Sheffield City Region
MAYORAL COMBINED AUTHORITY

IT Policy

Document Properties

Change Record

Version	Author	Description	Date
1	SD		25/05/18
2	LG		25/11/19
3	IL	Replaces: IT Policy (P26) (April 2011) Social Media Policy Reference: (P49) (April 2014) Procedure for the transfer of personal data (P43) (December 2009)	Mar 2020
4	RR/ AD		June 2021

Document Approval

Approving Body or Person	Role (review, approve)	Date

Contents

1. Policy Statement

1.1. This policy governs the use of all Sheffield City Region Mayoral Combined Authority (SCRMCA) IT systems and services and the use of external systems and services by its staff. IT systems and services include but is not limited to PCs and Laptops,software, telephones (fixed and mobile), email, social media and the Internet. The use of personal social media where it may reflect on the values and services of SCRMCA is also included.

1.2. SCRMCA views IT services as valuable business tools. The organisation wishes to gain benefit from the use of IT services without subjecting itself and stakeholders to undue risks through security weaknesses or misuse.

1.3. All users of SCRMCA IT systems and services are expected to abide by this policy. The term User within this policy refers to any person, not just employees, working with SCRMCA who have access to SCRMCA systems and services for whatever reason.

1.4. With the pace of technology, it is impossible to be prescriptive of every eventuality. Users are expected to conform with values of SCRMCA in everything they do. As long as you use SCRMCA systems for authorised purposes in accordance with the organisations values and seek support from the IT department when appropriate you will be using IT systems and services appropriately

1.5. Users are reminded that SCRMCA engages with the public and staff in a way that requires the organisation to collect, store and use personal information. Failure to abide by this policy could lead not only to the organisational disciplinary process but to criminal investigation and sanctions under the Data Protection Act 2018, General Data Protection Regulations (GDPR) and the Computer Misuse Act 1990.

2. Detailed Policy Elements

2.1. Detailed policy elements specific to IT services are included as appendices to this policy. These are:

- Appendix A – Email & Instant Messaging Communication
- Appendix B - Internet Access
- Appendix C - Cyber Security
- Appendix D - Telephony / Audio Visual
- Appendix E - Mobile Working
- Appendix F - Social Media
- Appendix G - Transfer of Personal Data

3. General

3.1 Service Desk

a) SCRMCA IT services are managed using ITIL best practices. The starting pointfor all Users who have any IT issues or requests is the self-help facilities followed by the Service Desk.

b) To help manage the capacity of the Service Desk and ensure it is available when needed, all users will (where possible) use self-help facilities and log calls via the ServiceDesk portal prior to calling the Service Desk.

c) The IT department publish self-help guides on the intranet and provide the means for people to self-reset their passwords(link).

d) Data from the service desk from the system may be used to identify additional training or self-help guides that may be required.

4. General Exclusions on Usage

4.1. No user shall:

a) use, or allow any other person to use, SCRMCA systems in an unauthorised way.

b) disclose any information to unauthorised parties which would allow those parties access to the organisation's systems and information or those of its partners, suppliers, customers, or users.

c) use, or allow any other person to use, SCRMCA systems to gain access to store, modify or distribute material which could be considered to bring the organisation into disrepute or is illegal in nature.

d) use SCRMCA’s IT resources for personal monetary gain, nor for commercial purposes that are not directly related to SCRMCA business.

e) transmit SCRMCA owned information (which is not already in the public domain) to individuals or organisations except in the normal execution of their duties

f) participate in any activities via IT services (including non-SCRMCA services) which could reasonably be considered to bring the name of the organisation into disrepute.

g) create, communicate or share anything of an offensive nature, including defamation or harassment of colleagues or others, this will be considered as bringing the organisation into disrepute.

4.2. No contract should be entered into for external / 3rd party IT products and/or services, without the prior approval from the Head of Information Technology or nominated deputy.

4.3. No IT system, including but not limited to hardware, software, applications and databases shall be developed or procured through any means without the prior written approval of the Head of Information Technology or nominated deputy.

