Using Systems and Data Policy

Contents

1. Overview / introduction

All users of the Council's ICT services have a duty to protect the systems, information and data that they use. There is an equally important duty to share information appropriately where this is in the interests of service users (eg where sharing information with partners in health or the police will protect the wellbeing of individuals).

This policy explains your responsibilities in relation to use of the Council's systems, information and data, and how you must use them in such a way that the Council can fulfil its obligations to keep sensitive and personal information secure and deliver high quality public services.

We also have to meet legal and regulatory standards for information security, including:

- Data Protection Act
- Computer Misuse Act
- Freedom of Information Act
- Obscene Publications Acts

If we don't protect the information we use or if we fail to comply with legislation, we could face substantial fines and damage public confidence in us. Our access to essential data that is shared with us by government departments, agencies and other partners to deliver our services could also be taken away.

Staff who do not comply with this policy may be subject to disciplinary action under the Council's Code of Conduct (refer to the Council's Disciplinary Policy and Procedure for details of this).

Any misuse or abuse of Council supplied ICT services or equipment by Members is a breach of the Council’s Member Code of Conduct.

Audience

This policy applies to all users of the Council’s systems and data, including:

- Members of the Council
- directly employed staff
- temporary workers (including agency workers, contractors and consultants)
- third parties / any other users accessing the Council’s ICT resources (including suppliers, partners, staff working in shared service arrangements, work-experience staff, students)

2. Keeping information safe

This policy explains your duties and obligations for keeping sensitive and personal information secure. It also outlines related Council policies and procedures which you need to comply with.

2.1. Why is this important?

We are trusted with handling sensitive and personal information from a range of citizens, staff, partners and suppliers. We all have a responsibility to keep this safe. If we don’t, people and services could be put at risk.

The Council’s ICT service is responsible for the implementation, maintenance and management of technical security controls defined in separate ICT security policies. However, most data breaches happen when staff misplace information (eg laptops, papers etc), mistakenly share it with the wrong people (eg by email or fax), or don’t dispose of it safely.

This means that we all have a vital role to play in keeping information safe.

2.2. Requirements

To keep the Council’s information secure when using its systems, information or data, you **must**:

2.2.1. Make sure you understand and comply with this policy and any other policies, guidelines or legislation specified within it when using the Council’s systems and data.

2.2.2. This includes the policy and guidance for use of social media and other online posting in section 4.2.3 below.

2.2.3. Comply with the following policies and procedures:

- the Council’s Information Classification and Marking Policy - this explains how you must classify and mark information that you have access to
- the Council’s procedures for data protection, including reporting information security breaches
- the Council’s records management policies and procedures
- all relevant information sharing agreements when handling data that belongs to a third party organisation (eg government departments, police, NHS partners etc)
- other relevant policies which relate to your area of work, such as those relating to

the Regulation of Investigatory Powers Act (RIPA)

2.2.4. Never attempt to circumvent the security arrangements that have been made to protect the Council's information.

2.2.5. Alert your manager if you believe there has been a breach or potential breach of this policy. Members should alert the Member Services team.

2.2.6. Contact the Council's ICT service if you have any questions about this policy or how to comply with it. Members may also ask the Member Services team for advice and guidance.

2.2.7. Make sure any staff you manage or third parties you have responsibility for (ie by sponsoring their access) are:

- aware of and follow this policy
- suitably trained and have any relevant resources made available (eg appropriate equipment, secure disposal facilities etc)
- provided with, and understand, any changes or updates to this policy

2.2.8. Take reasonable care to protect access to the Council systems, information and data that you have access to, including ensuring that you:

- never share your account password or access to your account with other people (including managers, other members of staff, or with family members and friends)
- never use someone else's account to access the Council's systems, information or data

Be aware that the Council will monitor the use of the communications tools and services that it provides to ensure compliance with this policy and other legal or regulatory requirements. This includes a record of the websites you visit (or attempt to visit) which can be provided to your line manager (or Member Services where these records relate to Members) if inappropriate use is suspected.

By using Council facilities you are accepting that your use is monitored. A disclaimer is automatically attached to each outgoing email to let external contacts know about this monitoring.

2.2.9. Where there is a genuine business need to access information in another user's account or device (eg emails or files in the event of someone not being available due to sickness or annual leave, or for an investigation) or to review monitoring information, a written request approved by a Director (for Members this should be the Council Monitoring Officer) should be submitted to ICT. ICT will only process properly authorised requests and will keep a record of these.

3. Use of devices

This policy explains your responsibilities relating to any device that you use for work (eg laptops, mobile phones, tablets, etc). This includes all devices you have been provided with by the

Council (work devices) and also any personal devices that you use for work purposes / Council business.

