STAFF ACCEPTABLE USE OF INFORMATION SYSTEMS POLICY

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

Owner: SIRO
Document ID: ICT-PL-0117
Version: 1.3
Date: March 2021
Review date: March 2023

DOCUMENT MANAGEMENT

Version	Date	Summary of Changes
1.1	October 2018	First version
1.2	March 2021	Review and Updates

Accountable Owner		Approval date
Senior Information Risk Owner (SIRO)	Chris Bally	06/07/2021

Responsible Owner		Approval date
Head of Information Governance	Peter Knight	18/05/2021

Reviewers	Role	Approval date
Policies Review Group: Russell Armstrong (policy review lead) Philip Barbrook Anna Stephenson Joanne Withey Corporate Information Governance Board - ratification	 IT Security Manager Enterprise Architect DPO & Compliance Manager DP & Training Manager	18/05/2021 29/07/2021

Publication information		
	Published (if YES, enter document location)?	**Location**
All staff	Yes	mySCC
Public	Yes	SCC website

Contents

1. Introduction

a) The purpose of this policy is to provide instructions for all Suffolk County Council (SCC) staff and Councillors on their usage of corporate IT systems and tools and handling of information in all formats.

b) This policy has been designed to enable staff and Councillors to manage information security risks to an acceptable level, whilst also recognising the flexible ways in which staff need to work: in various shared buildings, at home, on the move and on occasions using personally-owned devices.

c) The information in this policy balances the need for legal compliance (e.g. data protection law) with the business requirements of SCC taking into account the privacy rights of individuals and the practical needs of staff.

d) This policy has been designed so that SCC can reduce the cyber threats which seek to exploit staff behaviours and unacceptable usage of information systems (e.g. an attacker obtaining a password used via social media which is the same one for access to SCC or accessing SCC network using a laptop which has not been secured).

e) This policy includes at, Appendix A, a list of definitions that are used throughout the document.

f) This policy should be read in conjunction with the following documents:

- Data Protection Policy
- Classification and Labelling of Information Policy
- Information Security Incident Reporting Policy
- Password and Authentication Management Policy

2. Background

a) SCC information systems have a range of in-built technical security controls which are managed by IT and Buildings teams. But by far the most important controls are those relating to how our staff use these tools and information assets on a day-to-day basis.

b) Statistics shows that most significant information security incidents at SCC and elsewhere are due mainly to staff misunderstandings and errors. Most of these incidents can be avoided (or the impact reduced) if staff receive the right training and advice on corporate-wide information systems when they join SCC and at regular intervals afterwards and receive support in local teams on specific IT tools and **understand the corporate acceptable usage rules.**

c) Understanding acceptable usage requirements is no longer as simple as it once was because:

i. As information systems have developed over time new standalone policies had appeared in isolation (e.g. clear-desk policy, Internet policy, email policy etc.). This can be confusing, and staff may not have the time to read them all. The aim of this revised policy is to bring all these elements together into one logical place and show the linkages between them (i.e. how physical security of buildings impacts information systems and vice versa).

ii. As information systems, solutions & technology has evolved, staff find themselves using their own personally-owned devices to access or share SCC information, and lines can be blurred between home life and work life information. The aim of this policy is to give clarity as to what is acceptable and what is not.

iii. Ways of working have changed. We are now more mobile and spend more time out of the office, and some older policies did not define the ground rules for handling SCC information in different contexts such as wireless Internet 'hotspots' for example. The aim of this policy is to set out the rules for handling information and using corporate solutions in all contexts – including when business continuity plans are invoked - and not just the traditional office environment.

iv. As the mix of staff changes in SCC to meet the current challenges, there can also be a diverse set of personal and ethical views as to what is acceptable use of information systems based on where a person has worked prior to SCC (e.g. straight from further or higher education, having worked for a business or charitable body etc.). The aim of this policy is to set out what SCC has decided is acceptable for a public body which has specific compliance and other requirements. In some areas these may be necessarily more stringent than staff may have experienced before in other organisations.

v. Finally, the types of cyber security threats to our information have changed and therefore more attention now needs to be given to those staff behaviours which can have the most significant impact on our information and systems.

3. **Scope**

This policy covers all SCC staff & Councillors and external third parties.

This policy does not apply to:

a) personnel working in schools in Suffolk regardless of the way in which they are funded. Schools are data controllers (individually or as groups) with IT policies that reflect their own business requirements and information risks.

4. Roles and responsibilities

a) **Information Governance team**: has been tasked with implementing this policy and monitoring its effectiveness.

b) **Managers:** are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy. Line managers have additional responsibilities which are outlined throughout this policy.

c) **The Monitoring Officer**: is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them so as to implement this policy.

d) **Users**: all users should attend the appropriate training courses. SCC delivers modular training to all users who have access to the council's data and network. These training modules inform users of the requirements of the ICT Security Policies. All users must engage with this training and complete all mandatory modules. Line managers have a responsibility to support this training and must raise with HR if any staff member does not, or cannot, complete the training.

e) **Non-compliance with this policy** may lead to further action and investigation under the Council's Disciplinary Procedures. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

Non-compliance with this policy could also lead to criminal or civil action if illegal activities are involved or legislation is contravened. SCC will not hesitate to bring to the attention of the appropriate authorities any use of its systems which it believes might be illegal.

Non-compliance with this policy by Councillors may contravene compliance with the Members' Code of Conduct which may lead to a referral to the Council's Monitoring Officer.

f) Security incidents: all staff must report any suspected security incident via the IT Service Desk.

