Overview and Scrutiny Committee in March 2019 and it was recommended that Cabinet approve the Policies.

9. CONCLUSION

9.1 The policies ensure the Council fulfils its duties under both GDPR EU 2016/679 and the DPA 2018 and is needed to ensure it has a legally robust approach complying with all legislation and good practice.

Background Papers	
Document	Place of Inspection
RBC Members' Social Media Policy	Appendix 1
RBC Members' Internet & Email Acceptable Use Policy	Appendix 2
RBC Members' Mobile Phone Policy	Appendix 3
Initial Equality Impact Assessment	Appendix 4

Rossendale Borough Council Members Social Media / Networking Policy

Jan 2019

Other formats are available.
Please call 01706 217777 or
visit our One Stop Shop at
Futures Park, Bacup.
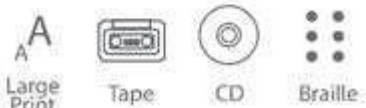
Responsible Section/Team	ICT	Page Number	1
Responsible Author	Andrew Buckle	Date Agreed / Agreed At	
Date Last Amended	15.01.19	Due for Review	15.09.22

1. Scope

This policy applies to all Rossendale Council Members and applies to both Council work related social media use and personal social media use. It is aimed at protecting all Members and the reputation of the Council. It applies whether social media is accessed using Rossendale equipment or otherwise and whether used or accessed during working hours or otherwise.

With the advent of the new General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 it applies whether or not you consider you've restricted your privacy on a particular platform by using the privacy settings and whether or not you consider that you're in a 'private conversation'.

2. What is social media?

We understand how important social media is in today's world. This policy deals with personal and business use of all forms of social media including Snapchat, Instagram, Facebook, Twitter, blogs, YouTube, Pintrest, Wikipedia and networking sites such as LinkedIn or Local Government Knowledge Hub Forums, are all examples of social media, though they are not an exhaustive list.

The term refers to any online technologies and practices that are used to share content and covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations.

3. Why do local authorities need social media? (Benefits and Risks)

Currently Rossendale Borough Council uses Twitter and Facebook and a variety of other mediums, but as the world of social media is ever changing and growing this may change and the Council may look to become involved in other forms of social media. Rossendale Members can utilise their smart devices to engage with Social Media.

Local authorities and other public sector agencies are increasingly looking to social media to engage with their audiences for many reasons:

- Have a more active relationship with the community
- As it is both fast and responsive it can offer immediate communication, residents expect prompt responses from their Council
- Helps to engage the younger people more
- It's cost effective to use
- Better interaction with other organisations, key stakeholder, and the media
- It can reach a mass audience quickly, it is more accessible to the community
- It presents are more "human" face of the Council
- Central Government are promoting the use of social media.
- It can bring people together over common interests
- Useful way to consult with residents and get feedback
- Authorities can publish their own message, which other media may ignore
- It can provide engaging live coverage of events (e.g. elections, incidents and events we are part of)

However, social media must be treated with respect and caution, as there are risks to its use. These include, but not exclusive to:

- Comments / posts may stay public for a long time and possibly never be removed.
- Comments / posts can be republished on other websites.
- Comments / posts can be copied, used and amended by others.
- Comment / posts could be changed to mis-represent what has been said.
- Social media can attract comments and interest from other people and the media.
- Social media can be seen by anyone.
- Social media accounts can be hacked, bringing the reputation of the Council into disrepute and tarnishing the public image of the Council.
- Criticism of the Council from the general public can often be seen by a mass audience and can threaten the image and reputation of the Council.
- Comments and posts can affect the credibility of Members.

There is a requirement to always be aware of the standards, conditions of use and guidelines for posting laid down by the owner of any site or network and make sure they are complied with.

4. Legal Implications

Social media use still has legal implications around libel, deformation of character, copyright and data protection.

Libel is the publication of a statement about a person that damages his / her reputation and causes others to have a lower opinion of them. If an employee publishes a statement about a person, which is damaging to their reputation they may take a libel action against them.

Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc.) without permission is likely to breach copyright. Permission should be sought in advance of publishing. Breach of copyright may result in an award of damages against the individual. The posting of images and/or footage of people online and tagging people in photos can infringe their privacy.

Personal data of individuals should not be published. Members must not disclose anyone's personal details, without their express written permission, and they must ensure that and personal or sensitive information is handled in line with the General Data Protection Regulation the Data Protection Policy 2018.

5. Using social media and your role at Rossendale Borough Council

If Members use social media for their own personal use or within their Member role at the Council there is a requirement to stay within the law at all times, and to be aware that fair use, financial disclosure, libel, defamation, copyright and apply on-line just as in any other media.

Members need to be aware that people may see social media information whether

individuals identify themselves as an elected member of Rossendale Council or not, and there is a need to think carefully about how much personal information you make public.

Members are advised that personal details like home addresses, phone numbers, financial information or full date of birth should never be given out to prevent identity theft.

Where Members choose to make comments on council-related matters, they must make it clear that they are speaking personally, or as an elected Member, and not on behalf of Rossendale Council. The easiest way to do this is to write in the 'first person' (I think / my view is.) and include a visible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of Rossendale Borough Council."

Members need to also be aware that they may attract media interest as an individual, and therefore care is needed whenever social media is used for personal or business reasons.

There is a need to remember obligations to residents, service users, partners, suppliers and colleagues and to protect the Council's reputation. Details of or dealings with colleagues, customers or partners should never be given out without their explicit consent.

Offensive comments should never be made about any customer, supplier, partner or any of their employees or Council colleagues. Racist, sexist or LGBT phobic slurs, personal insults, obscenity, unacceptable language or behaviour, which is unacceptable in the workplace, should not be used; this could bring the Council into disrepute, break the law and could result in disciplinary action and/or prosecution.

Individuals should ensure that they:

- Don't "pick fights".
- Are the first to correct personal mistakes.
- Refrain from altering previous posts without indicating that they have done so.
- Aren't afraid of being themselves, but there is a need to be considerate about other people's views, especially around 'controversial' topics such as politics and religion, individuals can challenge without being abusive or rude.
- Are credible, accurate, fair and thorough and do the right thing.
- Stay within the legal limits.

You must not use social media to;

- Make false or misleading statements.

- Impersonate colleagues or third parties.

- Express opinions on our behalf other than with our written authority.

- Associate your comments with our logos, slogans or other trademarks.

- Suggest that your own personal views are in any way connected with us.

- Connect with contacts made in connection with your employment other than with our approval.

- Post anything that could damage our reputation, or that of our clients, customers, suppliers, products, services, consultants or employees.

- Post any information which contravenes, commercially sensitive information or personal data (other than in respect of yourself).

Information that is gained from social media can be shared with others, where appropriate.

6. Personal Use of Social Media

Members must be aware that, where they using social media and are identified, directly or indirectly, as an elected Member of Rossendale Borough Council they are expected to behave appropriately and in line with the Council's values and policies.

Any information you post on social media can be accessed around the world in seconds and will be publically available for all to see. In light of this **some guidelines** are;

- Add a disclaimer to your social media account to make it clear that this is your own personal account and not affiliated with the Council.
- Check your privacy settings.
- Your work email address should not be used when registering to a social media account for personal use.
- Mature discretion should be exercised in all personal communications   on social media.
- Gross misconduct can also apply to activity on personal social media accounts When it has threated the reputation and image of the Council and brought the Council's name into disrepute. This may be referred to the Standards process.
- Do not be tempted to "let off steam" on social media, you may post comments you later regret and you may not be able to delete them.
- Do not be tempted to share or retweet gossip / hear 'say – posting untrue comments about someone, or even just repeating untrue things that someone else has said could constitute libel.
- Think about social media as an online CV.
- Members are advised to use their judgment; Members are reminded that there are always consequences to what is published.
- You are responsible for the information you are putting online.