4.4. Personal Use and Responsibility

a) Users are required to return all business-related IT equipment, records and documents in their possession if they leave SCRMCA, failure to return identified equipment may result you costs incurred.

b) SCRMCA's IT services are for business use and resources are limited. Network bandwidth and storage capacity has finite limits, and all Users have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include but are not limited to, playing games, uploading or downloading large files, accessing streaming audio and/or video, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses.

c) Occasional personal use of the internet and email is permitted provided it is carried out in the user's own time. Personal use should not interfere with the user's performance of their duties or require changes to the organisations firewall.

d) Through its automated monitoring systems, the organisation has the ability to identify personal use. The organisation reserves the right, , to change for any personal issues that sees additional costs incurred by the organisation.

e) If a user receives an offensive communication through any IT service includingtelephony, they should inform the Service Desk. In such circumstances do not delete any such message from any storage system unless instructed to do so. The IT Department and Human Resource Team will, where necessary, carry out an investigation before making any decision on the matter.

f) Where goods or services are purchased by a User, for their own use, using the organisation's IT Services, then this is done at the User's own risk.

4.5. Systems Access

Unauthorised use of SCRMCA IT systems or the information contained within them is not permitted.

a) Users must keep all passwords and security codes secure.

b) Users are personally responsible for all their activity using any IT system or service.

c) With mobility it is possible to access systems from anywhere. Secure behaviour is expected from every user. Users should take precautions to stop

unauthorised use of their login credentials by not writing them down and ensuring they lock their device (⊞ +L) when leaving it unattended even for a short time.

d) Individuals who are found to have damaged any systems or accessed any systems without authorisation whether through deliberate or negligent action may be subject to SCRMCA's disciplinary procedures.

4.6. Representation of SCRMCA

a) No user shall purport to, or allow any other person to purport to, represent the organisation except in areas where they have the authority to do so.

b) Any personal statements not directly connected with the business of SCRMCA must contain a clear statement to the effect that

"This is an individual view and not necessarily an expression of the views or policy of Sheffield City Region Mayoral Combined Authority".

4.7. Legislation

a) All SCRMCA information and data is subject to the Data Protection Act 2018

b) In the event of SCRMCA receiving a Subject Data Access Request, under the Data Protection Act 2018, the organisation retains the right to search all IT systems and devices for the requested information. Where the search includes personal drives, Users will be informed that this will occur prior to the search taking place, this however may not always be possible, in which case users will be notified after the search.

c) In the event of SCRMCA receiving a Freedom of Information Request (FOI), under the Freedom of Information Act 2000, the organisation retains the right to search all IT systems and devices for the requested information. Where the search includes personal drives, Users will be informed that this will occur prior to the search taking place, this however may not always be possible, in which case users will be notified after the search.

4.8. Monitoring of Systems

a) The Information Technology Department is responsible for the secure operation of any monitoring systems and services which the organisation determines should be operated to ensure the integrity of its systems and data,to ensure they remain secure and fit for purpose.

b) Use of many IT systems which include telephones, email and Internet are subject to routine audit to enable system performance and monitoring of costs to take place. The detailed content of these logs is retained for a maximum of 3 years.

c) Within the M365 environment automated version tracking makes itpossible for Users to see who has modified files. Users can only access documents they have permissions to.

d) The organisation has, and will maintain, the ability to monitor specific individual

usage of IT Services including storage, printing, internet, TEAMS, voice calls and email services.

e) The organisation reserves the right to carry out audits of the use of any IT service at any time.

f) If a user is absent from work and unable to give timely authorisation for access to be granted, SCRMCA retains the right to check IT services for business related correspondence when there is a justifiable business reason.

g) Approval for access to user systems in these circumstances will be required from Human Resources member, prior to the user's Line Manager or other nominee being able to access the relevant system.Access to the user's system will be removed as soon as reasonably possible following the individuals return to work or notification that such access is no longer required.

h) Routine manual inspection of the content of electronic information will not take place. Manual inspection will only occur if there is good reason to believe that the user's usage:

   i) contravenes any SCRMCA policy

   ii) contravenes criminal law,

   iii) contravenes his/her employment contract,

   iv) contravenes discrimination law,

   v) amounts to a civil wrong (such as defamation),

   vi) means aspects of this policy are being broken,

   vii) or is required to protect health and safety

Users will be informed before any manual inspection takes place if appropriate or possible.

i) Should the organisation detect use of a system, or information obtained from any system, by its users that could be deemed to appear to contravene United Kingdom or International law, the matter will be referred in the first instance to the Principal Solicitor and Secretary. The Principal Solicitor and Secretary will decide whether the matter should be referred to the Police or other official body.

j) It is possible that any external telephone, video call, email message or access of Internet sites is being logged or recorded by others as well as SCRMCA. Thepolicies of other organisations will vary from those of SCRMCA. As a result, SCRMCA cannot guarantee the Users safety, security or anonymity when using external IT systems or services.