5. Joining, moving within and leaving SCC

a) Security clearance

i. It is the responsibility of line managers to check with HR that all relevant documentation, including any security screening and identity checks, has been completed and checked prior to the new member of staff joining regardless of whether they are temporary, permanent, or other staff.

ii. It is the responsibility of the joiner to follow the screening process. Failure to do so could lead to not being able to access SCC information systems or buildings.

b) **Staff photo identification pass**

i. It is the responsibility of line managers to arrange for any new member of staff to obtain a photo identification pass as near to the first day as possible (with temporary day pass arrangements if necessary). It should be clear which buildings the new person will need to access and the time-frame (and for this to be communicated to the buildings team managing passes).

ii. It is the responsibility of all staff to safeguard the ID badge / pass and any building access codes that have been issued to them, not to share them with anyone else and report immediately to their building reception team if it has been lost. If a member of staff suspects their pass has been misused, they must discuss this with their line manager and report it as an information security incident.

c) **Mandatory training**

i. It is the responsibility of all new staff to fully complete the mandatory online information governance training.

ii. It is the responsibility of the line manager to ensure that new staff have undertaken the above training package (ideally in the first week of joining). Existing staff will also need to complete the training and will be expected to undertake the training again at the request of their line manager or at the next scheduled deployment across all SCC staff.

iii. Failure by staff to comply with managerial reminders to complete the mandatory information governance training may mean that staff have their access to SCC systems removed, unless the Senior Information Risk Owner (SIRO) has instructed them otherwise.

d) **Issuing of IT equipment**

i. It is the responsibility of line managers to ensure that the right equipment (together with initial access rights to required services) has been ordered or requested prior to the new member of staff joining and that new staff know how to use their equipment within the context of SCC. This may include a desktop, laptop, tablet, smart phone etc. An assessment should also be made at the outset to identify whether Health and Safety issues or disabilities (such as visual stress, eye-sight impairment or Musculoskeletal) may require adjustments to official equipment and its configuration.

ii. It is assumed that new staff have satisfactory proficiency in IT *prior* to joining SCC (i.e. use of devices and passwords, Internet-browsing, use of standard word processing and spread-sheet packages etc.). SCC line managers are responsible for ensuring specific software solutions (e.g. Social Care or Fire & Rescue case management systems) and specific security controls are explained prior to such tools being used. Staff may not access case management systems until they have taken the relevant training course.

iii. It is the responsibility of all staff to safeguard their official laptop or desktop /smart phone devices by ensuring they are shut down (laptop, tablet or desktop) or screen locked (corporate smart phone) and stored securely at the end of each day. This could mean that the devices are either taken home at the end of each day or locked away in the office / flight locker or securely cabled to the desk (in buildings that permit this). Any loss of such equipment must be reported immediately to IT using the information security incident process in the IT Self Service portal.

iv. SCC equipment issued to staff has been configured to minimise cyber, information loss and other risks. Staff must not attempt to tamper with this official equipment by seeking to change hardware or software settings or bypass any security features. It is not permissible for staff to seek assistance from any person or company (other than SCC and its approved contractors) to analyse or repair or change SCC devices in any way.

v. It is not permissible for anyone other than the IT Service to disconnect and move non-portable equipment such as desktop computers, scanners, servers etc. to other locations even within a floor or building.

vi. It is not permissible for any staff to attempt to introduce and set up their own IT or similar equipment on SCC premises. This includes, but is not limited to, surveillance cameras, wired or wireless routers, printers, scanners and non-SCC managed laptops or tablets etc.

vii. It is not permissible for users to allow any third parties to use, or remotely access, SCC issued IT equipment or services without permission from IT in the form of the SCC Code of Connection process.

e) **Passwords**

i. A BitLocker encryption password will be issued to staff which relates specifically to the encryption of their laptop/tablet and they will be given a separate password that will allow them to login to the SCC network and access core systems.

ii. Upon receipt of your laptop, you must remove the label containing the BitLocker password immediately. The label must be securely destroyed e.g., shredded or, if in the office, placed in a confidential waste bin/sack. You are permitted to store the password securely until you have memorised it, but the storage of the password must always be separate to the laptop's location.

iii. Passwords must not be shared with anyone else, including your manager and IT staff. **Passwords must not be kept with or attached to the device**, because if the device is lost or stolen it will not be very challenging for the third party to decrypt it and login as you.

iv. Some job roles may require additional credentials (username and password) to allow staff to access information systems/tool. It is the responsibility of the line manager and information asset owners to ensure that such business-specific passwords are unique and relate to an individual member of staff's access. It is the responsibility of staff to safeguard such passwords and not to share them.

v. It is acceptable to write down the above passwords in a non-descript manner for a short period (e.g. in a personal notebook), until they can be memorised. But they should never be kept on, with or adjacent to the device(s).

vi. The SCC password will need to be changed at regular intervals pre-determined by SCC. It is acceptable to change the password, such as in the event of being 'locked out', using the SCC password reset tool at any time. The choice of password needs to follow the convention (right number of characters/numbers) and must not be the same as any other password you have used before, either at work or in personal life.

vii. The IT security team alone has the authority to force any member of staff to change a password at any time if, in its judgement, there is a security issue (e.g. a password has been compromised).