7. Speaking for the Council

Those using social networking sites should not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council) unless they are authorised to do so. From time to time, this will be regularly reviewed.

Members need to ensure that any wiki entries, articles or comments are neutral in tone, factual and truthful. Rude or offensive comments on any online encyclopaedias or sites should never be posted. You will also need to check the house rules of the site. You may also need permission form the relevant wikieditor and the council's People and Policy Team.

If you edit online encyclopaedias at a Council office or on a Council device, the source of the connection may be recorded as a Rossendale Council IP address. That means it may look as if the Council itself has made the changes. If this is correcting an error about the Council, that is fine – there is a need to be open about our actions, in other circumstances care needs to be taken not to bring the Council into disrepute.

8. Social Media Use in Council Meetings

Legislation has recently been passed by the Department for Communities and Local Government that allows members of the press and public to live report Council meetings via social media. People wishing to do this should ask the Council about the facilities to do this. This provision for social media is details in Rossendale Borough Council's Constitution and Section 40 of the Local Audit and Accountability Act 2014.

Members must not publish or report on meeting which are private or internal (where no members of the public are present or it is of a confidential nature).

9. Risks

Risks that Members should be aware of, that come with social media use are;

- Virus or other malware (malicious software) infection from infected sites.
- Disclosure of confidential information GDPR / DPA 2018.
- Damage to the Council's reputation.
- Social engineering attacked (also known as 'phishing').
- Cyber Bullying, witch-hunting, stalking or harassment.
- Civil or criminal action relating to breaches of legislation.
- Breach of safeguarding with images or personal details leading to the exploitation of vulnerable adults.
- Breaking of privacy GDPR / DPA 2018 laws.

Due to the above risks, it is important that your actions and activities be in line with this policy.

Remember that everyone can see what you post on social media, even private messages at times; this is a wide and uncontrolled audience. There is also the

potential that the post is there to stay, deleting it may not always get rid of it completely, or it may have been passed on already.

Members must make sure that all video and media is safe to share, does not contain any confidential, discriminatory or derogatory information, and is not protected by any copyright or intellectual property rights. If the content is official Rossendale Council l content then it must be labelled and tagged as such. Employees need to ensure that any material considered obscene should not be published and is a criminal offence.

The use of social media can compromise the privacy and security of personal data and GDPR / DPA prohibits this. Please make sure you never give out any personal details on social media without seeking their consent.

Safeguarding issues are paramount because social media sites are often misused by offenders. Safeguarding is everyone's business at the Council – all Members have a responsibility to report any concerns about other site users. Contact the Council's 'Designated Safeguarding Officer' (DSO), on 01706 252457.

10. Complaints – Misuse of Social Media

If a Member has any concerns about anything posted on a social media site, which the Council has responsibility for, or an account linked to an employee or Member, they should contact the People and Policy Team in the first instance and provide any supporting evidence to enable appropriate action to be taken.

11. Conclusion

These guidelines are to protect Members and the reputation of the Council - they are not meant to restrict genuine and work related use of what is an important method of communication and engagement. By its nature though, social media is fast and responsive so when a mistake is made it can rapidly get out of control.

Authorisation form - use of social media for work related purposes

I confirm that I have read and understand the Social Media / Networking Policy for Members using Social Media regarding Rossendale Borough Council.

Name:

Signature: **Date:**

Responsible Section/Team	ICT	Page Number	8
Responsible Author	Andrew Buckle	Date Agreed / Agreed At	
Date Last Amended	15.01.19	Due for Review	15.09.22

Rossendale
BOROUGH COUNCIL

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 (GDPR), Data Protection Act (DPA) 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 ICT systems are a useful and integral part of our daily lives, Internet and e-mail access has been provided. 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 the 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, radically 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 the RBC Mimecast 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 & ICT.

The above list is not exhaustive by any accounts.

