Acceptable Usage Policy

Contents

1. Overview / introduction

All staff and other users of the Council's IT 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 (e.g. where sharing information with partners in health or the police will protect the wellbeing of individuals) or where there is a legal requirement for the Council to do so.

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:

- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- 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, you, your manager or your organisation, could face substantial fines. Our access to essential data that is shared with us by government departments, agencies and other partners to deliver our services could also be removed or restricted.

If you don't comply with this policy, you may be subject to disciplinary action.

1.1. Audience

This policy applies to all users with access to any of the Council's computer systems or information including:

- Councillors
- permanent staff
- temporary staff (including contractors, interim, short term and consultants)
- third parties accessing the Council's IT resources (including suppliers, partners, staff working in shared service arrangements, work-experience staff, volunteers and students etc).

This policy does not apply to the public who might access a public access computer in reception or library areas.

2. Keeping information safe

This policy explains your duties and obligations for keeping information secure. This will include sensitive and personal data. 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. In some cases, this can mean a threat to someone's life or health.

Whilst the Council's Digital & IT service is responsible for the implementation, maintenance and management of technical security controls defined in separate IT security policies, the majority of data breaches happen when staff misplace information (eg laptops, papers etc), mistakenly share it with the wrong people (eg on Google Drive, email), or don't dispose of it safely.

This means that you and your team 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. You are required to complete mandated training when it is offered.

2.2.3. Comply with the following policies and procedures:

- your organisation's Information Classification and Marking Policy - which 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
- the Council's policies on the use of social media
- registering information sharing agreements with the information governance team.
- 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. This includes forwarding Council data to a personal email address.

2.2.5. Do not connect unauthorised equipment to any telephone or computer network that is in the control of the Council. This includes (not an exhaustive list) computers, desktops, laptops, mobile devices, tablets, wireless access points, routers, switches, telephone or other electronic devices.

2.2.6. Alert your manager if you believe there has been a breach or potential breach of this policy. The process for reporting a data breach can be found on your organisation's intranet.

2.2.7. Contact Digital & IT if you have any questions about this policy or how to comply with it.

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

- are aware of and comply with this policy
- complete all mandatory training and have any relevant resources made available (eg appropriate equipment, secure disposal facilities etc)
- are provided with, and understand, any changes or updates to this policy

2.2.9. 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 or other members of staff)
- never use someone else's account to access the Council's systems, information or data

2.2.10. 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.

2.2.11. Digital and IT will monitor the use of communication tools and services, including access from overseas, where it has been approved. (See working overseas policy on the intranet).

2.2.12. Where unusual or suspicious activity is detected or suspected, we reserve the right to suspend or terminate access without warning.

2.2.13. Where there is a genuine business need to access information (e.g. emails or files) in another user's account or device, a request (which will form an audit trail) will need to be raised on the Support Hub. Digital & IT will request approval from an Assistant Director or Director and will only process properly authorised requests.

2.2.14. A leavers form is found on the Support Hub and must be completed when any of your staff members, contractors or suppliers leave or no longer need access to the Councils systems. Failure to do so is considered a breach of security. In this situation, the severity of the non-compliance will be assessed and the manager may be required to complete a security breach report.

2.2.15. Digital & IT reserves the right to remove your personal data saved on the network or company owned devices, including but not limited to exclusion from backups or deletion, without warning.

3. Use of devices

This policy explains your responsibilities relating to any device that you use for work (e.g. ChromeBooks, 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 (see the BYOD policy).

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 and you could face disciplinary action.

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. Where this facility is not available the device must not be used to connect to Council services or process or store Council data.

- notify Digital & IT immediately if your Council issued 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
- 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)
- Do not leave the device unattended where it can be stolen or misused.
- never use public printers or public cloud print services, as this could result in printouts of sensitive information being given to unauthorised people or information being lost.
- Do not use services such as on-line PDF and Word document converters that are not part of the approved productivity tools.