viii. All staff have a responsibility to report any security issues – such as possibility of password being compromised – immediately**,** by creating an Information Security Incident on the IT Self Service portal, so that the IT Security team can carry out a thorough investigation.

f) **Changing roles and extended absence**

i. When a member of staff changes roles within SCC, it is the responsibility of line managers to ensure that the access to job-specific systems and information are updated accordingly (e.g. IT access permissions rescinded).

ii. Where a person has changed roles and there is no business need to access information relating to the previous role, the member of staff should not attempt to access such information. In the event of an investigation, the onus will be on the staff member to justify the business need for such access. IT may provide managers with audit trails to show staff activity on those systems.

iii. When a member of staff is due to be absent (or has been absent) from SCC for any reason including maternity, sickness, career break, disciplinary, outward secondment etc.) for more than 90 days then IT must be notified, and all SCC equipment returned and access to all information systems ended[1].

iv. In addition to being notified by line managers about absences, IT will also run automated tools to discover which accounts are active and have up to date security patches and other necessary updates/versions. If a user's device, such as laptop or tablet, is not connected to the SCC network (wired or via SCC WiFi) at least once for a minimum period (e.g. 4 hours) in a defined period (e.g. 3 calendar months) then such devices will be disconnected from the SCC network.

g) **Leaving SCC**

i. It is the responsibility of line managers to inform IT when a member of staff is due to leave SCC no less than one week prior to the member of staff's leaving date.

ii. It is the responsibility of line managers to arrange for the handing in of all IT equipment and photo identification pass prior to leaving the buildings on or prior to the last day of work.

iii. It is the responsibility of line managers to assess whether all SCC information is filed in the correct places and that any information held outside of the office (e.g. at home) is handed in prior to leaving. Line managers must ask the member of staff to sign the Leavers' Declaration form confirming this.

iv. It is the responsibility of all staff to hand in to line managers any IT equipment such as phones, laptops, any removable media, or paper files as well as identification pass prior to leaving and to ensure that corporate information is filed in the correct places. Note: even after leaving SCC employment, individuals – including councillors - can be prosecuted under Data Protection and other laws for misusing personal and corporate data relating to a previous

[1] The end of access to SCC network and information systems does not mean that communications with such staff on temporary absences should be ended, as 'staying in touch' is important. Instead, other means should be found to communicate such as telephone calls, emailing to personal accounts, access to staff extranets and collaborative tools etc.

employer. The content in email accounts and in employee-created stores (e.g. OneDrive) will be deleted three months after leaving SCC unless there is a business need for it to be retained for a longer period. In this case an exception must be created by the line manager before the data has been deleted.

6. **Office security**

a) **Entering/exiting buildings**: when entering and exiting SCC buildings which require a photo-identification pass all staff will follow the correct procedure and will not attempt to tail-gate, force or climb over any gates or barriers. Where a pass has been left at home or there is a difficulty using the gates at entrances, all staff must ask the front-of-house security/reception teams for assistance.

b) **Use of surveillance cameras**: SCC will deploy surveillance cameras within the footprint of its buildings (including inside certain buildings) to ensure the health and safety of all staff and the security of its assets. These cameras must not be interfered with by any staff (other than the asset owner or its agreed supplier).

c) **Screen Lock devices when unattended**: all devices such as laptops, desktops or tablets must have their operating system screen-locked when left unattended for any length of time. When finishing work, such devices must be shut-down, put in a bag and brought home OR locked away in a lockable cupboard within the office OR locked with a cable (in buildings which provide and operate them).

d) **Clear desk policy**: SCC operates a clear-desk policy. This means while working at a desk/office environment paper files should be kept to an absolute minimum (especially anything which contains RED / Official Sensitive level data) and such papers must be locked away at the end of the working day (i.e. leaving a clear desk) and not left near printers, unlocked cabinets or other work surfaces.

e) **Waste paper**: waste paper with information on must be disposed of in designated secure bins (those for AMBER / RED level) information and in regular recycling paper bins for GREEN level (i.e. document does not contain personal or sensitive information).

7. **Remote working within the UK**

a) **Working on the move**: it is permissible for staff to access and view SCC information in any format (paper or digital) while on the move providing that:

i. No RED level information can be viewed by non-intended persons (e.g. adjacent seats on public transport, passers-by etc.).

ii. The device, such as a laptop, must be shut-down and placed in a bag and safe-guarded when not in use, even for short period of time.

iii. The loss of a device must be reported immediately as an Information Security Incident using the IT Self-service portal or contacting the IT Service Desk.

b) **Working from home**: it is permissible for staff to access and use SCC information up to and including RED level in any format (paper or digital) while working at home providing that:

i. "Home" is defined as a property such as a flat/house which is lockable and has at least one room which can provide a similar level of privacy to that in a designated SCC office space.

ii. Only a minimal amount of SCC paper files or printed outputs are kept at home (i.e. for next day or week of visits/meetings etc.) and should be secured when not in use.

iii. The device, such as laptops, should be shut-down when leaving your home even for short periods.

iv. Due care needs to be taken when other residents of the household are present and in shared areas of the home so that non-intended persons cannot view SCC information etc.

v. Waste paper with SCC information on should be machine shredded at home or brought into SCC to dispose of in designated secure bins.

vi. The loss of a device must be reported immediately as an Information Security Incident using the IT Self-service portal or contacting the IT Service Desk.

