Information Security

Acceptable Use of Information Technology

Updated October 2023

1. Introduction

This document sets out our policy and guidelines on the permitted use of our Information Technology (IT) and what action may be taken if you breach this policy.

It outlines our minimum standard to be followed by Glasgow City Council.

Other members of the council family may adopt stricter standards than outlined in this policy. If not, then the Glasgow City Council standard applies. For further information contact your relevant Service/ALEO Information Risk Owner. A list can be found here.

This document replaces all previous versions.

2. Responsibilities

All users of our IT resources are required to read this policy and to comply with it at all times.

If you are a manager or a supervisor **you must:**

- make sure that your staff are aware of this policy and that **a User Access Form has been submitted for the staff member** before using any of our IT resources
- **authorise** use of IT resources in your area
- make sure **your staff comply** with this policy when using our IT resources
- deal with **breaches of this policy** (more information in section nine)
- make sure that if you have any **staff changes** - new staff starting, moving, or leaving, you complete the relevant forms and send them to CGI and Customer and Business Services. This will allow the access rights to our IT assets to be correctly updated for the member of staff using that asset. For more information on our assets read our **Information Security - staff guidelines on Connect.**
- **monitor your staff's use** of email and the Internet, in line with **section nine** of this policy document.
- make sure that you and your team have completed the information security course

3. Policy

We rely heavily on our IT to conduct our business. Access to our IT resources is strictly controlled and monitored. Unauthorised use of our IT is not permitted - all users must have been authorised by management.

Section six and seven of this policy outline the authorised use of our IT.
Personal use of our IT resources is authorised, but this is at the discretion of your manager, and your use must comply with **section six** of this policy.

We reserve the right to withdraw permission for personal use if you breach this policy. Action may be taken against any individual or group, under our disciplinary code, who do not comply with our guidelines. This action could result in dismissal for gross misconduct, and in certain circumstances the matter may be reported to the police.

For more information you can contact:

- **The Head of Information and Data Protection Officer via the Asset Governance mailbox at AssetGovernance@glasgow.gov.uk**
- **your Service HR**
- **CGI service desk on 74000 or (0141 287 4000 from an external line)**
- **Internal Audit on 0141 287 3777.**

4. Scope - Users

This policy applies to all members of the council family who use our IT resources.

This includes:

- staff
- contractors
- consultants
- students
- voluntary workers
- interns
- Modern Apprentices
- any other person (except those listed below) who have access to our IT.

This policy does not apply to:

- Elected Members
- use of our website by the public
- members of the public using public access PCs in libraries and learning centres

- use of IT associated with the schools network which is used by children and young people. Please note there is a separate Acceptable Use Policy for school pupils which can be found here.

5. Scope - Resources

This policy applies at all times, to all council working arrangements which includes office, home, hybrid and mobile workers.

This policy applies to all IT resources accessed by you to conduct our business. This includes:

- PCs
- telephones (including mobile and landline phones)
- mobile devices (including laptops, Blackberrys, iPhones, tablet/hybrid devices, iPads and other Personal Digital Assistants - PDAs)
- USB storage devices (including pen-drives)
- business applications (for example, SAP or CareFirst)
- networked and cloud-based document storage areas
- fax machines
- our communications networks – landline and mobile
- radio systems
- printers and scanners
- video and audio conferencing
- streaming services

The policy also applies to access to council systems from 'unmanaged' devices, such as your own personal, non-council issued, IT devices, where this has been approved.

Guidelines on the use of our IT resources by Trade Union Representatives can be found in **section seven** of this policy.

6. Guidelines on personal use of our IT resources

You are not allowed to use our telephone landlines, or a council mobile phone (including Blackberrys and smartphones) for personal use, except in an emergency.

This restriction also applies to the use of a council laptop or tablet which is connected through a mobile phone network or mobile broadband (4G).

However, if you use WiFi or a broadband connection for your device, you are allowed personal use as shown in the guidelines below.

You are allowed to use your device for personal use provided it does not:

- hinder our business
- incur any additional cost to us
- adversely affect the running of our systems
- bring us into disrepute.

Personal use **must:**

- only take place during your own time, unless in exceptional circumstances and it has been approved by your line manager - working hours vary across the council and our Services, make sure you understand your working arrangements
- not breach the general guidelines on use of IT resources in **section seven**
- not make use of business information which has not been made available to the public, for example our Council Tax System - access is explicitly prohibited and this would be a criminal offence under the Computer Misuse Act 1990 and data protection legislation.

