Information Security

Information Security - staff guidelines

Updated December 2023

This guide is for all members of Glasgow City Council's (the Council) family including any volunteers that may handle or use information held by us. It will help you to understand that the information we use as part of our day-to-day work should be:

- **protected**
- **held securely**
- **handled with care**

It is important that you use it to know how to protect our paper and electronic information – at home, in the workplace and anywhere else you find yourself on work related business.

1. Introduction

Information Security is increasingly important to every organisation, even more so in today's society. As a Council **we must** be aware that:

- there can be public outcry when public agencies, such as the Council lose personal or sensitive data
- **we have** legal responsibilities on how we hold and use information
- our staff work in many different ways in addition to office based, for example from home as flexible workers, or on the move, increasing the possibility that information can be lost
- there are dangers of fraud or identity theft because of information being lost
- large amounts of information can be stored on small devices, such as a USB memory stick which can easily be lost
- if you have access to personal information about staff or customers, then it must be treated as **strictly confidential** – it is a serious offence to use that information for anything other than for council business purposes

2. Keeping your information safe

To keep your information secure **you must** follow some basic guidelines:

- **be careful** about **general security in the office**, especially when you leave it and no other colleagues are present, and while working from home and other locations
- **be aware** of people attempting to follow you through a **controlled entry door** who are not wearing the correct identification

- **if you feel safe to do so**, ask unaccompanied strangers/anyone not wearing an ID badge if you can help, or else contact reception or the facilities manager for the building
- always wear your **ID badge** where others can see it - your manager **will remind you** if you do not wear it. Always use an approved lanyard
- keeping your **desk clear** can avoid opportunistic theft and the loss of information
- **do not** keep large amounts of **unnecessary information** - if you no longer need it please dispose of it to save office space in line with our records management policies which can be found here. If you need to take **work out of the office**, **only take** what you need, know where you are taking it and exactly what the information is, and get your manager's approval for doing so
- use the **MyPrint secure print function** when collecting information off a printer and always **make sure** you have only collected your own prints
- if your print doesn't come out of the printer, **clear the job from the print queue** and report the issue to the CGI Service Desk on 0141 287 4000
- if you **find someone else's printed information** in the printer output tray or near the printer, if you can identify the owner, contact them or leave a note to say you have the information, or, if this is not possible, put the information in the confidential waste facility
- **make sure** that any letters you send are **correctly addressed** and only contain the correct information.
- **change** the default PIN on your office phone and keep it to yourself to prevent someone else logging in as you.

2a. Tips on how to keep any sensitive paper information safe

- **make sure** that any sensitive information you have is **held securely**, such as in a locked cabinet
- **avoid taking notes down on paper** if possible (use your Council mobile device instead if you have been issued with one)
- **if you must** take notes, **avoid including full personal details** – use initials, reference numbers or some other identifier which would be meaningless to an outsider. Transfer information from the notes into computer format **at the first available opportunity** and **make sure** the hard copy is then securely disposed of, or else physically transfer the necessary pages into the relevant paper file
- **do not use** internal mail to send paper based sensitive information around the organisation. Instead, hand deliver it
- in the office, only print if you absolutely must, and make sure any material is promptly collected from the printer
- if working at home you should only print when necessary and only print sensitive information if you have approval from your Service/ALEO Information Risk Officer (SAIRO). List can be found **here**.
- if you **no longer need** the sensitive information, shred it, or dispose of it in a confidential waste bin. Sensitive confidential material must never be disposed of via domestic waste or recycling.
- If sending sensitive information by external post, where practical and economically viable, use registered post, **make sure** the correct address has been used, and it is

good practice to place the information in an additional envelope before placing it in the addressed envelope

- avoid **sending faxes wherever possible and use more secure methods of communication, but**, if you **need to fax** sensitive or confidential information then please **make sure** that the correct person has received and collected your fax

For more information on sending a fax, read our guidelines on Connect.