3.2.2. Work (corporate) devices

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**:

- never allow other people, including family members, to use equipment that has been issued to you
- never download and or install software unless you are authorised to do so, as this could introduce malware and information security risks to the device - if in doubt, you must contact Digital & IT for advice
- be aware that the Council is not responsible for, and does not support, any of your personal data stored on the device
- be aware that the Council may delete any personal data or applications that you have installed, including those stored on the corporate network
- return all work-issued IT equipment to Digital & IT or your line manager when you stop working for the Council

3.2.3. Public Computers

Never use public computers to access Council systems, data or services.

3.2.4. Personal devices (BYOD)

BYOD (Bring Your Own Device) is the concept of employees using their personally owned device(s) for work purposes.

Wherever possible a work-issued device should be used, but you may also use a personal device, owned by yourself, to access Council services and data, as long as the following is complied with:

General principles :

- Passwords or biometric controls must be enforced. In the case of passwords, these must not be shared with anyone else, be suitably complex and not easy to guess.

- The device itself must not be shared with anyone else.

- Screen locks must be configured to lock if the device is not used for more than 5 minutes.

- Council or personal data must not be downloaded onto the personal device. This includes, but is not limited to, documents, screenshots, 'cut and paste' of data and recordings/transcripts of Google Meet video meetings.

- The operating system and all software applications must be maintained to current supported levels.

- Where technically possible, the device must have a current version of anti-malware software which is kept up-to-date with current signatures and configurations.

- Where technically possible, disc encryption must be enabled.

- Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.

- Staff are responsible for all mobile data or wifi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

- Technical support from the Council's IT department will be limited to the Council's authorised software applications and will not include the user's personal device itself.

- The organisation records and monitors usage of BYOD devices including the make and model of devices in use and the version of the operating system currently installed. Where operating systems are found to be out of date the staff member will be informed and expected to upgrade to a supported version. Failure to remediate will result in access to BYOD services being withdrawn.

Device specific guidance :

3.2.5. Mobile phones :

- Personal mobile phones may be used to access Council information via the authorised Google mobile apps. Only the authorised apps will be permitted. To install and authorise these apps, you will need to contact the IT department.

- If you lose your personal mobile phone, you must immediately inform the IT department, who will disable the device and wipe any corporate data. This will not affect any of your personal apps or data.

- Personal mobile phones must have a password enforced and must be encrypted. If these measures are not in place, the device will not be able to access Council services and data.

3.2.6. Computers including, but not limited to, laptops, desktops and tablets:

- Computer devices, other than mobile phones, may be used to access Council information via a Chrome browser. Access to Modern Desktop may only be via the Chrome Browser and the Citrix Receiver extension.

- If you lose the device, you must immediately inform the IT department, who will disable its access.

- Personal computer devices must have a password enforced and must be encrypted.

A particular note :

No access is allowed to DWP systems from a personal device. Only a work-issued device can be used.

We also reserve the right to restrict access to other business systems at any time.

Note that the organisation reserves the right to revoke access if staff do not follow this policy.

3.2.7. USB removable media

- It is not acceptable to store or transfer any Council information onto removable media. This includes any such device such as USB memory stick or external hard drives etc

- Connecting of cameras is only acceptable for the transfer of work-related photos, audio and video after approval from Digital & IT.

4. Use of communications tools and services

This policy explains your duties and obligations when using digital tools, services, applications and extensions that have been approved for use by the Authority.

4.1. Why is this important?

The Council allows staff 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, Google Apps etc) and the business processes for your service area.
- be careful who can see your screen when accessing systems.
- 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). If you do discover an error in access control (access where you should not have access) you must report this to Digital & IT
- comply with your organisation's 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 appropriate care to ensure that your communications are addressed / directed to the intended recipients (eg making sure that you use the correct email addresses)
- take appropriate steps to make sure that the person you are communicating with is who they say they are and that they are authorised to see the information you are sharing
- take considerable care when communicating with untrusted and / or unknown contacts
- Notify Digital & IT if you believe, or know, that information has been sent to the wrong recipient.
- never click links to URLs (web addresses) or open attached documents received from untrusted or unknown sources or contacts. Also be aware of phishing techniques that will attempt to trick you into doing something

- 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.
- If you are accessing data from other organisations that is covered by a memorandum of understanding (e.g. DWP, NHS) you must not access the data from locations that are not allowed under the MOU (usually not allowed from outside the European Economic Area).