Downloading and Using Information

While RBC tolerates limited personal use of its ICT facilities, Members should use them responsibly, and be mindful that 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 and disks. This includes removable storage devices, SD cards etc.
- 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.

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, radically 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.
- Soliciting for, or pursuing personal gain or profit.
- Circumventing RBC security controls to access unauthorised Internet or e-mail services.
- Any illegal activities.

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 RBC 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 RBC 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

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 as per GDPR and DPA requirements.
- 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 as per GDPR and DPA requirements.

Remote Access

Members using remote access to RBC managed ICT 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, smartphones, tablets, usb sticks, etc. and including the information, reports and any data they hold.

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

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 ....

Rossendale Borough Council Members Mobile Telephone Policy

Jan 2019

Contents

1.0 Rationale

Mobile and Smart phones are a key business tool in today's working world and also have such strong information and health and safety risks associated with them, the policy is designed to ensure that mobile phones are used in a safe, responsible and cost-effective manner.

2.0 Summary

- Mobile phones are issued to all Members.
- Members must declare if they intend to make private calls from their Council provided mobile and if so then they must pay for any costs incurred.

3.0 Introduction

3.1 Definitions

Mobile telephones provide an invaluable means of keeping in touch with colleagues, clients and customers are provided by the Council as a business tool.

3.2 Scope

The policy:

- This policy applies to all Rossendale Borough Council (RBC) Members.
- Covers all calls, all text messages (SMS and MMS), data usage, cost of any downloaded applications and any costs whatsoever incurred outside of RBC corporate contract.
- Complies with the information management requirements of General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

3.3 Authority

This policy is authorised by the Chief Executive, RBC.

4.0 Objectives and Basic Principles

4.1 Objectives

- To mitigate the risks associated with mobile phone use by Members.
- To provide appropriate devices and services to meet the business requirements and service delivery.
- To recognise and appropriately manage the health and safety risks associated with the use of mobile phones.
- To educate and publicise the risks and procedures regarding mobile phones to all Members.

4.2 Basic principles

RBC needs to manage risks and opportunities of mobile phones to ensure that the Council is not compromised by the use of them.

5.0 Roles and Responsibilities

5.1 Roles

RBC Head of Customer Services and ICT will:

Be responsible for:

- Managing the development and upkeep of this policy.
- Ensuring that documentation is relevant and kept up-to-date, including legislation.
- Determine Council policy and minimum requirements on mobile telephony matters and ensure that the policy and subsequent updates are communicated and implemented effectively throughout the Council.
- Ensure all Members are aware of the Council's mobile telephony policy and their obligations within it. Arrange mobile telephony investment and contract proposals.
- Be responsible for defining the requirements for the mobile telephony infrastructure.
- Ensure that this Policy and its minimum requirements are applied to all mobiles and resources and are compliant with local legislation, regulatory and safety requirements.

5.2 Responsibilities

All Members:

- Familiarising themselves with this policy.
- Adhering to this policy and following the associated procedures when applicable.
- Reporting any security breaches or incidents.
- Reporting loss of Telephone ASAP to O2 on 0800 328 0002, EE 07953966250 or Vodafone 03333040191 asking for a bar to be applied to your RBC mobile telephone number. Failure to do this may result in call charges being accrued; it is the responsibility of the user to inform O2 / EE / Vodafone straight away to avoid this. **Any such costs will be recharged to the Member.**
- Under no circumstances do users let anyone other than an RBC approved mobile phone user, use their device. If they do and the phone is lost or damaged, any costs incurred as a result of this will be recharged to the user.

- Highlight any personal calls that are made to Finance and make the necessary payment to cover costs.
- The usb cable, AC power adaptor (charger), headphones etc. have to be returned to RBC; if anything is missing from the original equipment list the user will be charged.

Please see appendix A for details of the RBC Mobile Contract

5.3 Non-compliance

Non-compliance with policy requirements will be dealt with by RBC Head of Customer Services and ICT and the Section 151 Officer.

The right of appeal will be to the Chief Executive.