2b. Tips on how to keep computer information safe

- your computer **must be password protected** – it must be difficult to guess and **must be** kept secret
- **you must not** use someone else's password to login and access their work account – even if offered
- use a **strong password** – fmore information on how to set a strong password for your computer can be found here
- except where circumstances require temporary local storage, all **business-related** work **must be** saved on **your shared council drive** or in our **Electronic Document Records Management System (EDRMS)**
- documents containing sensitive information which are shared internally, must either be emailed, or shared using a secure and restricted area of the EDRMS
- **you must not** store your own data, such as photographs or music onto our council network or EDRMS
- **do not allow** anyone to access information using your account
- if you leave your computer unattended, protect your information by locking it. Press the Windows key on your keyboard followed by L or hold down **<CTRL> <ALT> <DEL>, then select Lock Computer**
- **when you receive notification that software updates are ready to install on your computer you must allow these to download as soon as possible. Do not unnecessarily defer these updates by, for example, never switching your computer off.**

3. Managing and protecting our information assets

Various IT devices are used to access and store the council's information assets, including:

- desktop computers
- tablets
- laptops
- iPads
- mobile phones
- memory sticks
- cameras

- point of sale terminals

We all have a responsibility to protect and care for these IT devices as well as the information accessed using them, as both the device and the information have value.

Please note:

- most IT devices **will have** been issued to a **named member of staff** who has the principal responsibility for safeguarding the device. Where more than one member of staff has access to a single device such as a point of sale terminal, responsibility for safeguarding the device lies with the relevant manager
- your manager is responsible for notifying CGI of any changes of ownership to IT devices so that the **asset register** can be updated
- where applicable, your manager is responsible for notifying **Pay360@glasgow.gov.uk** so that the **asset register** for all point of sale /chip and pin devices **can be updated**
- if you need to **change the owner of any asset** in your area, **CGI must be** informed immediately to co-ordinate this change or transfer
- **if a member of your team leaves the council** your manager **must follow** the corporate **leavers process** so that their equipment can be collected, asset registers updated and passwords and accounts disabled
- any unused computers must be returned to CGI as these are a **security risk**, take up unnecessary office storage and cause us to incur unnecessary expense if we have to buy new ones
- be careful about **general security in the office** especially when the office is left empty, and while working from home and other locations.

4. Using the internet at work

Staff use of the internet and email is monitored, so it is important that you understand what is acceptable and what is not★.

You are reminded that you are not allowed to use Council telephone landlines, mobile phones, laptops, and tablets - connected to a Council provided mobile phone or broadband network (4G), for personal use, except in an emergency.

During lunchtimes, before or after work, you are allowed to use the internet via your Council device for personal purposes. Please bear in mind that you are using Council equipment and any website you access should be of a suitable nature. Do not subscribe to personal IT services using your Council email address.

We will block access to any websites that we feel are inappropriate.

Occasionally, due to the type of work that you do, you may need to access certain websites from which you are blocked. To get permission to these sites **you will** need to complete a **CGI Internet Access Request Form**, which your manager and **Internet**

Approvals team will need to approve. If you work in a school, **you must** complete the **'Internet Unblock Form – Schools'** and follow the instructions within the form. Once you no longer need access to these sites you should ask for your permissions to be removed.

You must not download or install any unauthorised software.

You should also be aware that downloading photographs, graphics, audio, or video for business purposes can take up space on the IT network and slow it down. Downloading material of these types for personal purposes is not allowed.

Please take a responsible approach to what you look at online and what you download.

If you are required to use, or are considering using an IT service hosted by a third party which is accessed using the internet, your manager should contact **your Strategic Information, Innovation and Technology (SIIT) team Business Partner** (you can find out who this is for your Service by clicking **here)** who will check if the site is already approved, or will arrange for a technical security assessment to be carried out. You may also be required to complete a Data Protection Impact Assessment if your Pre-screening Questionnaire identifies that personal data is involved.