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

When you use communications services (eg phone, SMS, Google Chat, Google meet 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, whiteboards 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). *Be aware that there is no technical method to tell if you are being recorded.*
- 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. Voice and Video recording

If you create a voice or video recording you accept and agree to the following:

- You will obtain consent from all participants on the call before recording takes place
- You understand that recording a person without their consent is unethical and must be avoided. **If the recording is used for anything but your own personal use, or you lose control of the recording, you are committing a criminal act and may be prosecuted.**
- you are responsible for the data file and its secure storage.
- You are responsible for the impact of the recording if it was to be exposed to third parties.
- You accept that recordings could be requested under FOI or under the Data Protection Act as a Subject Access Request and will manage the recording file accordingly.
- You accept that you are responsible for deleting the information once it is no longer required or inline with the Council's Retention schedule
- if the information recorded is sensitive, you will ensure it is marked as OFFICIAL SENSITIVE and share on a need to know basis.

4.2.4. Online posting

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

- 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 and comply with the Council’s Social Media Policy
- never share sensitive or personal information on a public forum
- make sure you have permission to publish content that may be protected by copyright, fair use or financial disclosure laws
- make sure you have permission to comment or report on work-related meetings or discussions (you must not name or make reference to customers, partners or suppliers without their prior approval)
- behave appropriately and professionally, with the understanding that you are representing the Council when using your work persona
- alert the Council’s Communications Team immediately if the press or media contact you
- Do not represent or appear to represent the Council, implicitly or explicitly unless you are authorised to do so.

4.2.5. Fax

The use of fax is prohibited unless pre-authorised via the exception process.

- You must notify the recipient prior to sending sensitive information so it can be collected and secured by the recipient and not left unattended.
- If **any** fax is not received by the intended recipient, this must be reported as a security breach via the normal reporting methods. Accidentally dialling an incorrect destination number is a common cause of data breaches and fines from the Information Commissioner’s Office

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 or personal devices (that is being used for work purposes) at any location you perform work.

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. This includes cybersecurity and reputational risk, through the use of prohibited or malicious online services.

5.2. Requirements

5.2.1. General principles

Council resources are provided to facilitate carrying out business activities. 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
- understand that log files are kept of your internet activity and your activity may be monitored.
- contact Digital & IT immediately if you 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
- never download music files, games, software files or other computer programs that do not relate to your work - these types of files are a significant cybersecurity risk, consume storage space and may violate copyright laws.
- Unless part of your official job role, 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
    - 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 including on-line fraud.

6. Keeping your workspace secure

This policy explains your duties and obligations for helping to keep your workspace safe and secure. Your workspace is anywhere you conduct work.

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.

6.1.1. 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
- ensure that printer queues are cleared prior to leaving the printers unattended
- keep papers in locked storage (eg a locker or cabinet) when not in use
- take proper 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.
- 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
- documents must be returned to the office for secure shredding / disposal.

When working from home, it is your responsibility to apply the above guidance but tailored to suit your environment and facilities. In broad terms, keep paper and your technology appropriately secured. **Lock them up when not in use.**

7. Version history

Version ref	Author	Comments	Approvals		
			AfC	RB Kingston	LB Sutton
1.0	Rob Miller	Original version	21 Jan 2016	1 Feb 2016	14 Jan 2016
1.1	Rob Miller	Amendments following feedback from LBS Employee Side		16 May 2016	13 May 2016
1.2	David Grasty	Amendments following circulation to all staff			12 Jan 2017
1.3	Mark Lumley	Amendments following review for GDPR		22nd Feb 2018	23rd April 2018
1.3	Steve O’Connor	Review. No changes made			February 2020
DRAFT 1.4	Lee L, Rhian, Matt V, Deb W	Major amendments pre-Security board 09/11/21			
2.0	Info. security board	Major amendments finalised		May 2022	March 2022