Personal use **must not** include:

- allowing others, such as friends or family to use your council IT devices
- the storing of personal files, such as music on our IT devices and network – we reserve the right to delete such files
- accessing social media, such as Facebook or Twitter for personal reasons
- using instant messaging due to the risk of viruses
- installing and downloading programs such as games or tool bars
- accessing audio, radio or video content - streaming these for purposes unrelated to your workplaces unnecessary strain on our network
- using file sharing programs
- using your business email address to subscribe to mailing lists, services and clubs which are not related to your work
- use of web mail services, such as Gmail, unless you are authorised to do so
- accessing records about you held in the council or partner's business systems other than records created and owned by yourself
- accessing records about people not related to your work which are held in council or partner's business systems that you have access to.

We will **not accept responsibility** for:

- making or restoring backups of personal files
- any financial loss you incur as a result of personal transactions made using our ICT facilities.

7. General guidance on the acceptable use of our IT resources

These guidelines apply to both business and personal use.

- **Software** - including media files such as music and video, must only be used in accordance with licence agreements and UK copyright law. Making, using or

distributing unauthorised software copies is illegal and is not permitted on our IT facilities.

- **Sensitive data** - you must follow our Information Security - staff guidelines, Data Protection guidelines and Protective Marking guidelines on keeping our information secure and your accounts protected. Our guidelines include best practice such as:
  - using encryption for sensitive business data where necessary
  - marking emails and documents which contain sensitive information with an OFFICIAL-SENSITIVE protective mark
  - using a strong password which is not shared with anyone
  - not allowing anyone else to use your IT account
  - not using anyone else's IT account.

- **Business use of social media**
  - Staff who have a responsibility, as part of their role, to use social media for business purposes will be given support and training by their manager in its appropriate use in line with our media protocols.
  - If your role requires you to post updates to social media sites, remember you are representing the council and anything you publish reflects directly on the organisation. If you think you've made a mistake online, notify your manager immediately.
  - You should use the same safeguards - as you would with any other form of communication regarding the council, other organisations and yourself when in the public domain.
  - Therefore, you should not publish personal and other confidential information on social media platforms.

Always consider any potential risks before publishing on social media and have plans in place to mitigate them.

- **Video and audio conferencing**
  - Council provided facilities for video and audio conferencing must only be used for business purposes.
  - When organising an audio or video conference, care must be taken to ensure that you only invite the correct parties to attend. This is especially so, where you are inviting people to join the conference who are not employed by the council.
  - Before the conference starts, the meeting organiser or someone assigned by the organiser should monitor who is joining, or requesting to join the conference, before the meeting gets underway, and should not proceed if an unauthorised attendee is present.
  - For all uses of video and audio conferencing, regardless of whether it has been provided by the council or a third party, professional standards of behaviour are expected of our users at all times. Downloading of files from untrusted sources is prohibited.
  - If the facility provides the ability to record the conference, all participants must be made aware and agree to this prior to the start.

- If you have access to, and the ability to set backgrounds in video conferences you must only use backgrounds that have been approved corporately and meet corporate branding standards.
- If your device does not allow you to set backgrounds, you must ensure there is nothing visible that may be damaging to the reputation or professional image of the council.
- The use of an avatar to represent yourself in a video conference is not considered to be professional business practice. Avatars must therefore not be used.
- When using video or audio conferencing, participants must be mindful of their surroundings and who else is around them particularly if discussing details about service users, staff, and other sensitive material.
- Both video and audio recordings plus the content of online chat discussions may be regarded as council records and may have to be released under FOI and Data Protection requests. If the content of a chat warrants retention, arrangements must be made to replicate the information the chat contains in a suitable document which can be stored in the EDRMS.