Your Business Partner will advise on the outcome and specifically if the request to use the IT service is approved. If the assessment identifies that the IT service in question holds our data outside of the UK then the request will require to be approved by the Information Security Board. Further guidance on international data transfers can be found **here.**

★More information on our Acceptable Use of IT on Connect

5. Using email at work

Email is a critical business tool for many of us and is often the main method we use to communicate with external parties. However, this also means it is the easiest way for information to be sent out of the organisation, so it is vital that everyone who uses email is careful to **make sure** your information only goes to the person it is intended for.

Email is also increasingly used by criminals who attempt to induce us into providing information for fraudulent purposes, and as a means of introducing viruses and ransomware into our networks to disrupt services and extort payments. We therefore must be extra vigilant and keep a look out for emails which appear to be suspicious.

Email can also be seen as a less formal method of communication compared to sending a letter for example. However, if you are using a Council family email address, your communication is seen as formal and should be written in an appropriate business manner.

You are allowed to use the email system for personal email outside of your working hours.

When sending an email, **you must make sure** that:

- where possible, you avoid **emailing personal data** or other sensitive information – if you need to send it only supply the minimum data required
- you always **check the email addresses** you are sending your message to **make sure** auto-completed addresses are correct and that you have not clicked 'reply to all' instead of 'reply'
- you thoroughly **check your content** before you send your email - a long email chain could contain personal data further down in it
- you **apply an appropriate protective marking** in line with the content
- If the protective marking software alerts you that the email is being sent externally you must check that the recipient is who you intended
- **you must not set the auto-forward function** on your email to an external email address, such as your own personal email address
- **you must only** use the **auto-forward function** when sending emails onto another user of the Council family email system.
- you **must use the BCC function** if sending emails internally to large numbers of people, and when sending to multiple external email addresses.

Other key points to remember when using email:

- where possible try to **make sure** that attachments **do not contain viruses** and make sure you are not sending unintended personal data in them
- keep in mind that it **may be necessary to release emails** as part of
- Freedom of Information request
- personal data **must never be sent** to your home email address
- **do not** forward emails that contain large address lists, as you may not have the permission of all the recipients
- if you receive **inappropriate material**, **report it** to your Service/ALEO Information Risk Owner – they can decide whether this needs to be reported to the Integrity Mailbox (integrity@glasgow.gov.uk) and your Service's Director
- if you receive images that contain child abuse or exploitation by email, this **must be** reported immediately to your line manager and integrity@glasgow.gov.uk without forwarding the illegal or offensive material itself
- if you receive an email **asking for your personal bank account details** **you must** send this to Trading Standards at ts.enquiries@glasgow.gov.uk
- if you receive an email asking you for personal details or for a financial transaction that is not part of your duties, or seems unusual, then **you must** first verify if this is genuine via a separate communication channel. If in doubt do not action it and forward the email to integrity@glasgow.gov.uk
- **be wary of external emails from unknown sources** that request you click on links or download material as these could be related to cybercrime activity such as ransomware. If you do click on a link and then realise something isn't in order, you must phone **CGI** on **74000** (**0141 287 4000** from an external line) immediately
- if you **have to share sensitive information outside of the Council**, the preferred method is by using a secure file sharing platform (SharePoint) or the secure email facility

  However, if you are required to send the information to a ".gov.uk" email address, or the email has been marked as "Official Sensitive" using the Council's protective marking software, and use of other means is not practical, the content can be sent by email and it will be encrypted while in transit by Transport Layer Security (TLS).

If for any reason this fails, you will receive a notification informing you of this, and you should use the secure email facility instead

- Your **business email address should only be used to subscribe to mailing lists and services that are relevant to your work**. You must **not use** your business email address for subscriptions and services which are unrelated to your job. This not only makes sure that we do not receive quantities of non-business related emails into our network, but also reduces the risk that your business email address could be used for cybercrime purposes if these external sites are hacked.