3.1. Why is this important?

The option to use a range of devices gives you greater flexibility wherever and whenever you need to do your work. However, you are responsible for making sure that any work-related information which you access or store on any device you use is kept secure at all times.

If you don't take the necessary steps to protect work-related information by following this policy, it could put our customers and services at risk.

3.2. Requirements

3.2.1. General principles

For any device which you use to access or store the Council's information (including phones, tablets and cameras), you **must**:

- take reasonable precautions to protect it from unauthorised access, misuse, damage or theft
- make sure devices are locked and protected by a passcode or password when left unattended (if this function is available on the device)
- notify the ICT Service Desk or Out-of-Hours Service immediately if your device is lost or stolen so they can take appropriate steps to protect your account and any information stored on the device - you must not delay doing this as it could lead to sensitive information being lost (Members may also report lost or stolen devices to the Member Services team, who must notify the ICT Service Desk / Out-of-Hours Service immediately)
- report security concerns in line with the Council's security breach procedures if you believe that unauthorised people may have seen or accessed work-related information or data
- be aware of your environment and not access personal or sensitive information where it could be seen by unauthorised people (eg in a café or on public transport)
- use suitable security equipment (eg a 'Kensington Lock' or lockable storage) to secure equipment in areas that are not protected by access controls (eg swipe access)
- never use public printers or public cloud print services, as this could result in printouts of sensitive information being lost

3.2.2. Work (corporate) devices

During work hours, the Council expects you to use its resources to help you with your job and for business purposes. Reasonable personal use of work devices is permitted provided it complies with this policy and any associated policies and standards specified in it.

When using a work-issued device, you **must**:

- make sure you are using the latest operating system and security software - if you don't know how to download or install these, contact the ICT Service Desk
- make sure that your use of internet / mobile data is within reasonable limits (for example, you **must not** use the Council's internet / mobile data services to stream large videos and **must not** use the Council's mobile data services for extended

internet connection from PCs / laptops – also known as ‘tethering’). Excessive use will result in costs being recharged and may also result in the service being cut off
- never allow other people, including family members, to use corporate equipment that has been issued to you
- never install software that is not from a trusted source, as this could introduce malware and information security risks to the device - if in doubt, you must contact the ICT Service Desk for advice
- never install software without complying with copyright and/or licensing requirements
- be aware that the Council is not responsible for, and does not support, any personal applications that you install on the device
- be aware that the Council is not responsible for, and does not support, any personal data stored on the device
- be aware that the Council may delete any personal data or applications that you have installed
- return all work-issued ICT equipment to ICT when you stop working for the Council / stop being a Member, or if required to do so for any reason

3.2.3. Personal devices

When using a personal device for work purposes, you **must**:

- be aware that the Council remains the owner of its information, regardless of whether you store, process or transmit it on your personal device
- be aware that the Council is not responsible for, and does not support, any personal devices
- be aware that if your device is lost or stolen, the Council will take reasonable measures to protect any work-related information that may be stored on it
  - If necessary, this includes deleting (‘wiping’) all data on the device where this is enabled when you connect to the Council's systems. The Council does not accept any liability for any loss that you incur as a result (eg through loss of personal data on the device).
- download available software updates promptly and use suitable anti-virus protection so your device and any information held on it is protected against vulnerabilities
- never use non-standard versions of a device’s operating system software (eg you must not ‘jailbreak’ or ‘root’ the device)
- use an account that belongs to and is unique to you
- protect your device with a password that complies with the Council’s protocols (as explained when setting up your password for the first time):
  - eight characters long and contains numbers as well as letters (PCs and laptops)
  - five characters long (phones and tablets)
- never download sensitive or personal information onto a personal device (this is especially important for any personal information or information marked OFFICIAL - SENSITIVE).
- never use shared or public computers unless they are protected by an individual account that is used to access the computer, with a password that only you have access to.

3.2.4. USB removable media

When using USB removable media, you **must**:

- only use encrypted USB media devices issued by the Council
- do not use a USB device for general storage (they should only be used for a specific purpose and when there is no other alternative available)
- delete your data from the device as soon as it is no longer needed
- never copy or store third party data (eg government data marked OFFICIAL or OFFICIAL - SENSITIVE) on a USB device without getting explicit written consent for this (eg as part of an Information Sharing Agreement)
- never leave removable media unattended in an unsecure location

4. Use of communications tools and services

This policy explains your duties and obligations when using digital tools, services, applications and extensions that are provided by third parties (eg Trello, Doodle, Dropbox etc).

4.1. Why is this important?

The Council allows staff and Members to use a range of communications tools and services to carry out their work, including online services provided by third parties. This means you can use such tools to plan, manage and deliver your work.