c) **Visiting clients and customers:** it is permissible for staff to access and use SCC information up to and including RED level while visiting clients/customers and patients in their homes or other non-SCC building in the community. This is provided that:

i. The amount of paper files brought out on visits is kept to an absolute minimum (files needed for that visit/day which should be enclosed in a bag).

ii. The SCC device being used to access or input information relating to clients is shut down when not in use and is carried in a bag.

iii. Any information viewed on screen relates to the current client (i.e. the customer being visited should not be able to view or hear about

any information that relates to another person or otherwise sensitive corporate information).

iv. Any information left at the customer's property should only be that which is designed to be safe-guarded by the customer (e.g. information left in property to assist handing over of social care tasks). If information is left at a customer's property, the SCC staff needs to explain why this is happening and what to do if the information is lost/misplaced by the customer.

v. Loss of a device while out visiting, or any other information security incident (such as suspicion that information has been viewed by non-intended persons) should be reported immediately as an Information Security Incident using the IT Self-service portal or contacting the IT Service Desk.

d) **Remote access using SCC devices & wireless 'hot spots'**: it is permissible for staff to connect an SCC device, such as a laptop or tablet, to a wireless Internet 'hotspot' using the 'Public Wireless Access' client on the device providing that:

i. The wireless hotspot is located within the premises of a business partner such as NHS, district or borough council, community interest company etc. and is intended to enable such connections.

ii. Commercial wireless hotspots (e.g. cafes, hotels) should be used with great caution because the environment is public (i.e. persons could view SCC information on screen). Staff should only use such premises in the UK when it is essential and in the case of SCC laptops/tablets only using the 'Public Wireless Access' client button and process.

iii. Staff must not use Internet-cafes where they are using another party's access device such as desktop/laptop that is provided by the 'Internet café' to access any SCC services where a login is required (i.e. do not attempt to access SCC email or other services where corporate data is displayed).

iv. It is permissible for staff to view SCC information via SCC cellular devices such as smart phones, provided they use the secure logon process. No SCC data should be saved onto them, unless explicit permission has been given by IT, as they have not been set up to be corporate information stores.

e) **Use of personally-owned devices to connect to SCC services**: it is permissible for staff to access certain SCC Internet-based systems or platforms (such as Office 365 SharePoint/Outlook or Oracle Fusion) using their personally-owned devices providing that:

i. The member of staff is content that his/her personally-owned device can be used to access SCC services for the convenience that this brings (i.e. rather than being issued with a separate SCC owned device).

ii. The personally-owned device to be used meets the minimum technical specification required for the SCC services.

iii. The member of staff understands that although 'personal life' applications and data are segregated from SCC services as far as possible, there are certain instances where SCC will require the user to follow specific instructions and/or downloading security software.

iv. Where there is a security concern, or the user is absent from SCC then organisational data held on the device can be remotely wiped. In exceptional circumstances, on the advice of the IT security manager, SCC may attempt a full wipe of data on the device (which could include the user's personal non-work data and applications being permanently deleted). This needs to be understood by staff who agree to use their personally-owned device for SCC work.

v. Such access needs to follow the agreed login process. Where services are accessed in this way, no Amber or Red level information should be downloaded/saved onto the personally-owned device.

vi. Any security incident or concern (such as suspicion that a password issued to access SCC services has been compromised or the loss of the personally-owned device used to access SCC services) should be reported immediately as an Information Security Incident using the IT Self-service portal or contacting the IT Service Desk.

vii. Where SCC credentials are being used to access a 3rd party cloud or application solution, this can only be done if the product has undergone a full Cloud Security Evaluation and Data Protection Impact Assessment.

8. **Remote working outside the UK**

a) **Where can I take & use my SCC provided laptop / tablet or smartphone abroad?** You can take your SCC work provided laptop, tablet or smartphone for work purposes to the following locations **only**:

Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and Norway.

b) Users are not authorised to take or to use any corporate devices in any country not listed in paragraph (a) above, as they do not meet the required adequacy levels for data protection.

c) **Can I access my SCC work account on my own device whilst abroad?** Yes, you can, but multi-factor authentication is required, and caution should be taken when accessing SCC data and services. You can access your work data on your own device in the following countries **only**:

Argentina, Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Ireland, Isle of Man, Italy, Jersey, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Cyprus, Iceland, Liechtenstein, Andorra, Israel, and Uruguay.

Users are not authorised to access work data in any country not listed above and this will be technically enforced where possible. For more information about the reasons for this, see Appendix B.

d) An information security incident must be logged in the IT Self-Service portal if any of the country rules are not adhered to.

e) Staff must not use Internet-cafes in the UK or abroad where they are using another party's device such as desktop/laptop provided to access SCC services (i.e. do not access SCC email or services where corporate data is displayed using the computer equipment provided in the Internet café or similar shared facility).

f) Paper files should be kept to an absolute minimum and should not contain any customer/client personal data while abroad. If in exceptional circumstances sensitive personal or otherwise RED level information needs to be taken abroad then this needs to be agreed by a Head of Service acting on the advice of the Head of Information Governance.

9. **Removable media**

Removable media should be avoided as far as possible, with preference given to other forms of remote access and secure transfer of data. However, where there is clear business need supported by a head of service then such media can be used providing:

a) The media meets the technical specification (e.g. fit into laptop/tablet ports).

b) Staff follow any on-screen prompts which a) encrypts data and b) scans the data for malware.

c) The transfer of data from SCC to another party using removable media should be avoided as far as possible. If removable media is used as there

is no secure way of electronically transferring the data safely e.g. there is too much data, the data on the media must be encrypted and sent via a tracked postal service.

d) Any removable media that is no longer required, and which may contain SCC data, must be either handed in or sent to IT Customer Service using internal courier for secure destruction.

e) The SCC IT Security manager reserves the right to disable any type of removable media if it poses unacceptable security risks.