For contact details for your **Service/ALEO Information Risk Owner** visit **Connect**

For contact details for your **SIIT Business Partner** visit **Connect**

For more information read our **Guidelines for Staff Using Email & Messaging**

Further information on how to use **Secure File Sharing and Secure Email** can be found on **Connect**

6. Using mobile devices

You should take extra care that these devices are secure to prevent loss or theft.
Please remember that:

- any mobile device you use to store personal or sensitive information **must be encrypted. You can check by going into the device's Settings** – if your device is not encrypted, please phone **CGI** on **74000** (**0141 287 4000** from an external line) as a matter of urgency to arrange for this to be addressed
- **never give your password to anyone**
- never store Council information on an **unencrypted** USB stick or other unencrypted add-on device
- if leaving mobile devices in a vehicle, make sure they are kept **out of sight**
- know where your mobile devices are at all times and store them securely when not in use
- if you leave your mobile device unattended, protect your information by locking it
- if you use your mobile device outside of the office, be aware of who can **hear your conversation or see** information over your shoulder or who is in your vicinity
- **if you lose** your mobile device or **it is stolen, please report** it immediately to **CGI** on **74000** (**0141 287 4000** from an external line), your line manager and then complete the Data Breach Form which can be found on Connect **here**. The completed form should be emailed to databreach@glasgow.gov.uk.
- **you must** connect your Council mobile phone to Wi-Fi regularly to **make sure** it receives any software updates and that these are installed in a timely manner.
- **you must not** use a device which has not been issued by your employer, such as your own personal mobile phone, to contact citizens, customers, and service users regarding a work-related matter, except in an emergency.
- you **must not connect a personal device to the Council IT network,** or a

mobile network provided by the Council unless this has been approved by your Service and ALEO Information Risk Owner (SAIRO).

- use of your personal mobile device is permitted, in instances where you have not been issued with a Council mobile device, in order to **authenticate access** to council IT systems
- **you must not give citizens, customers, or service users** the number for your 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 any device, 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 **must 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 must delete the message once you have listened to it**
- do not transfer the SIM card from your Council mobile phone to a mobile device that has not been issued to you by the Council
- if you have been issued with a Council mobile phone, **make sure** you change the PIN for the answering service from the default code. Contact the CGI IT Service Desk for advice on how to do this on extension 74000 (0141 287 4000 from an external line).

7. Use of Unencrypted Devices

Please note the following:

- in some areas of the business, **you may** need to use a mobile device, such as a camera (for general guidance on using a camera for business purposes please read the staff guide for this on **Connect**) or data stick, that is not encrypted – your manager will grant permission to do this once they have reviewed any risks
- **any unencrypted device that needs to connect to the corporate IT network** for business purposes must be whitelisted. Contact your **SIIT Business Partners** for information on how you go about this
- if you use an unencrypted device, **you must** minimise the amount of personal or sensitive information you store on it – in most cases this must be avoided
- if you have a legitimate business need and have had approval to store such information on an **unencrypted device you must** remove the data as soon as you have finished with it - **never leave** the data on it and also re-format the device to reduce the risk of it accidentally being recovered and used.

8. If you need to take information out of the office, including for home working.

- **you must only ever take** information out of the office if you have a business need to do so and only where there is no alternative

- if you need to take personal data away from a Council building you will need to get **written permission** from your manager – refer to your local authorisation procedures which your manager should have
- **avoid taking paperwork containing personal information away from the office** unless there is no alternative. If you need to, you must carry your paper information in a **secure file, envelope or bag that is not see-through**
- **do not** open paper files containing personal data in a public place
- **you must** only take personal or sensitive electronic information out of the office on an **encrypted memory stick**, **laptop, tablet, or mobile phone**
- if you take personal information out of the office it must **never be the only copy** that exists
- **you must** not store any Council information on your own equipment at home
- if working from home, **you must only print material** if you absolutely have to, and if the information is sensitive, only with approval from your SAIRO. All printed material should be stored and disposed of securely. For more information about Working from Home click **here .**

9. Payment card industry requirements

All staff have a responsibility for ensuring the Council's systems and data, and data relating to our citizens and service users, are protected from unauthorised access and improper use.