4.9. Software

a) SCRMCA is committed to using software for which it is properly licensed and will not accept the use of unlicensed software or more copies of software than it

has licences.

b) All computer software must be procured through the Information Technology Department. No user may procure software by any other means

c) Software must not be installed on any equipment unless carried out either by the Information Technology Department or with the express written permission of the Head of Information Technology or nominee. If a User requires additional software this may be requested via the Service Desk.

d) The Information Technology Department may use tools to remotely install and remove software from organisations devices to ensure ongoing compliance with organisational policy, licensing and security.

e) There must be no transferring of software between computers without the express permission and involvement of the Information Technology Department.

f) It is forbidden for Users to load and operate software obtained from the Internet, via email or other sources including 'public domain', 'shareware', 'freeware' or 'evaluation' software without the prior written permission of the Head of Information Technology or nominee. Permission will only be granted following suitable testing and the organisation having or being able to obtain an acceptable licence for the software. The security of the organisations systems, data and services is the paramount concern when making the decision.

4.10. Copyright

a) Users may not illegally copy material protected under copyright law or make that material available to others for copying. Users' are responsible for complying with copyright law and applicable licences that may apply to software, files, graphics, documents, messages, and other material they wish to download or copy. Users' may not agree to a licence or download any material without first obtaining the express written permission of the organisation from the Head of Information Technology or Principal Solicitor and Secretary or nominees as appropriate.

b) Copyright exists in all Ordnance Survey and other mapping material (including internet-based services such as Google and Microsoft) the User must ensure that an appropriate licence is in place for the intended use of a map. Advice on mapping licences should be sought from a member of the IT Team.

Under no circumstances should mapping of any form be posted on the Internet withoutauthorisation of the Head of Information Technology or nominee.

5. Equality and Diversity

5.1. The organisation recognises its responsibilities and legal obligations under the Equality Act and will endeavour to respond with reasonable modifications to IT equipment and services

5.2. Any member of staff having physical difficulties with the use of IT equipment and services, should in the first instance consult with his / her Line Manager to carry out an assessment who may then consult the Health & Safety Advisor for a further personal assessment.

5.3. Several alternatives and modifications to equipment are possible and can be made if the personal assessment advises so.

5.4. This Policy and all public facing systems are assessed for impact against the Equality and Diversity framework.

6. Links to Other Policies and Procedures

6.1. The Head of Information Technology and member of the Human Resources Team will decide if there has been any infringement of the contents of any part of this policy, including the appendices, which may subsequently be subject to SCRMCA's Disciplinary procedures.

6.2. This policy should be read in conjunction with the organisation's other publishedpolicies and IT guidance documents which can be found on the intranet.

7. Review

7.1. This policy will be reviewed annually or in line with any changes in legislation. Feedback from staff and information gainedfrom the monitoring of the policy will be used to improve the policy. Appropriate legislative changes will be incorporated as a matter of course.

7.2. Changes to this policy shall be communicated to all staff and contractors through the standard internal communications methods.

Appendix A

Email & Instant Messaging

1. Disclaimer

The ability for users to exchange messages with individuals and other organisations using the Internet is a key business requirement. The provision of this service leads to the risk of unsolicited and potentially harmful messages being received by a user. The organisation uses appropriate tools to stop as many of these messages as possible from reaching users.These tools will be maintained to ensure the protection is as effective as possible. It is not however possible to stop all unsolicited messages, so users are expected to exercise due diligence with all messaging to keep themselves and the organisation safe from harm.

2. General Exclusions on Usage

2.1. Messaging systems such as (but not limited to) e-mail and Microsoft Teams should not be used to download or import software onto SCRMCA's systems without the prior written permission from the Head of Information Technology or nominee. Unless these forms a normal part of their duties. This includes software and shareware available on the Internet that may be apparently free.

2.2. Automatic forwarding of emails to non SCRMCA email addresses is forbidden.

2.3. Email is **not** a suitable repository for files. Any documents and files sent or received as attachments should be saved to the appropriate storage area and not left only in the User's email account.