10. **Use of email and messaging tools**

a) **Email:**

i. Staff will be provided with an individual SCC email account. “Individual” means an email account with an address that includes your first and last name and ‘@suffolk.gov.uk’.

ii. The individual SCC email account must only be used by the named member of staff and access must not be shared with anyone else.

iii. The SCC email address/account must not be used to send or receive messages relating to non-SCC business activity.

iv. Personal or non-SCC email accounts must not be used for SCC business (other than the business continuity circumstances in section below).

v. The SCC email address must not be used to register yourself for services that do not relate to SCC business (i.e. not linked to personal social media or leisure websites).

vi. SCC email accounts can be used to send all types of information in the body of the email and/or attachments, but if it is deemed to be RED/OFFICIAL-SENSITIVE then the OFFICIAL-SENSITIVE marking feature must be applied prior to sending the message.

vii. Where personal data needs to be sent via email all staff should keep the amount to an absolute minimum (i.e. one email and its content relates to just one person as far as possible) and take advice if large amounts of personal or otherwise sensitive data needs to be sent.

viii. All staff have a responsibility to avoid opening and actioning messages which appear suspicious and should be dealt with according to the spot it, report it and delete advice from IT Services. SCC email must not be used to send any content which is illegal, abusive, threatening, which constitutes spam or chain-mails or would bring the council into disrepute. If a member of staff receives

such email, then it should be deleted and not forwarded on to anyone.

ix. **Health and safety of staff:** If any such message is targeted at individual members of staff and could have health or safety impacts (e.g. a threat to a member of staff) then line managers must be informed.

x. All staff have a responsibility to report an information security incident where they feel an SCC email account has been compromised in some way or if they have inadvertently downloaded or tried to download something malicious or suspicious via email.

xi. Email should be used as means to communicate and must not be used as a record repository (see records management below).

b) **Instant messaging, video and photography**:

i. It is permissible to use SCC's Microsoft Teams messaging tools for sharing any kind of information including RED/OFFICIAL SENSITIVE, either via the written Chat and Post tools or via the video and audio calls function[2].

ii. All communication using these tools should use professional language, and if any notes need to be kept of meetings where one or more SCC staff is using Teams then such notes need to be kept in the usual way (i.e. exactly in the same way as in physical face-to-face meetings).

iii. No other form of instant messaging / video conferencing tool should be used for SCC business. If an external partner with a different video conferencing tool asks for staff in SCC to take part, then it is the responsibility of the SCC participants to check with IT whether this is possible on technical and security grounds and whether it is suitable. SCC staff who are taking part in such external video conferencing sessions should only provide information up to AMBER level. But Teams should be the preference and if a 3rd party wants to use another meeting solution ask if they will accept an SCC Teams request to host the meeting.

iv. Unless agreed by your Head of Service and risk assessed through the data protection impact assessment process, no personal instant messaging tools (i.e. those linked to personal non-work social media) can be used for SCC business.

[2] SCC does **NOT** corporately need to keep audio or video transcripts of outputs from Teams for Business meetings/instant messaging sessions, so it is the responsibility of the meeting host to keep official minutes or to record the meeting etc.

v. No personally-owned portable cameras or smart phones with cameras can be used to hold or send SCC work related photographs unless it is for GREEN level information. If there is a business requirement for photography for AMBER or RED level information, then the business unit needs to risk assess and procure suitable equipment and agree how such data can be transmitted and the format in which it can be held in SCC information systems.

11. Telecommunications

It is permissible for staff in SCC to use the following to communicate verbally with others using:

a) Fixed telephones in SCC offices.

b) Fixed telephones in partner offices such as other councils, NHS, Police etc.

c) SCC mobile phones[3].

d) The use of personally-owned non-work fixed and mobile phones are permissible for SCC business provided they are only for verbal conversations by mutual agreement of SCC staff and line managers.

e) Staff should not attempt to move/export any data contained on SCC mobile phones such as contact lists onto any other device.

f) Text messages that relate to SCC business should not be sent from/to personally-owned mobile phones unless GREEN level information).

g) **FAX:** It is not permissible for SCC to set up or use FAX for SCC business (other than business continuity section below), as they are deemed an insecure method of transmitting data.

h) It is not permissible for SCC to set up or use two-way analogue phones for SCC business (other than business continuity section below)

12. Use of Internet

a) Browsing sites

i. All staff may access the public internet using SCC devices either in the workplace, in the community, on the move or at home.[4]

[3] The content of text messages should have little or no personal data and no higher than GREEN/AMBER level.