If you handle payment cards and the data associated with them, you must ensure:

- cardholder information is handled and protected in a manner which is appropriate for information carrying a high level of sensitivity
- information from cardholders must not be stored and should be securely destroyed after use
- personal data relating to a card is not disclosed
- accounts that hold cardholder data and records of transactions that relate to them are held securely
- passwords that relate to cardholder data are held securely, and never shared
- desks, counters, till points etc are left clear of sensitive cardholder data
- card details are not kept on any computer or in email. It is strictly prohibited to store the contents of the payment card magnetic stripe (track data), or the CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever, and the Personal Identification Number (PIN) or the encrypted PIN Block under any circumstance
- all data is securely disposed of when no longer required, regardless of the media or application type on which it is stored. All hard copies containing the full card details must be manually destroyed when no longer required
- information security incidents relating to payment card information are reported, without delay, to the Data Breach Team at databreach@glasgow.gov.uk using the Data Security Incident Reporting form which can be found here and in line with the Council Data Incident and Breach Procedure
- you seek advice from your line manager in the first instance, if you are unclear about any aspect of handling payment card information.

Managers with responsibility for processes that involve card payments must ensure:

- the approved list of card payment technologies and devices and personnel with access to such devices is maintained. Managers are responsible for notifying **Pay360@glasgow.gov.uk** so that the asset register for all point of sale /chip and pin devices can be updated
- requests to establish new cardholder software, hardware, third party connections, etc, are made through your **SIIT Business Partners** and will be subject to the standing processes for reviewing and approving such requests
- devices, including chip and pin devices, must be inspected either daily, weekly, or monthly for tampering as agreed by your service and the dates of inspection must be recorded. Types of tampering can include additions of card skimmer hardware or a swapping of devices. A list of serial numbers for all devices will be held per service area and the ownership and updating of the list will be the responsibility of that service and should be checked at least twice a year.

10. If something goes wrong - who should I contact?

If you need to report an issue here are the contact details:

1. Lost or stolen information or equipment – please report this immediately

- report missing equipment to your **CGI IT Service Desk by phone on** extension 74000 (0141 287 4000 from an external line) **or email** at **GCCservicedesk@cgi.com**
- report lost information to **your manager** and immediately email a completed data breach form to **databreach@glasgow.gov.uk**

2. Lost or stolen payment information or chip and pin equipment – please report this immediately

- report missing equipment to your **manager and email** **Pay360@glasgow.gov.uk**
- report lost information to **your manager** and immediately email a completed data breach form to **databreach@glasgow.gov.uk**

3. Virus or threat to network – first isolate the device from the network then report to CGI IT Service Desk

- **by phone on** extension 74000 (0141 287 4000 from an external line)

4. Mis-use of Council equipment or information – you can report this to

- Your manager
- phone the Whistleblowing Hotline on **0141 287 3777** or use the online form that can be found **here.**

In the case of information, further details can be found in the Council Data Security Incident and Breach Procedure

11. Failure to comply

Failure to follow, or deliberate actions to circumvent, our **Information Security Policy**, related policies. or the guidance in this document is a breach of your conditions of employment and can result in disciplinary action, up to and including dismissal in serious cases.

12. Staff support

All staff, volunteers and temporary workers are required to complete the Information Security course on an annual basis.

This course can be completed through our online development programme on GOLD by clicking **here** or through a face-to-face training session or handout for non-PC facing staff.

If you have not completed this course, **please speak** to your line manager as soon as possible to arrange a time to complete it.

For more information

- contact your SAIRO - details can be found **here**
- contact your SIIT Business Partner. The list of SIIT Business Partners can be found **here**
- phone the **CGI IT Service Desk** on extension 74000 (0141 287 4000 from an external line) or email at **GCCservicedesk@cgi.com**
- contact the Head of Information & Data Protection Officer by email at **AssetGovernance@glasgow.gov.uk**
- visit **Connect**