- **Email and Messaging** – any messages you send from our council email system or other messaging facilities identifies us as the sender – emails, texts and other electronic messages are therefore the same as sending a business letter on headed notepaper. You must make sure that any information you send is appropriate and does not include any personal comments that may conflict with our policies or damage our reputation.
  - **You must not seek to bypass controls which the council has put in place, such as protective marking, by using forms of email where this is not present**
  - Where you are required, for business continuity purpose, to use web mail services which do not have automated protective marking present, you should apply the required protective marking manually
  - If you need to send bulk emails or messages to external recipients, for example, emails to more than 100 recipients, who are not Glasgow City Council employees, **you must** contact the CGI IT Service Desk for assistance.
  - For security and data protection reasons, any bulk email or message sent to members of the public **must always** be done on a blind recipient basis (BCC) so that no recipient can see who the other recipients of the email or message are.
  - For small distribution lists, the BCC function on Outlook and the use of Groups in message applications can be used to achieve this.
  - For larger distribution lists (for example, 100 recipients or over), contact the CGI IT Service Desk for assistance.
  - It is also good practice to use BCC for internal emails which are intended for large numbers of recipients to avoid the potential for recipients “replying to all” unnecessarily and generating large volumes on unwanted email traffic.

- When using email, if your facility allows you to **set an image in your profile**, this must only be in line with corporate standards. You should also be aware that any image you have selected will be visible externally, and so if you wish to do so, the image must be in keeping with our business. If you do not wish your photograph to be visible outside of the organisation, then don't select this option.
- For full guidance read our **Guidelines for Staff Using Email and Messaging.**

- **Mobile Devices** – you must take care with the security of any of our IT resources, especially mobile devices. Try to avoid leaving equipment such as laptops, tablets and smart phones in a vehicle – if you have to do this, please lock them securely out of sight, for example in the boot.

- **File Sharing Services –** where there is a requirement to share council information with a third party you must only use file sharing services which are approved by the council's Strategic Information, Innovation and Technology (SIIT) team. The only exception is where there is a specific reason why we must use a third party's file sharing facility.

- You **must only** use a device which has been approved by your employer to contact citizens, customers and service users.

- You **must not** give citizens, customers or service users the number for you own personal mobile phone, or store the numbers of, or any information about citizens, customers or service users on your personal mobile phone.

- If you find yourself having to use a device, such as your own personal mobile phone which **has not** been issued by your employer, to communicate with another staff member or partner organisation for business purposes, and the nature of the communication includes information which may be sensitive, you must exercise caution and be aware of who else might be in the vicinity in order to protect council and service user information, and yourself.

- If you have cause to contact another employee's personal mobile phone but have to leave a message this should be limited to basic information such as 'Please call me back'. If someone else has left a message on your personal voicemail and this contains sensitive information, you should delete the message once you have listened to it.

- Users **may not** access, use, create accounts with or submit data to any web-based software or service unless that web-based software or service has been approved by the Strategic Information, Innovation and Technology team (SIIT).

- If you are required to access council IT networks remotely you must only do so using methods approved by the Strategic Information, Innovation and Technology team.

- Users **must not connect** or attempt to connect any personal device (or any file storage device, gaming device, camera, personal memory card or other similar device) to the council IT network, or mobile network provided by the council, either physically or remotely without approval from the Strategic Information, Innovation and Technology team.

- Users should be aware that the **network is monitored and audited.**

You **must not use our IT resources** as follows:

- for illegal activities, including defamation and fraud
- to operate a private business
- to run personal or private software - there is a risk of viruses and to the council network
- for any purpose that would breach our Information Security - Staff Guidelines, Equality Policy, Harassment Policy, Employee Code of Conduct, or our Code of Discipline
- install or use any software or tools on council issued devices or access IT services from them which undermine or bypass our security systems and policies - this is only permitted by technical staff when authorised by management or when authorised by the Strategic Information, Innovation and Technology Team following technical assessment by our IT service provider. This includes any software that would:
    - identify passwords for files and accounts
    - secretly record keyboard input
    - hide the user's identity
    - intercept traffic transmitted across the network
    - enable mass mailing.

(This above list of examples is not exhaustive).

If you are not sure that your use of our IT resources is appropriate, please speak to your line manager.

8. Guidelines on the use of IT resources by recognised Trade Union Representatives

Where IT resources are provided as part of the Trade Union facilities within your Service, any Trade Union duties, as defined by the Advisory Conciliation and Arbitration Service (ACAS) Code of Practice, will be treated as authorised council business use.

Our IT resources **may not be used for other Trade Union activities** (except by agreement of management) or used in conflict with our interests (for example, opposition to council decisions or ballots for strike action).