2.4. Transmitting personal/sensitive information should only be done by people who are authorised to do so and using the additional secure tools Users will find in their Outlook email system. For further information see guidance on the intranet or contact the Service Desk.

3. Representation of SCRMCA

3.1. Users will create and attach standard email signature to their email correspondence according to the specifications of the Communications & Marketing Team 'Branding Guide' available on the Intranet.

3.2. A footer will be attached to all external emails automatically. This footer gives details about the company, the appropriate confidentiality notice and disclaimer.

3.3. All personal statements not directly connected with the business of the organisation must contain a clear statement to the effect that:

This is an individual view and not necessarily an expression of the views or policy of Sheffield City Region Mayoral Combined Authority

Users must include this text themselves when appropriate, as it will not be included automatically

4. Monitoring of Emails

4.1. All emails received by the organisation from external sources will be passed through scanning software before it reaches a user's account. As part of this process certain generic categories of email attachments will be automatically removed due to the risk of virus or other malicious software being imported in SCRMCA's systems. This process checks for viruses and malware but is not fool proof. If a user is uncertain about the source or content of an email or email attachment, then they should contact the Information Technology Department before opening the attachment or clicking on any links in the email.

5. Instant Messaging / Chat

5.1. Increasingly online services include the ability for engaging in a chat session. Internally SCRMCA provides Microsoft Teams as part of its M365 suite of services which includes instant message chat service.

5.2. Personal Chat facilities should not be used to transfer personal information or software unless prior approval is obtained from the Head of Information Technology.

.

Appendix B

Internet

1. Disclaimer

1.1. Users are cautioned that the internet is a largely uncontrolled global environment. Whilst the internet brings huge benefits it also contains offensive, sexually explicit, and other inappropriate material that is incompatible with the values of SCRMCA. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly dubious content. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive or malicious content. Users should be vigilant and cautious in using the internet to both ensure the security and reputation of themselves and the organisation. Users are individually accountable for their actions whilst using the internet.

2. General Exclusions on Usage

2.1. Internet access is governed monitored and recorded by automated systems so that any threats to the security and integrity of the organisation and its staff may be identified and managed appropriately.

2.2. Users deemed to be accessing or attempting to access inappropriate sites deliberately and for a time exceeding that associated with an innocuous search may lead to disciplinary action. Inappropriate sites are those that other users may find intimidating, upsetting, embarrassing, humiliating or offensive or are otherwise incompatible with the values of SCRMCA.

2.3. The Internet should not be used to download or import software onto the organisation's systems without the prior written permission from the Head of Information Technology or nominee. This includes software and shareware available on the Internet even if it is apparently free, including but not limited to screen savers, games and other applications.

2.4. In accordance with their duties staff in the IT department regularly download software patches, tools and code. Such use is authorised under this policy however as technical professionals they are expected to follow best practice to ensure the security of the organisations systems and services. For example, this may include only downloading to specific test and development environments for testing.

3. Internet Access

3.1. Connection to the Internet for any purpose will be through appropriate security systems, the configuration and performance of which will be the responsibility of the Information Technology Department.

SCRMCA devices should **not** normally be connected to the internet in such a way as they bypass the security measures in place. The IT department may bypass systems for the purposes of testing configurations and updates so as to ensure the security of the organisation.

3.2. SCRMCA devices will be configured by the IT department so that when they are used off the organisation's premises, they can securely connect to any available internet connection.

3.3. The organisation has the right to and will utilise software that makes it possible to identify and block access to Internet sites, other services that use a disproportionate amount of the organisations Internet resources or where these sites are not directly related to its business.

3.4. Should the standard level of access not meet the business needs for a given User they should request support from the IT Service Desk. The request will be reviewed by the IT department and actioned appropriately.

4. Security and Privacy

4.1. Standard internet-based file sharing and distribution services such as drop box should not be regarded as secure for business purposes and should not normally be used for the distribution or transfer of organisation information. Requests for access to services such as drop box will be refused. The use of Google tools is also discouraged. The IT department has configured a secure system for file sharing which should be used. Search for file transfer on the Intranet or contact the service desk.

4.2. If you need to send other people's personal details to someone else, then you must follow the procedure for the transfer of personal data which forms part of the organisation's data protection policies and conforms to The Data Protection Act 2018 and GDPR. These procedures can be found on the Intranet.

4.3. If you need to distribute information to 3rd parties in bulk electronically then advice should be sought via the Intranet IT self-help files or failing that the IT Service Desk.