5.4 General Use

Members are accountable for using mobiles in a responsible fashion and for protecting the mobile equipment from unauthorised access or loss, in particular:

- Exercise good judgement and economy when using mobile phones for business purposes.
- Do not make any calls to premium rate numbers unless there is a defined business need to do so. Calling "adult chat lines" or similar services is specifically prohibited.
- Do not use any directory enquiries service.
- Do not use data abroad, the Council's most cost effective way of accessing emails abroad is via either of the following: https://webmail-uk.mimecast.com/

Please see appendix A for further details.

- Call charges abroad vary according to destination. International roaming is disabled by default and must be agreed by the respective Group Leader and RBC Section 151 Officer.
- Due to RBC smartphones being unlocked any costs associated with apps, widget games, downloads, texts, media or images and so on will be recharged to the Member. The owner of the device will be held responsible for anything that has been downloaded onto the device.
- Any malware downloaded on the phone will be the responsibility of the owner who may have to replace the device if the malware destroys the phone. The Member will be charged for a replacement device.
- Any individual user configurations outside of RBC business requirements will not be supported by ICT in terms of support, use and functionality.
- The mobile phones are only to be used for business calls, text messages and data usage, any personal usage made will have to be detailed and paid for. Unless the call is deemed as an emergency call that the individual has made.

- Social networking facilities on RBC smartphones are only to be used for RBC business, e.g. Facebook and Twitter accounts etc.
- Not make abusive, threatening or otherwise malicious calls, or any other action that will reflect poorly on RBC's name or reputation.
- Be considerate whilst using mobile telephones, such as by leaving the room to take a call and setting a low ringer volume.
- Ensure when sending SMS or MMS text messages they do not purport to be representing RBC when they are not.
- An anti-virus application will be loaded to the smart phone any attempt to download any malware the device may be automatically reset to factory settings and also sound an alarm.
- RBC has the right to delete any application / widget / information or any download on the device without notifying the user.
- RBC will use a Mobile Device Management (MDM) to control the device and the device can be accessed at any time by RBC staff.
- Do not store any customer data on the device or storage card (SD Card).
- Only use the RBC Mimecast Secure email system to send RBC information, do not use a personal email address.
- Do not store RBC information on the device or SD card.
- Phone passwords must not be shared with colleagues, friends and family members.
- All GDPR and DPA requirements apply to any RBC mobile devices.
- **Failure to meet all of the conditions may lead to the device being removed and serious breaches may be referred to Standards.**

5.5 Health and Safety

Members must take due care and attention in their actions to ensure that neither the Council nor they are placed at risk through actions that are considered illegal, inappropriate or an unacceptable risk, particularly:

- Comply with local instructions restricting use, for example in hospitals, aircraft etc.
- Do not use when operating machinery.
- Do not use a mobile phone device when driving, unless when using a legally approved hand free device in a safe and satisfactory manner (that is, in full control and not distracted whilst driving). Driving also includes a stationary vehicle with the engine running.

However, the Council accepts that there may be occasions when a Member receives a telephone call when driving a vehicle. If the Member chooses to answer the telephone call whilst driving this will be at their own accountability.

5.6   Personal Calls

Members must make an initial declaration of whether the telephone will be used for personal calls in addition to business purposes, and renew the declaration if circumstances change.

By declaring intent to use a Council provided mobile phone for personal calls, you agree to the monitoring of your mobile phone bill to ensure that personal calls are paid for. Spot checks may be carried out to enforce this.

Members must reimburse RBC for all personal calls made including Value Added Tax (VAT). Individual itemised call statements are provided for this purpose.

5.7   Provision

Mobile phones will be provided to all Members following appointment.

6.0   Agreement

I have received a copy of Rossendale Borough Council's Members Mobile Telephone Policy Guideline. I agree to abide by all the terms and conditions set out in the above policy.

Signed…………………………………………Date ………………………

Print Name ………………………………………………………………….

Group / Party …………………………………………………………..