While this gives you the flexibility to use different services, you are responsible for making sure that any work-related information you use is kept secure at all times. If you don't take steps to protect work-related information while using such tools, it could put people and services at risk.

4.2. Requirements

4.2.1. General principles

When using any communication tools, services, apps or extensions to access or store the Council's information, you **must**:

- be aware of, and comply with, guidance provided on the intranet for use of specific tools provided by the Council (eg secure email services, *myoffice* etc) and the business processes for your service area
- never attempt to access Council systems or information for which you do not have authorised access, or which you ought not to have access to (eg if you discover you are able to access files that should not be available to you)
- comply with the Information Classification and Marking Policy (which explains how you must classify and mark information that you have access to) and only use tools that are suitable for the classification level of the information you are accessing or handling
- be aware that other organisations may use different information classification and marking schemes, and that you are responsible for making sure information is handled in line with the Council's policies and procedures, including any information sharing agreements that may exist with partners
- be aware that applications or services that are not provided by the Council may have lower levels of data security and privacy assurance - you must only use Council-assured applications and services for sensitive and personal information
- be aware that agreements or contracts entered into electronically (eg by email) are as binding as written documents (it is your responsibility to ensure that the content of communications are correct)

- take reasonable care to ensure that your communications are addressed / directed to the intended recipients (eg making sure that you use the correct email addresses)
- take reasonable steps to make sure that the person you are communicating with is who they say they are and that they are authorised see the information you are sharing
- take reasonable care when communicating with untrusted and / or unknown contacts
- never click links to URLs (web addresses) or open attached documents received from untrusted or unknown sources or contacts
- never send sensitive or personal information to your personal email account, personal cloud storage service (eg Dropbox, Box.com, SugarSync etc), or other services or applications that are not provided by the Council (eg Trello, Doodle etc)
- never distribute information that is offensive or in any way breaches the Employee Code of Conduct or if you are a Member, the Member Code of Conduct
- do not use Council systems for sensitive personal communications such as medical information or communications with a Trade Union representative. Any email may be monitored and there can be no guarantee of privacy
- do not use Council facilities to circulate unsolicited information to colleagues. This includes circulating information on campaigns and activities not related to the work of the Council

4.2.2. Instant messaging, SMS (‘text’ messages), video chat and telephone

When you use communications services (eg phone, SMS, Google Hangouts, Skype etc), you **must**:

- make sure you can’t be overheard if you are discussing information that is sensitive in any way (eg you must never discuss sensitive or personal information in a cafe or on public transport)
- make sure your camera isn’t positioned in such a way that it could accidentally film sensitive documents or computer screens on nearby desks
- make sure your microphone isn’t positioned so it can pick up sensitive conversations taking place nearby
- check if the conversation is being recorded. If it is, you must treat the recording in the same way as written communication (ie by following the Information Classification and Marking Policy)
- update any appropriate business systems so that there is a record of any points discussed / decisions made where required as part of your business processes

4.2.3. Social media and other online posting

When posting content online (eg comments, status updates, photos, links, videos etc), you **must**:

- never post information or express views that breach the Council’s Code of Conduct (or for Members the Member Code of Conduct), are disrespectful to others or could bring the Council into disrepute
- be aware that you are personally responsible for all content that you publish online
- never post sensitive or personal information which may put individuals or the Council at risk
- never share sensitive (including commercially sensitive) information or personal

information on a public forum or other online service, unless it has been assured by the Council as a safe way to share such information

- make sure you have permission to publish content that may be protected by copyright, fair use or financial disclosure laws
- behave appropriately and professionally, with the understanding that you are representing the Council when using your work persona
- understand that your comments may be associated with your role with the Council even when using a personal social media profile
- alert the Council's Communications Team immediately if the media contact you about anything you have posted online, or if other groups / individuals respond to anything you've posted online in a way that may be contentious or have the potential to bring the Council into disrepute
- never appear to speak on behalf of the Council without authorisation from the Councils Communication Team

Additional guidance for Members

- It is recognised that Council Members may wish to use social media / online posting as part of their political roles. Members are personally responsible for any statements made and must always ensure that they comply with the Member Code of Conduct.
- Members must be be aware that anything they post on social media could be taken as being the official position of the Council. In particular Cabinet Members should take particular care when posting on issues over which they have Cabinet responsibility, especially when there is ongoing consultation or key decisions outstanding.