4.4. Suitable controls are in place to prevent security breaches or other negative consequences, such as accessing inappropriate information. All information downloaded from the Internet will be automatically scanned for viruses, this will also include attachments which are received by external e-mail.

4.5. Automated monitoring tools are in place, and records may be accessed in conjunction with the HR Team should an investigation be deemed necessary.

Appendix C

Security

1. Disclaimer

1.1. Security is everyone's responsibility. Whilst SCRMCA IT department will configure, monitor and support all systems and services in a way that meets the National Cyber Security Centre's best practice guidance it cannot guard everyone against every eventuality. All Users are expected to exercise caution and diligence when it comes to security of information and systems. "**If you are not sure ask**" The IT department will provide advice and guidance on security matters through the intranet and the Service Desk.

2. Physical Access

2.1. Sensitive IT areas will be protected by locked doors, access to the keys or codes will be restricted to authorised personnel. Access monitoring including CCTV, may be used to enhance security of these areas.

- Sensitive areas include all areas where uncontrolled access could pose a datasecurity risk. For example, areas like server rooms and network cabinets.

2.2. All confidential and licensed material will be held in secure cabinets and only available to authorised people.

2.3. Only authorised equipment may be connected to network ports in the organisation this includes ports on IP desk phones. IT may deploy intrusion detection measures to ensure unauthorised connections are identified and shut down.

2.4. Guest Wi-Fi and HDMI cables are provided in meeting rooms to enable guests to use the meeting room facilities. There should be no need to connect a guest's PC to the corporate network or use a portable storage device which could pose a risk to SCRMCA systems and services

3. Personal and Laptop Computer Security

3.1. It is the responsibility of each user to take all reasonable precautions to safeguard the security of their device and the information contained on it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine, leaving your device in a vulnerable place such as a car or cafe and adherence to this policy.

3.2. The storage of documents on the fixed hard disks (C:\ drive) of PCs is at the Users own risk. Local drives are not backed up. The IT Department will **not** be able to recover documents lost in this way. Storage of documents on a laptop C: drive or re-movable hard drives of PCs should be for as short a time as possible to

minimise the risk of data loss. Users should use the network storage facilities provided rather than the local drive wherever possible.

3.3. As M365 facilities are rolled out and enhanced across the organisation Users will be encouraged to use SharePoint sites, One Note and Teams instead ofnetwork drives. This will greatly improve the security, version tracking and collaboration with documents being capable of recovery in more circumstances of loss. Further guidance will be made available on the Intranet as the services are rolled out.

3.4. The Information Technology Department will use appropriate tools, including encryption, to protect data in the event of loss of physical devices; this does not replace the need for users to ensure appropriate physical security precautions are taken.

4. Network Security

4.1. Developments and expectations in our digitally connected and mobile world are such that Users may struggle to understand or know what network they are connected to. The IT department will configure all SCRMCA devices that might feasibly be used out of the SCRMCA network in such a way as they will remain secure. This will include but is not limited to automatic configuration of firewalls and virtual private network (VPN) connections.

4.2. SCRMCA will follow NCSC guidance and adopt a strength in depth approach to its network security with firewall boundary controls, effective monitoring and detection of suspicious network usage.

4.3. All systems and services connected to the SCRMCA network will be configured securely so as to ensure the security and availability of all systems and data.

4.4. Should Users have any security concerns they should notify the Service Desk using the self-service portal accessed via the Intranet or failing that by calling.

5. USB Storage Devices

5.1. The use of USB and other storage devices (including but not limited to Cameras, MP3 players and mobile phones) not supplied by SCRMCA for the transfer of organisational or partners data is prohibited.

5.2. All authorised USB data storage devices will have encryption enabled.

5.3. Automated monitoring tools are in place to control and report on USB devices being connected, for example the Anti-Virus software detects suchactivity to protect the data, systems and services of the organisation.

6. Connection of Non- SCRMCA IT equipment to the organisation's network

6.1. The normal method of securely exchanging information between the organisation and its suppliers or other bodies will be through the organisations email or secure

file transfer systems.