Responsible Section/Team	ICT	Page Number	7
Responsible Author	Andrew Buckle	Date Agreed / Agreed At	
Date Last Amended	15.01.19	Due for Review	15.09.22

APPENDIX A

RBC O2 Contract Deal

Inclusive Minutes
Under the new O2 contract for Smart phone users Council has unlimited minutes to the following:

- **01/02/03 Local Geographic Numbers -** These three codes are used for everyday local and national calls (calling your neighbour or a relative in another part of the country).
- Cross network mobile numbers.

RBC EE Contract

Unlimited minutes

RBC Vodafone Contract

Unlimited Minutes

O2 to O2, EE to EE and Vodafone to Vodafone calls.

Any calls from O2 to O2 are free regardless of inclusive minutes.

070 calls

Watch out for 070 codes. They look like mobile phone numbers, but can cost up to 50p a minute. 070 phone numbers are intended to act as a forwarding service – known as personal numbers, they divert calls to the owner's location.

However, because they are easy to mistake for mobile phone numbers, some criminals use them to try to con you into calling them and making money out of it. If you receive a missed call on your mobile from a 070 number, do not call it back – it is likely to be a scam.

Non Geographic Numbers

These phone numbers include 03, 0844, 0845, 0870 and 0871. Non-geographic phone numbers aren't tied to a geographic location, so you can't tell where in the country you're calling. Large organisations like them because they can use one phone number for all customer communications, which won't have to change if they move office location.

Most of these numbers called maybe unavoidable and although the volumes are quite low the charges are high. These tend to be calls to stakeholders, for example:

- Lancashire County Council Various
- Animal Wardens
- Disability & Living Allowance Helpline
- Countryside Services

It may be worth investigating if we have direct dials for any of the back offices to avoid calling the non-geographic numbers and associated charges. The following website may help in some cases.

http://www.saynoto0870.com/search.php

Premium Rate Calls

09 calls

Phone numbers starting 09 are charged at a premium rate, and are the most expensive type of phone number to call. Premium-rate 09 phone numbers are often used for TV phone-in quizzes, which at least you have a choice whether to call or not. But alarmingly some companies use them for technical support.

The most you're likely to pay from a BT landline is £1.50 a minute for a call, but charges for calling premium-rate phone numbers from a mobile phone can be much higher.

Freephone numbers

Calls to 0500, 0800 & 0808 numbers are free from landlines, but typically cost between 15p and 30p a minute from mobiles and are not included in 'free' mobile minutes

Voicemail

To access your voicemail simply dial 901 or even easier press and hold the number 1 on the keypad. The first time you do this you will need to enter 901 when prompted for the answer phone number and you may also be asked to set a pin number on the handset, this will only happen when you set this service up for the first time.

Call Return (Pressing 3 from Voicemail)

Please do not use this facility as it could turn out to be costly.

Directory Enquiries

Please do not use this facility as it could turn out to be costly.

We would recommend the following approach:

In the office - Google or alternative search engine
Out of the office - Call a colleague to use Google or alternative search engine
We realise that this is not always practical but try to use this approach wherever possible.

International Calls

Outside Europe, call charges vary and some are very expensive. If you are planning on using your phone abroad for work related calls please contact the ICT Team to arrange the best price dependent upon location.

https://www.o2.co.uk/international/internationalhub

https://ee.co.uk/help/help-new/roaming-and-international

https://www.vodafone.co.uk/explore/costs/travelling-abroad/

Text Messages

Under the new contract the Council has unlimited Text messages per month for smart phone users.

Inclusive Data

This only applies to users who have both voice and data tariff.

Under the new O2 contract, the Council users have a limit of 3 GB of Data per month anything in excess of that will be paid by the person using the phone.

If a Member requires additional data, this has to be agreed by the respective Group Leader and Section 151 Officer.

Vodafone have 2GB per user per month.

EE have 4GB data per user per month.