[4] All Internet activity is logged and recorded, so in the event of performance investigation on staff Internet usage data (in terms of time, and type of sites visited) can be made available by IT (see policy on staff privacy etc).

ii. All staff may use SCC computing resources (devices and network) to browse the Internet for leisure purposes during breaks, at the discretion of line managers, provided it does not interfere with work or disrupt other staff (i.e. having audio on). Passwords used to access such non-work sites (e.g. banks, personal email accounts) must be different from those used for SCC computing resources and services.

iii. Staff must be aware that the following content is considered inappropriate and should not normally be created, accessed, or stored on any IT facilities or equipment:

a) Sexually explicit content.

b) Material that gratuitously displays images of violence, injury or death.

c) Material that is likely to lead to the harassment of others.

d) Material that promotes intolerance and discrimination on grounds of age, disability, gender, gender reassignment, marriage and civil partnerships, pregnancy and maternity, race, religion or belief, sexual orientation.

e) Material relating to criminal activity, for example buying and selling illegal drugs.

f) Material relating to any other unlawful activity e.g. breach of copyright.

g) Material that may generate security risks and encourage computer misuse (except where it is strictly and necessarily required for your work, for example audit activity or other investigation.

iv. You must not use your Internet enabled user account to:

a) Subscribe to, enter, or use peer-to-peer networks e.g. Darkweb or TOR.

b) Install software that allows sharing of music, video, image or other in breach of copyright materials.

c) Subscribe to, enter, or use online gambling or betting sites.

d) Subscribe to or use “money making” sites such as “paid to click”, “paid for easy tasks” or “paid to create content” sites.

e) Access the Internet via SCC network to run a private business.

v. The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. Such material would include data, images, audio files or video files the transmission of which is illegal under UK law, and material that is against the rules, essence and spirit of this and other Council policies.

vi. Where a member of staff attempts to access a legitimate site and finds that it is currently blocked as it has not yet been categorised, the onscreen instructions should be followed to allow our service provider to review & categorise the site.

vii. Social media usage by staff in SCC for administering SCC business is covered by the SCC Social Media Policy, including guidance on how to use it safely. Where staff use social media in their personal lives, they should be aware of the council's Code of Conduct if they refer to their role at SCC and Councillors should be aware of the Members' Code of Conduct in this respect.

b) **Downloading software and applications**

i. It is not permissible for staff to attempt to manually download or run any software from the Internet onto any SCC device. This includes desktops, laptops, smartphones or tablets. If new applications or updates are required, then this must be ordered via the IT Self-Service portal.

ii. Where a member of staff has inadvertently downloaded software or an application or enabled something to happen to file types by clicking on something then this should be reported as an Information Security incident in the IT Self-Service portal so it can be investigated immediately.

iii. It is not permissible for staff to attempt to change any standard settings on devices or attempt to disable any security features (e.g. anti-virus).

iv. All staff must follow SCC IT instructions, whether via automated message or other route, to download security updates/patches/versions which are there to safeguard the entire SCC network, data and assets.

v. Staff must not make online purchases or enter into any contracts on behalf of SCC without the authority of the approved procurement procedure.

vi. **Social engineering:** all staff should take reasonable precautions against following instructions from non-SCC staff by phone, email or

other channel (i.e. social engineering attacks) by being familiar with SCC processes from induction and other training (i.e. how to contact SCC IT and query a suspicious phone call etc.).

13. Storing staff personal information at SCC

a) SCC information systems are designed so that only its corporate information – including personal data about customers and staff – are held on them. They must not be used for holding information that relate to what staff do outside of work (e.g. do not file information on your family, friends, social life, personal finances, personal photographs, music files, information on other jobs, hobbies etc.)[5].

b) The exception is that personal information which is generated during the course of working for SCC which employees co-own or generate themselves but is still related to their employment. This information can be legitimately filed in record repositories where the employee has a higher degree of control over and access is limited to individual employees. This includes (list not exhaustive):

   i. Copies of annual appraisal and development plans.

   ii. Correspondence about personnel matters in SCC (e.g. maternity, health, terms and conditions).

   iii. Correspondence generated where Trade Unions membership relates to employment at SCC.

   iv. Documents relating to professional activities which overlap with SCC (e.g. CVs, registration, accreditation, professional exams, conferences etc.).

c) Those with line management responsibilities should keep information about the staff they manage in their 'personal' files to an absolute minimum and be mindful that such information may be disclosable in the event of Subject Access Request (SAR) or other legal request.

   Such information should be filed in:

   i. Named 'OneDrive' which is designed to hold such information which the employee would consider 'personal' in a work context.

   ii. Designated personal drives for digital files.

   iii. Paper copies filed at home.

[5] While held on SCC systems, such information can still be made accessible for authorised purposes (e.g. when staff member is absent/business continuity or because of an investigation). When employees leave SCC, employee-created personal information on SCC systems will be deleted within three months after leaving the organisation.

14. Access, storing and sharing of SCC information

a) **Access permissions:** all staff should be able to access and share the information they need for their role(s) in SCC[6].

i. Business units will have their own specific permissions based on roles and other criteria (e.g. for contractors/temporary staff), and line managers have a responsibility to explain them to their staff.

ii. All staff need to be able to demonstrate that any access to data in SCC systems is:

a) legitimate (i.e. you have a relationship with the customer/client).
b) time-bound (your current role and current case-work means it is necessary, and
c) proportionate (i.e. you can justify the amount and range of data if challenged in the event of a privacy investigation).

iii. Access and actions on SCC systems - which all have a form of audit trail - should always be traced to individuals, and staff should not share credentials/passwords or allow others to view or change data using their account (i.e. non-repudiation).[7]

b) **Filing corporate information and records**

i. All staff must file information that they create or receive during their day-to-day work in the appropriate corporate record repositories. One or a combination of the following must be used:

a) Team shared drives with a structured folder structure.

b) Team SharePoint site with structured document libraries.

c) Team case management system (i.e. to hold information on customers/clients/ buildings etc).

d) Specific local information systems designed to hold structured information (such as a database).

ii. **Email**: Staff must not use email as a records management system and should file what is needed to be retained in the above repositories and keep the amount of data inboxes to an absolute minimum.