6.2. Where automated exchanges of information are required (electronic data interchange; EDI), suitable EDI facilities must be built into the packages, products or database applications used. Responsibility for ensuring that such features are specified rests with the managers controlling the development and acquisition process for the software involved. The specification for these facilities will comply with or exceed the recommended best practice from the UK Government Digital Service (GDS)

6.3. Under normal circumstances, direct access to the organisation's IT systems by suppliers or other associated bodies will not be permitted. It is recognised, however, that where there are close relationships with suppliers involved with major parts of the organisation's business, such direct access may be required. In such cases the business case must be agreed between the requesting manager and the Head of Information Technology. This must explicitly cover the provision and proof of adequate security.

6.4. Connection of individuals or contractor's PC's to the organisation's networks by any method other than the guest network will only be allowed if prior agreement has been given by the Head of Information Technology or nominee.

7. Passwords

7.1. The username and password given to users, agents and suppliers to allow access to IT resources are for the use of the individual for whom the account is created. Passwords must never be shared with anyone, even someone from, or claiming to be from, the Information Technology Department.

7.2. If there is a need to allow someone to access information you have on the computer systems, then this can always be done by means other than password sharing. Check for guidance on the intranet or contact the Service Desk for assistance.

7.3. SCRMCA operates a complex password policy. For specific advice on passwords please read the password guidance on the intranet.

7.4. Sharing of personal passwords will be deemed a serious breach of this policy. Remember the monitoring systems used by the organisation may trace computer misuse back to an individual account and if you let someone else use your account you will be accountable for this.

8. Mechanisms for reporting actual or suspected security incidents

8.1. All users of SCRMCA have a duty to report any actual, attempted or suspected breach of IT security, including loss of physical device such as laptop or USB device, immediately. Such reports should be passed to the IT Service Desk, and suitable action will be taken.

Appendix D

Telephony / Voice & Video

1. General

1.1. The distinction between telephony and other forms of communication is becoming increasingly blurred in this digital age. Your telephone, desk or mobile, is now considered a device and can make voice and or video calls in numerous ways. Equally your PC, tablet or laptop can be used to make and receive voice and video calls. This section of the policy deals with User behaviour whatever technology they may be using.

2. System Access

2.1. Connection to voice & video services for any purpose will be through appropriate security and filtering systems, the configuration and performance of which will be the responsibility of the Information Technology Department.

2.2. SCRMCA has the right to, and will, utilise systems that makes it possible to identify and block access to specific phone numbers, regions and types of telephony services.

3. Mobile Telephony Services

3.1. It is recognised that some users are required to have access to mobile telephony services to enable effective operation of the business. The authority for issuing such services and any specific procedures relating to their use is subject to approval from the relevant line manager and budget holder.

3.2. A charge for personal use of these services will be made to the user.

3.3. There is no requirement by the organisation for staff to use their phoneswhen driving.

3.4. The equipment issued is the property of SCRMCA; it should not be tampered with or modified without prior written approval from the Head of IT or nominee. For the avoidance of doubt this includes installing SCRMCA SIM cards in personal phones and using personal SIM cards in SCRMCA phones.

3.5. The Information Technology Department will supply a phone suitable for the business requirement. A list of approved phones suitable for the organisations business requirements will be maintained by the Information Technology Department. Any variation to this list will be with the specific approval of the Head of Information Technology and will require a full business justification to be produced.

4. Monitoring of Telephony Systems

1.1 The organisation records calls made to Traveline, Gateway Hub and other specific services for training, quality management or legislative purposes. It is not the organisation's policy to monitor or record calls made to other services in such a way that the content of a given message is known, unless requested to do so by the Police orother such authorised authority.

1.2 The telephone system is monitored to ensure that it is well maintained, secure and fit for purpose.

5. Personal use and Responsibility

2.1 SCRMCA's telephones are for business use. Occasional and reasonable personal use of the telephone is permitted in the following circumstances:

- In a User's duties as a primary carer;
- To make appointments for medical or personal health reasons;
- Other brief, important matters that have to be dealt with during standard business hours.

In the event that personal use is required for any other reason explicit consent from your line manager on each occasion is required.

Appendix E

Mobile Working

1. General

1.1. Increasingly IT systems and services are being securely configured so that Usersmay work from anywhere they can get internet connectivity. This flexibly helps with collaboration across different organisations and areas as well as supporting flexible working, home working and improved work life balance.

2. Safety and Security

2.1. The Information Technology department will ensure that all devices, systems and services they provide are configured to meet or exceed the security recommendations from the National Cyber Security Centre (NCSC) and are compliant with all relevant legislation.