Data Abroad

We would recommend wherever possible the following:
- Data services are turned off before travelling abroad (Contact ICT Team if unsure how to do this);

- Free Wi-Fi be utilised if necessary for emails;
- Alternatively Mimecast can also be used if free Internet access is available:
https://webmail-uk.mimecast.com/login.jsp
Username – RBC email address
Password – RBC Office 365 login password.

Data abroad bundles no longer exist and although we get a reduced rate on data traveller charges through My Europe extra for data within Europe anything outside of Europe is very expensive and should be avoided at all costs.

Problems with Signal Coverage

The following link can be used to check signal coverage in a particular area:
http://status.o2.co.uk/
https://www.vodafone.co.uk/explore/network/
https://myaccount.ee.co.uk/networkchecker/checkservice

APPENDIX B

Mimecast Webmail - https://webmail-uk.mimecast.com/
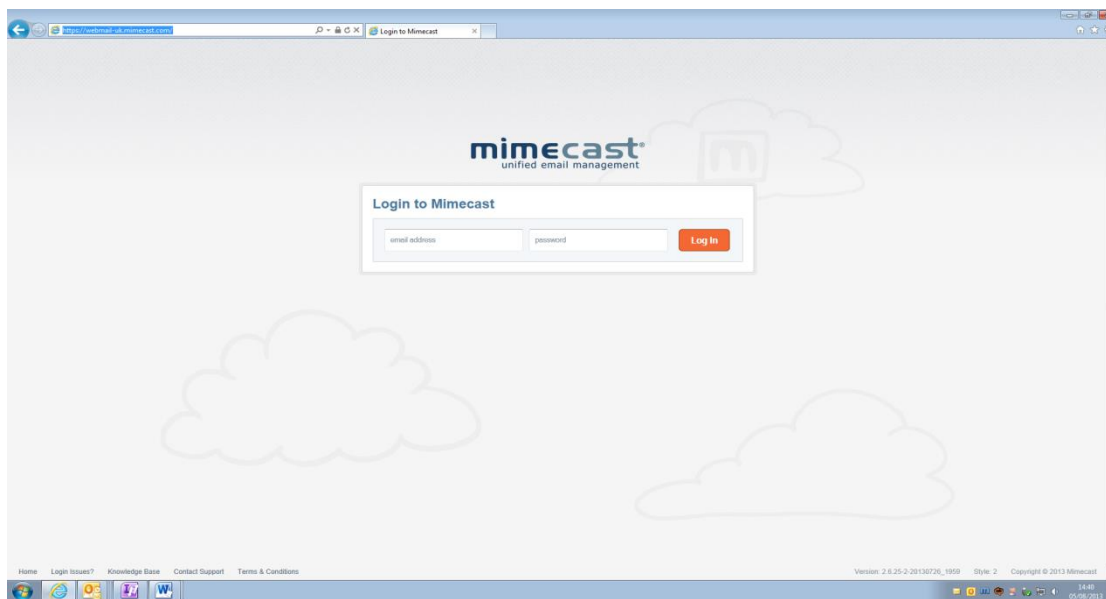
Login details are RBC email address, followed by network password.

Responsible Section/Team	ICT	Page Number	11
Responsible Author	Andrew Buckle	Date Agreed / Agreed At	
Date Last Amended	15.01.19	Due for Review	15.09.22

INITIAL EQUALITY IMPACT ASSESSMENT

Name of Policy, Decision, Strategy, Service or Function, Other: (please indicate)	RBC Members Social Media, Email & Internet Acceptable Use, Mobile Phone Policy.
Lead Officer Name(s) & Job Title(s) :	Andrew Buckle – Head of Customer Service & ICT
Department/Service Area:	
Telephone & E-mail Contact:	andrewbuckle@rossendalebc.gov.uk

Date Assessment:	**Commenced:** 14th February 2019	**Completed:** 18th February 2019

We carry out Equality Impact Assessments (EIAs) to analyse the effects of our decisions, policies or practices. The EIA should be undertaken/started at the beginning of the policy development process – before any decisions are made.

