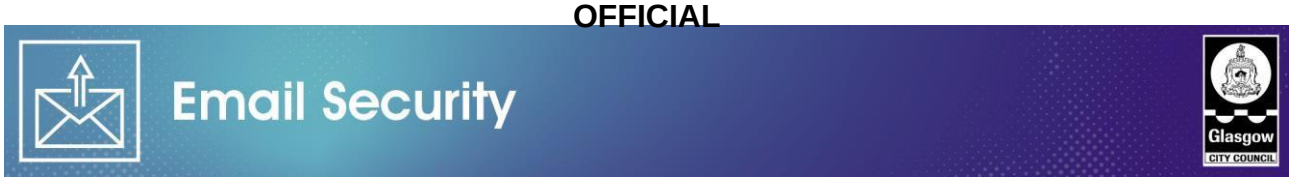


Guidelines for staff using email and messaging services

Updated September 2023

1. Introduction

Email systems play an essential role in our day-to-day business, helping you work more efficiently. Whilst the highly accessible and easy to use nature of text and other types of messaging services makes it attractive for communicating short messages quickly.

We are committed to **making sure** that our email systems and messaging services are used responsibly. These guidelines have been written to **make sure** staff are able to do so.

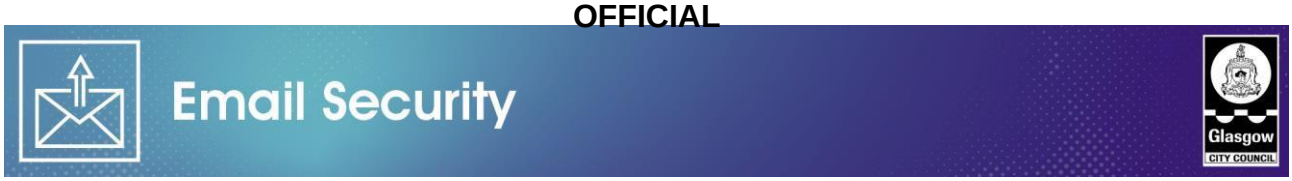
Please read these guidelines carefully. If you need more information, contact the CGI IT Service Desk on extension 74000.

2. Scope

These guidelines support our Acceptable Use of IT Policy and Information Security Policy. They will help you comply with the requirements of using our email systems and messaging services available through your council provided equipment. They highlight good practice **you should** follow when sending and receiving emails and messages at work and everyone who is authorised to use our email systems and IT and communications equipment which offers messaging services, such as employees or contractors, should follow them.

The use of our email systems and IT and communications equipment by other people, who are not members of staff or agreed contractors, **must be** supervised and governed by a binding agreement (for example, our Acceptable Use Policy for school pupils) and their use **must follow** these guidelines. The agreement **must be** signed by the user/contractor and retained by the Service responsible. Where our council disciplinary procedures **do not** apply, local arrangements **must be** put in place to **make sure** that this agreement and our Acceptable Use of IT and Information Security policies are enforced and followed.

If you fail to follow these guidelines it may bring serious risk to the council and could result in disciplinary action, including dismissal in certain circumstances, and even legal action.

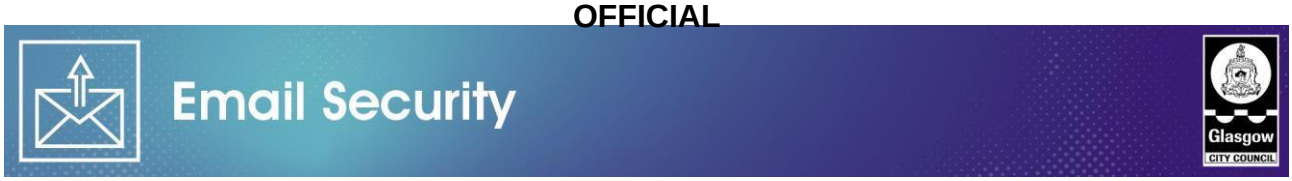


These guidelines refer to all electronic messaging systems including:

- our internal email systems
- internet mail systems
- webmail
- email on mobile devices
- email systems used by our staff in schools and other educational establishments
- secure email (encryption)
- text messaging
- chat, (for example, using MS Teams)
- messaging via social media platforms

3. Contents

Readers should familiarise themselves with all sections which are summarised here:



Personal information
Freedom of information
Using emails or messages for marketing or notification
Email message and mailbox size
Chat
Retention, disposal and archiving
Bulk email and messaging
Personal emails and messages
Use of business email address
Your profile photograph in email and other applications

4. Summary of acceptable use and good practice

MANDATORY

You must:

- conform to all relevant Glasgow City Council policies, including the Information Security Policy and the Acceptable Use of IT Policy, when using email and messaging services
- connect your PC, laptop or tablet to the network at least once every 30 days to make sure that the anti-virus software on your device is up-to-date and your login account is not deactivated
- regularly connect your council issued phone to WiFi to receive any software updates that are due
- use BCC (Blind Carbon Copy) in email, and Groups in text messaging to keep addresses confidential when sending messages to a group who have not agreed to share their addresses
- contact the CGI IT Service Desk if you want to send bulk emails or texts to external recipients
- remember that emails and other message types are a form of business correspondence.
- please take care over what you write, as some comments may give offence when read out of context
- remember that anything you say in an email, message or chat may have to be released under Data Protection or Freedom of Information laws
- protect your account or device from unauthorised access
- set an autoreply if you are not going to be able to access your email or messaging services advising what a sender must do if the matter is urgent
- arrange for your mail to be dealt with promptly in your absence.
- apply an appropriate protective marking to your correspondence before you send it.