9. Monitoring the use of our IT resources

Your manager, or supervisor, is responsible for reviewing reports about your use of our IT resources. In addition to this, Internal Audit monitors use to make sure that this policy is being applied.

Any breach to this policy will be reported to your Head of Service to deal with.

If you use our IT resources, you must accept that your usage will be routinely monitored to make sure you are complying with this policy. This monitoring will help to maintain the efficiency and integrity of our IT and includes:

- dialled telephone numbers - the date, time, and duration of calls
- the dates, times and addresses of websites visited
- the dates, times, subjects, senders, and recipients of emails
- details of all music, picture and graphics files stored on our network
- use of unencrypted USB devices (for example, pen drives)
- details of usage that identifies specific IT equipment
- use of video and audio conferencing, including associated chat
- use of streaming services
- details of devices used to access our network.

We will take reasonable steps to respect your privacy when using our IT resources whilst upholding our obligations, as both the service provider, and also your employer, in accordance with our **Privacy Statement.**

Any managers undertaking monitoring must make sure that they act in a reasonable and fair manner, for example, random spot checks of usage may be legitimate, however extensive monitoring of an entire staff group is unlikely to be legitimate and would require robust justification.

We may have to conduct detailed investigations, (including accessing the contents of files or email messages) for various reasons which can include:

- making sure our policies, conditions of service, business and security procedures are adhered to
- maintaining the effective operation of our computerised systems
- conducting council business in an employee's absence
- preventing/detecting unauthorised use of communications systems, criminal activities, or other serious misconduct

- providing information to individuals or outside agencies, as required by data protection legislation, the Freedom of Information (Scotland) Act 2002 and/or the Environmental Information (Scotland) Regulations 2004.

Where possible we use automated tools to manage our IT resources and to protect against inappropriate or malicious material or viruses being passed through our IT.

Where a trade union representative or member of staff pursuing a grievance is subject to monitoring, this should only be undertaken by the Service or ALEO HR team, Corporate HR, or Internal Audit. This is to avoid any perception that management monitoring is being done to undermine the activities of the union representative or the person raising the grievance.

Managers and supervisors should also avoid opening messages between union representatives and their members for the same reason.

If such messages require to be analysed, this should also be done by the Service or ALEO HR team, Corporate HR, or Internal Audit. In such cases the trade union will be advised of this in a timely manner and prior to any formal proceedings being instigated.

NOTE: This will not apply to general trade union correspondence such as the distribution of newsletters or members' offers.

10. Breaches of this policy or other misuse of IT resources

Action will be taken against any individual who breaches this policy or misuses our IT resources. The action taken will be appropriate to the circumstances and may include disciplinary action, up to, and including dismissal.

In certain circumstances, breaches of this policy may be reported to the police. If you are aware of any breach of this policy, you should advise your manager or supervisor, or report the matter to the Head of Audit and Inspection as soon as possible.

11. Employee benefits and resources

We recognise the benefits of this policy - which includes the personal use of our IT as detailed in **section six**, as being:

- responsible and productive use of our IT resources can enhance your skills and awareness
- flexible working practices tend to make boundaries between personal and work time overlap - personal use of our IT can help balance your work, lifelong learning, and personal life
- personal use of our IT is an opportunity to provide a benefit to you at no additional cost to us.

All staff must complete the current Information Security course. This course is available on our employee development portal called Glasgow Online Learning Development (GOLD).

You must complete this course annually so that you are reminded of your responsibilities when using our equipment and how to handle and protect the information you use at work. In addition to this mandatory course, you can also undertake courses on GOLD to help with your computer skills.

12. Other relevant policies, regulations and codes

For more information, please read our:

- Code of Conduct
- Code of Discipline
- Equality Policy
- Information Security Policy
- Information Security - Staff Guidelines
- Guidelines for staff using email and messaging
- Our Privacy Policy and Statement (please refer to ALEO equivalent material)
- Bullying and Harassment Policy

There are a number of other documents and regulations that are relevant to this policy. These include:

- Computer Misuse Act 1990
- Data Protection Legislation
- Freedom of Information (Scotland) Act 2002
- Information Commissioner's Employment Practices Code and Supplementary Guidelines.

13. Further guidance and information

For further information please contact Dr Kenneth Meechan, Head of Information and Data Protection Officer, at AssetGovernance@glasgow.gov.uk