[6] Not all access permissions can be upheld by technical permissions (i.e. just because the IT system or service allows you to view data does not mean that you have permission to access it).
[7] Having robust data to show that X and Y took place or did not take place by a particular person/role at a particular time.

iii. **Use of non-personal accounts:** staff must not file SCC information onto personal non-work (e.g. such as emailing to personal email accounts or uploading content onto social media or file-sharing tools).

Staff must not create any new paper files (unless in exceptional circumstances agreed with Strategic Information Agents). Any temporary papers printed or hand-written notes for convenience must be securely destroyed if they contain AMBER or RED level information at the earliest opportunity (e.g. once formal minutes have been filed).

iv. **Paper files:** legacy paper files must be locked away when not in use within SCC buildings and should not be left on desks or other work surfaces at the end of the working day.

v. **Payment card and financial details:** staff must not write down, digitally store or send payment card or other financial details such as credit card numbers. The only exception is where data is being inputted directly into the approved PCI DSS secure card payment system or an exception permitted by SCC Finance. Any member of staff who receives such payment card data (e.g. in an email or paper mail) or becomes aware of such data in SCC information systems must report this immediately as an Information Security Incident using the IT Self-Service portal.

c) **External information sharing**

i. All staff need to share information - including personal data – with SCC colleagues and external partners where it is lawful and there is a clear business need to do so.

ii. All staff have a duty to query if they are unclear on whether they should be sharing data outside SCC.

iii. Line managers, service managers and Strategic Information Agents must be able to explain the business justification (e.g. should be documented in information sharing agreements, contracts etc.) and instructions on how to share the information (i.e. the tools such as email, the volumes and formats and security controls). Guidance is available on the My SCC Intranet page: https://suffolknet.sharepoint.com/sites/myscc/myjob/Pages/Information-Sharing.aspx

iv. In all cases personal data should either be **pseudonymised** or **de-identified** (i.e. so a non-intended person cannot easily identify persons) and/or **encrypted** (i.e. cannot be read either while it is being transported or as a file ‘at rest’) or the amount of personal data to be kept to an absolute minimum prior to sending.

a) Where paper files containing RED level information are to be sent, they should be double-enveloped and tracked, so that the location and delivery status of the envelope can be verified unless a head of service has risk assessed and has agreed another method.

b) Where removable media (such as memory sticks) are to be sent from SCC, the data must be on SCC encrypted removable media.

c) Email should be avoided as far as possible as a means of sharing high volumes of personal data (i.e. data on many people within a single email, or significant amounts of data on one person/family).

d) Where data is to be shared using an online file-sharing tool, then it must be one which has been approved by SCC IT Security and has the appropriate controls in place.

v. In all cases, regardless of the information sharing tools used, staff need to be clear on:

a) Who transferred the data (identity of the person in SCC).

b) When it was transferred.

c) The destination and evidence that it was received and to report an information security incident without undue delay if you suspect that data has been lost, misdirected or compromised.

15. Business continuity

a) Where a member of staff is not available for any reason (e.g. sickness) SCC must be able to access all the information that the person would normally access while at work on SCC systems – including individual SCC email account, SCC OneDrive, SCC shared drives, SCC SharePoint and paper files – for business reasons. The process to be followed is:

i. The line manager can make a justification for a limited period.

ii. The line manager makes a request to IT to allow access to a named person to access the information systems for a limited period.

iii. In the event of access to OneDrive or any of the information that is employee-related or is contentious then advice should be sought from the Data Protection Manager. This is to ensure that the balance between business need and the privacy of correspondence of staff is considered.

b) In the event of a business continuity issue and/or invoking of business continuity plan the following are permissible:

   i. Staff can be contacted using their personally-owned email accounts and telephones. It is the responsibility of all staff and line managers that such out of hours contact lists are kept up to date.

   ii. Specified paper files and SCC encrypted media can be brought to other working environments including home in the event of an IT outage.

   iii. Exceptionally, staff can use their own personally-owned equipment to keep temporary records and for other tasks as set out in division business continuity plans.

16. **Security issues due to staff misuse of systems**

a) All staff are responsible for reporting any incident[8] that they become aware of which impacts on the confidentiality, integrity, or availability of information – by immediately logging an Information Security Incident on the IT Self-Service portal or by contacting the IT Service Desk.

b) Depending on the actual or potential impact of any non-compliance with the Staff Acceptable Use Of Information Systems policy, the following will be decided by IT security management in consultation with line managers and possibly Information Governance at any time:

   i. Suspension of access to some or all SCC systems and services.

   ii. Suspension of access to some or all SCC buildings.

   iii. Recall of equipment issued to staff to enable forensic analysis.

   iv. Recall of any information in any format such as paper files which may be held by staff.

c) The above action will be taken in the interests of protecting SCC systems or preventing further impact regardless of the circumstances (malicious and non-malicious activity on SCC systems).

d) Where any information security incident is due wholly or partially because staff did not adhere to this usage policy on information systems then the following will apply:

   i. Line managers and/or Strategic Information Agents will carry out an investigation.