4.2.4. Fax

When sending information by fax, you **must**:

- be aware that the Council does not consider fax to be a secure way to communicate, especially for exchange of personal or sensitive information
- It does, however, recognise that some partner organisations (eg NHS partners) can require communication by fax as part of their information sharing agreements, and use of a fax machine or fax service is permitted where an exemption has been approved in advance.
- be aware of and comply with any conditions set out in the authorisation of your request for an exemption to use a fax
- take care to dial the right fax number - accidentally dialling an incorrect destination number is a common cause of data breaches and fines from the Information Commissioner's Office
- be aware that faxes can be read by people not authorised to view the information you are sending (eg if the machine prints off your fax in an open office)
- To limit this risk, take due care to ensure the correct person receives your fax (eg by calling them in advance to let them know you are about to send it and confirming that they have received the fax).

5. Use of the internet

This policy explains your duties and obligations when using internet services provided by the Council or accessing the internet through work-issued devices.

5.1. Why is this important?

Access to the internet is provided to assist you with your work and service delivery, and you have a duty to protect any sensitive or personal information that you access while using it.

If you don't take steps to keep work-related systems, information and data safe by using the internet responsibly and following this policy, it could put people and services at risk.

5.2. Requirements

5.2.1. General principles

During work hours (including when you are carrying out Council business outside of normal officer hours – eg for Council meetings), the Council expects you to use its resources to help you with your job and for its business purposes. Reasonable personal use of the internet is permitted provided it complies with this policy and any associated policies and standards specified in this policy.

When using internet services provided by the Council, or accessing the internet through work-issued devices, you **must**:

- be aware that the Council uses filtering software to automatically block access to some websites which it considers inappropriate or a potential security risk
- contact the ICT Service Desk immediately if you accidentally visit a site which contains material that might be deemed illegal, obscene or offensive so that it can be added to our list of blocked sites
- make sure that your use of internet / mobile data is within reasonable limits (for example, you **must not** use the Council's internet / mobile data services to stream large videos and **must not** use the Council's mobile data services for extended internet connection from PCs / laptops – also known as 'tethering'). Excessive use will result in costs being recharged and may also result in the service being cut off
- other than for legitimate work reasons (such as managing a complaint from a resident referring to such material), never deliberately view, copy or circulate any material that:
    - is sexually explicit or obscene
    - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
    - contains images, cartoons or jokes that may cause offence
    - contains material the possession of which would constitute a criminal offence
    - promotes any form of criminal activity
- be aware that if you use the Council's internet services for personal use (eg for online shopping), the Council will not accept liability for default of payment, failure to provide services, or for the security of any personal information you provide online

6. Keeping your working environment secure

This policy explains your duties and obligations for helping to keep your workspace safe and secure.

6.1. Why is this important?

It is essential to be aware of your surroundings and any potential security risks to our systems, information or data. This way, you can take steps to prevent or minimise them. If you don't (or you simply rely on other people to do this) it could put people and services at risk.

6.2. Your responsibilities

6.2.1. Security badges

When working on site or representing the Council in an official capacity, you **must**:

- keep your security badge (sometimes referred to as a building pass, building access card or ID card) on you and visible at all times. At other times, you must store it in a safe place
- contact the Facilities Helpdesk immediately if your security badge is lost or stolen
- return your badge to your manager when you stop working for the Council (Members must return their badge to Member Services when they stop being a Member)

6.2.2. Visitors and guests

When visitors or guests meet you at an official building or site, you **must** make sure they:

- report to the visitors' reception
- are escorted by a member of staff all times
- wear a visitor's badge at all times and return it when they leave

6.2.3. Buildings and premises

When working at an official building or site, you **must**:

- where it is safe to do so, challenge anyone on the premises who does not have a security badge on display, and if you are not confident that this is safe then you must alert security staff
- alert security staff immediately if you see anyone doing anything suspicious on the Council's premises
- alert security staff immediately if you meet anyone on the Council's premises who can't show you their security badge
- make sure other people don't follow (or 'tailgate') you into secured areas if they don't have an appropriate security badge or access card
- make sure that any storage areas are kept locked and only accessible by authorised individuals

6.2.4. Documents and paperwork

When working with documents or other papers containing sensitive or personal information, you **must**:

- never leave papers unattended, especially in areas where they could be seen by unauthorised people
- keep papers in locked storage (eg a locker or cabinet) when not in use
- take reasonable measures to keep papers secure if you take them away from the Council's premises
- dispose of papers containing sensitive or personal information securely by using a secure waste bin or shredder
- return to the Council any information held on paper or non-corporate services /

systems when you leave

- never write down or print off any passwords or codes that allow access to systems or services that use or store work-related information (if you need to keep a record of your passwords, you must use a password-protected document or an approved password storage application)
- report security concerns in line with the Council's security breach procedures if you believe that unauthorised people may have seen or accessed work-related information or data

7. Version history

Version ref	Author	Comments	Approved by Information Governance Group
0.1	Rob Miller	Original draft	22 October 2016
1.0	Rob Miller	Final draft for IGG approval	23 February 2017