1. Overview

The main aims/objectives of this policy[1] are:
The RBC Members Social Media, Email & Internet Acceptable Use, Mobile Phone Policies are required to comply with the General Data Protection Regulation (GDPR) EU 2016/679 and Data Protection Act.

(Refer to **EIA Guidance** for details)

Is the policy or decision under review (please tick)

New/proposed☒   Modified/adapted ☒   Existing ☒

_____

INTERNAL ONLY
MANAGEMENT ACTION REQUIRED (to be completed by the relevant Head of Service following review by Management Team / Programme Board)

- Outcome of EIA agreed/approved by Management Team / Programme Board: Yes ☒   No ☐

- Is a full EIA required   Yes ☐   No ☒

- Referred back to Assessor for amendment :   (date)

- Published/made publicly available on: Rossendale BC Website (date) TBC

Signed: Andrew Buckle   (Head of Service / Director)   Date: TBC

Date of Review[2]: February 2021 – to coincide with the review of the policy.

_____

[1] Policy refers to any policy, strategy, project, procedure, function, decision or delivery of service.
[2] This date will be set on an annual basis as default for review unless otherwise specified by you.

2. Equality Impact

Using the table below please indicate whether the policy/strategy/decision has a positive, negative or no impact **from an equalities perspective** on any of the protected equality groups listed below. **Please also give consideration to wider equality of opportunity and community cohesion impacts within and between the groups identified. If you have identified any negative impact and mitigating actions are not sufficient, you** *will* **need to complete a Full Equality Impact Assessment.**

Equality		Positive Impact (It could benefit)	Negative Impact (It could disadvantage)	Reason and any mitigating actions already in place (to reduce any adverse /negative impacts or reasons why it will be of positive benefit or contribution)	No Impact
Age	Older people	☐	☐	Whilst older people could be priority need due to vulnerabilities caused by their age, and therefore the Council would be more likely to have a duty to assist with temporary accommodation, this is not changed by the policy.	☒
	Younger people and children	☐	☐	When considering location, where there is a choice, preference may be given to certain households with children and young people for an in borough placement.	☒
Disability	Physical/learning/mental health	☐	☐	People with disabilities or conditions may be prioritised for temporary accommodation placements closer specialist education or support,	☒
Gender Reassignment	Transsexual people	☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
Pregnancy and Maternity		☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
Race (Ethnicity or Nationality)	Asian or Asian British people	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to population as a whole.	☒
	Black or black British people	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒
	Irish people	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒

Responsible Section/Team		**Version**	
Responsible Author		**Due for review**	
Date last amended		**Page 2 of 3**	

Equality		Positive Impact (It could benefit)	Negative Impact (It could disadvantage)	Reason and any mitigating actions already in place (to reduce any adverse /negative impacts or reasons why it will be of positive benefit or contribution)	No Impact
	White British	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒
	Chinese people	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒
	Gypsies & Travellers	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒
	Other minority communities not listed above (please state)	☐	☐	No reason to believe any additional positive or negative impact to people of any ethnicity or nationality compared to the population as a whole.	☒
Belief or Religion		☐	☐	No reason to believe any additional positive or negative impact to people of any belief or religion compared to the population as a whole.	☒
Sex	Women	☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
	Men	☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
Sexual Orientation	Gay men, gay women / lesbians and bisexual people	☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
Marriage and Civil Partnership (employment only)		☐	☐	No reason to believe any additional positive or negative impact to this cohort.	☒
Contribution to equality of opportunity		☐	☐	Positive impact by assisting everyone into suitable accommodation that meets their needs.	☒
Contribution to fostering good relations between different groups (people getting on well together – valuing one another, respect and understanding)		☐	☐	No impact expected.	☒
Human Rights		☐	☐		☒

Responsible Section/Team		**Version**	
Responsible Author		**Due for review**	
Date last amended		**Page 3 of 3**	