[8] An incident relates to information that is in written, spoken or electronic format (see Information Security Management Policy for more details).

ii. In the case of potential breaches of personal data, the Data Protection Officer will advise and liaise with Information Commissioner if necessary.

iii. IT Security management may provide technical (e.g. audit trails) and other data.

iv. Staff involved in the incident will have an opportunity to explain the circumstances, including why part of the policy was not adhered to.

e) SCC's Senior Information Risk Owner (SIRO) can arbitrate in the event of a dispute between whether the action taken to deal with the risks relating to staff misuse of systems is proportionate.

f) In the event of potential misuse involving Councillors, the SIRO must consult the Assistant Director Governance, Legal and Assurance.

g) The SCC HR team - following its process - will decide with line managers whether any disciplinary action is to be taken (in the case of gross misconduct this could lead to dismissal). IT security team will provide any necessary technical data to support this, as well as evidence of staff cooperation during its investigation (e.g. handing in equipment and providing details of the incident promptly, not attempting to access systems when asked etc.).

h) In the case of any malicious activity, all staff need to know that over and above SCC disciplinary procedures relating to not conforming to the staff information systems usage policy, action could be taken against them as individuals under GDPR/Data Protection Act (2018) and Computer Misuse Act (1990) or other law.

APPENDIX A

Terminology and definitions

1. **'Staff' or 'member of staff'** for the purposes of this policy means anyone directly employed by SCC or anyone engaged in work for SCC in any capacity (i.e. regardless of their tenure, or working via an agency, contingent workers, inward secondees, volunteer etc.), who is given access to SCC computing resources and/or SCC information to carry out work for or on behalf of SCC as a legal entity and a data controller as defined by GDPR/Data Protection Act (2018). This should also include suppliers' employees where such persons are actually given access to core SCC information systems (i.e. login to the network, laptop, email account etc.).

2. Although Councillors are not SCC 'employees' or 'staff' they are also within scope of this policy where they are given access to SCC information systems in order to carry out their Council business. **Note:** where Councillors have another external role (e.g. councillor for district etc.) then they need to conform to the policies and procedures of that legal entity in regard to its information. Similarly, out of scope is the information and information systems which Councillors manage outside of SCC as data controllers (e.g. personal home computers and files kept on residents or political activity).

3. **'Information Systems'** primarily relates to staff use of IT such as network, infrastructure, computing devices and specific digital tools, but also includes the acceptable use of information in any other formats such as paper files. **Note:** SCC's dataset assets should be owned by specific business units as per the SCC Dataset Register, even though they may be supported corporately by the SCC IT team.

4. '**SCC-owned information'** any information held by SCC to perform its business – which includes HR-type personal data on staff - remains SCC-owned information regardless of whether it is accessed by a SCC-owned device or a personally-owned device (i.e. a device such as a laptop or smart phone which is owned and controlled by staff) and regardless of how it is stored.

5. **'Personally-owned information'** is that information which staff have obtained or created which is not relevant or necessary to SCC business and relates to their life outside SCC and should not be stored on SCC systems.

6. **'Personally-owned device'** for the purposes of this policy is defined as items of equipment such as phones, laptops and tablets which are selected, paid for, maintained and controlled by individuals primarily to help them in their personal non-work lives. Increasingly, these devices can also be used to access some SCC services (e.g. email and SharePoint). This is often known as ***'Bring Your Own Device'*** (or BYOD). This policy sets out the ground rules for such access.

7. **'Information Classification'** refers to the SCC traffic light approach which is defined as:

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
GREEN	No Impact - Information formally made public by SCC or information which would have no impact on privacy, business, or corporate reputation if it was to be put into the public domain by any other means.
AMBER	Strictly internal or agreed partners - SCC corporate information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - This could also include customer names, addresses and client numbers that pose little or no risk to privacy.
RED **OFFICIAL-SENSITIVE**	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity. gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families
	Employee & partner personal data - personal data on employees of SCC and its partners. This includes details about ethnicity. gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality.
	Corporate information which would have a significant impact on the reputation or business of SCC it is was seen by non-intended recipient because of commercial, legal, fraud, investigatory or areas where confidentiality is necessary.
	Special category data as defined under data protection law (UK GDPR and DPA 2018) i.e. personal data revealing **racial or ethnic origin;** personal data revealing **political opinions;** personal data revealing **religious or philosophical beliefs;** personal data revealing **trade union membership;** **genetic data;** **biometric data** (where used for identification purposes); data concerning **health;**

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
	data concerning a person's **sex life**; and data concerning a person's **sexual orientation.** Note: personal data about criminal allegations, proceedings or convictions falls under separate legislation but is classified as red level data.

Appendix B

Working outside the UK – reasons for restrictions

1. **Data protection law (UK GDPR and DPA 2018)**: SCC owned personal data must not be transferred or taken to countries which are not deemed to be 'adequate' under data protection law (see page 14 for the list of 'adequate' countries). This is because countries deemed not to be adequate do not meet the minimum levels of protection required under the law for personal data.

2. **Encryption technology**: the movement of 'dual use' technology, such as 'military grade' encryption is restricted and managed by the international Wassenaar Arrangement (the Arrangement). This arrangement allows the use/movement of certain dual use technologies so as to not impede commercial and personal travel. The arrangement is a secondary control to data protection law, because some countries who are deemed to have an adequate data protection regime do not recognise the free movement of dual use technology.

   This means that in countries who are not part of this Arrangement it is illegal to bring in encrypted devices and this could result in local law enforcement intervention, personal risk to the traveller or confiscation of SCC devices and the data contained therein.