2.2. Users are reminded that;

2.2.1. when working externally to the organisation they should be even more vigilant with their personal security and ensure that their login credentials andelectronic devices are always kept safe.

2.2.2. Special attention should be applied when accessing sensitive information, making sure that the screen of the device cannot be overlooked by non-authorised people for example.

3. International Travel

3.1. In theory it is possible to work anywhere in the world where you can get an internet connection with the services the IT department provides however there can be issues with security, local intranet connectivity and mobile phone connectivity.

3.2. If you are travelling for business purposes and require access to your device and SCRMCA systems and services whilst you are away, you should contact the IT Department via the Service Desk as early as possible so that advice and guidance specific to your needs and travel arrangements as well as any device modifications needed to work in the destination country can be made.

4. Emergency

4.1. Should any User suspect or discover that their device or credentials have been compromised in any way including being lost or stolen they should first ensure that they themselves are safe from harm, then contact the Service Desk so that the device can be remotely disabled.

Appendix F

Social Media

1. General

1.1. Social Media is an essential tool in today's digital world. SCRMCA use social media tools in a variety of ways to engage with staff and the public.

1.2. In addition to business use the majority of users will have personal social media systems and services they use.

1.3. All Users need to be mindful when using all social media of their responsibilities for their own behaviour and ensure they do not bring the organisation into disrepute.

2. Using social media sites in our name

2.1. Only individuals who have been granted access to our official corporate social media accounts and permitted to post material on a social media in our name and on our behalf; any breach of this restriction will amount to potential gross misconduct.

2.2. All posting of materials must be in strict accordance with other SCRMCA policies and procedures including our Code of Conduct and Media Relations Policy.

2.3. The setting up of social media accounts of any sort purporting to be SCRMCA, Travel South Yorkshire or other public transport brand, or involvement in the management of such an account without the correct permission, will amount to potential gross misconduct.

3. Using work-related social media

3.1. We recognise the importance of the internet in shaping public thinking about our organisation and our services, employees, partners and customers. We also recognise the importance of our employees joining in and helping shape industry conversation and direction through interaction in social media.

3.2. To avoid major mistakes and turning a well-meant social media comment into a reputational disaster, it is important that whilst you are permitted to interact on social media websites about industry developments and regulatory issues that we manage any potential risks through adopting a common-sense approach,

3.3. Before you include a link to a third-party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.

3.4. Be honest and open but be mindful of the impact your contribution might make to people's perceptions of us as an organisation. If you make a mistake in a contribution, be prompt in admitting and correcting it.

4. Personal use of social media sites

4.1. We permit the incidental use of using SCRMCA systems to access social media websites for personal use subject to certain conditions set out below. It must

neither be abused nor overused, and SCRMCA reserves the right to withdraw permission at any time.

4.2. you must not interfere with SCRMCA business or office commitments

4.3. you must comply with organisational policies

5. Rules for use of social media (Business and Personal)

5.1. Whenever you use social media, you must adhere to the following general rules:

5.1.1. Do not upload, forward or post a link that contains any abusive, obscene,discriminatory, harassing, derogatory or defamatory content.

5.1.2. Any employee who feels that they have been harassed or bullied or are offended by material posted or uploaded by a colleague onto a social media website should inform their line manager or a member of the Human Resourcesteam.

5.1.3. Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your linemanager.

5.1.4. Do not upload, post or forward any content belonging to a third party unless you have that third party's consent. Posts that are made public are deemed to already have consent of that third-party owner,

5.1.5. You are personally responsible for the content you publish or forward into social media tools — be aware that what you publish will be public for many years. You must not discuss colleagues, competitors, customers or suppliers without their prior approval and only if this information is already publiclyavailable and known to be accurate. You must not be critical of the SCRMCA and / or its partners regarding work related matters.

5.1.6. Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details (colleagues, competitors, customers or suppliers) without their prior consent.

5.1.7. In general, all users are expected to exercise discretion in their use of Social Media. You are individually responsible for what you do. It is yourbehaviour on social media including the content you post and forward thatmust be compatible with SCRCA values.

5.2. Misuse of social media can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you personally and the organisation. You must not behave in any way that will bring yourself or SCRMCA into disrepute.

6. Monitoring use of Social Media

6.1. Employees should be aware that any use of social media (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found action may be taken under SCRMCA Disciplinary Procedures and may result in dismissal due to gross misconduct.

6.2. Where evidence of misuse is found we may undertake a more detailed

investigation in accordance with our Disciplinary Procedure.

6.3. If you notice any use of social media by other users in breach of this policy pleasereport this to the Human Resources Team.

Appendix G

Transfer of Personal Data

1. General

1.1. Anytransfer of personal data must be carried out in accordance with The Data Protection Act 2018 (DPA), the General Data Protection Regulations (GDPR), complying with organisational policies and following organisational guidance.

1.2. It is incumbent upon all Users of SCRCMA systems and services to not deliberately or inadvertently disclose personal data. To do so may lead to disciplinary procedures and could also involve legal proceedings depending on the circumstances of the breach.

1.3. Personal identifiable data is any data that can be used to uniquely identify a living individual. This includes data stored in Databases, Spreadsheets and Word Documents etc. More information about what constitutes personal identifiable data can be found in SCRMCA's Data Protection Policy available on the intranet.

1.4. Any data breaches must be reported to the Senior Information Risk Officer (SIRO) who may also inform the Information Commissioners Office (ICO) depending on the nature of the breach.

2. Record Types

2.1. Paper Records include any hard copy documents e.g. application forms.

2.2. Electronic Records covers any personal identifiable data stored in Databases, Word and Excel documents, Emails etc.

3. Transfer of Personal Data

3.1. The transfer of personal data can be the process of passing on a single customer comment to an external organisation to the batch processing of thousands of records for marketing, mass mailing purposes etc. It can also include the transfer of personal documentation or work files that contain Personal Identifiable Data (PID).

4. Batched or Bulk Transfer of Personal Data

4.1. For these purposes batched or bulk data referrers to 5 or more individual records of Personal Identifiable Data.

4.2. Unless there is an approved secure business process in place for regular transfers of data, no employee shall transfer batched or bulk personal data without first having gained approval for the transfer by completing and submitting a Request for the Batched Transfer of Personal Identifiable Data form to the Head of Information Technology or nominated deputy and receiving confirmation that the transfer is acceptable.

4.3. The Head of IT or a nominated deputy must authorise all transfers or disclosures of bulk PID from SCRMCA.

4.4. If the transfer of the data is to take place on a regular basis then the process will need to be approved by the Head of IT or nominated deputy and it will be required to be followed every time that a transfer takes place.

4.5. The employee requesting the transfer of Personal Identifiable Data will be responsible for ensuring that the transfer request is justified and that the transfer takes place in a safe and secure manner.

4.6. The Head of IT or a nominated deputy can provide advice and support to help complete the process or to help with any individual issues or concerns about the sharing of Personal Data.

4.7. The employee who discloses or transfers the personal identifiable information will be responsible for ensuring that the Request for the Batched Transfer of Personal Identifiable Data form is completed and passed to the Head of IT or nominated deputy for final approval.

4.8. All transfers of Personal Identifiable Data must be made using a guaranteed transfer method which allows the tracking and tracing of the custody of the data at any given point during and after the transfer has taken place.

5. Electronic Transfer Methods

5.1. All transfers of Personal Identifiable Information must be made or sent using guaranteed methods of transfer as set out below.

5.2. Electronic Data transfer using FTP facilities – preferably using Secure FTP (SFTP)

5.3. Secure Electronic delivery facilities provided as part of a system or application containing the data.

5.4. Secure Electronic data transfer tools provided by the IT department.

5.5. Each individual Personal Identifiable Data record must be marked with the date of export and the purpose for which it has been exported (Marketing etc.) and to whom the data has been supplied to.

5.6. Any files that contain Personal Identifiable Data must be encrypted using best practice algorithms with a strong password or passphrase using upper- and lower-case letters numbers and special characters. The password must not be included with the data set and the receiver of the Personal Identifiable Data will be notified of the password by a different method to the transfer of the data once they have been identified as the correct recipient and in possession of the encrypted data.

5.7. Proof of delivery must be received every time from the person or the organisation providing the delivery service, followed by confirmation of receipt verbally upon receipt from the intended recipient and written confirmation as soon as practicable.

6. Failure of Transfer

6.1. In the event of any failure or suspected potential failure of the chosen delivery process or due to a breach in the transfer process then the Data Breach

Process should be followed

For and on behalf of UNISON

Chair, Branch Committee	Date
Secretary, Branch Committee	Date
Chief Executive	Date

Date