MANDATORY

You must not:

Email Security

- make personal use of email or text except as permitted in the Acceptable Use of IT Policy
- send racist, sexist, obscene or offensive material
- store, display or transfer unlicensed software
- engage in illegal activities
- send libelous or defamatory messages.
- make statements that conflict with the council's policies
- auto-forward email to external email systems
- email or message sensitive or personal council information to your personal email account or phone.
- send emails or text messages containing personal information to non-secure external email and networks unless you have the consent of the recipient
- undertake any financial transaction you have been asked to do from an urgent email or text you have received until you have verified that the sender is genuine and you are authorised to complete the transaction.

ADVICE ON GOOD PRACTICE

You should:

- check your email and messages regularly - at least daily
- make the subject of your message clear in the 'Subject' line
- let the sender know if you are not able to deal with their request promptly - the automatic receipt request is no substitute for a personal acknowledgement
- include contact details in every message in line with the council guidelines.
- set your Outlook to include your email signature in both new emails and forwards/replies
- identify yourself accurately and clearly, unless your personal privacy or safety is at risk.

You should not:

- give out your email address or mobile number unnecessarily, as it increases the risk of spam
- send messages all in capitals as it looks like you are shouting at the recipient
- send an angry reply without careful consideration, as comments can seem harsher in email and text, without voice tone or two-way discussion to balance the words
- use emoticons, for example 'the smiley face' :-), or emojis in formal writing.

Please read these guidelines carefully. If you need more information, contact the CGI IT Service Desk on extension 74000.

5. Authorised access and advice

Authorised access to our email system may be obtained by sending a User Access Form to the CGI IT Service Desk.

Text messaging normally comes as a standard feature of council issued mobile devices. If your work pattern requires it, you will have been authorised to use it, and been issued with a mobile device by your manager.

Certain council business functions may also use text or other messaging types as a tool to communicate short, simple messages. For example, messages to service users to remind about appointments or to notify about an unplanned school closure due to weather, or school attendance.

6. Monitoring

We have automated tools that scan all email messages and record the volume of email on our system. This is done to protect against viruses, protect against inappropriate or malicious material being passed through our systems, and to help administer the system. We take all reasonable steps to respect your privacy in line with the council's Privacy Statement, whilst upholding our obligations as both your service provider and employer. However, we may have to access the contents of your emails and texts for various reasons.

This can include:

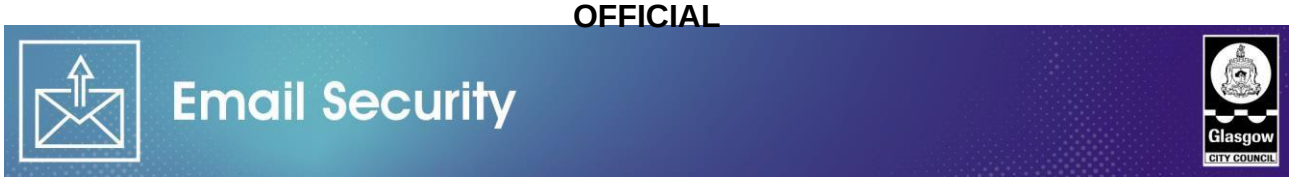
- making sure our business procedures and security procedures are always being followed
- helping to maintain the effective operation of our IT systems
- the need to conduct council business in an employee's absence
- preventing/detecting unauthorised use of communications systems, criminal activities or other serious misconduct
- providing information to individuals or outside agencies, as required by data protection law and the Freedom of Information (Scotland) Act 2002.

More information can be found in the **Privacy Statement for Managing the employment relationship between GCC and an Employee** which can be found here.

7. Security

USING OUR EMAIL SYSTEMS and MESSAGING SERVICES

Our email systems have many security features and it is the recommended method for you to send and receive email. Web-based email systems are not as reliable or secure, and



should not be used for official council business unless you have been given appropriate authorisation to do so.

As a result, access to such web-based email systems is blocked for most users.

Please note that if you are given the appropriate authorisation and use a web based email system for any business correspondence, this correspondence is still covered by these guidelines.

You would need to provide copies of relevant correspondence in response to a Freedom of Information or data protection request covering the information contained in it.

Mobile devices provided by the council usually come with a messaging function which provides a quick and easy method of communication. However, users need to be conscious of information security and in particular, data protection considerations, when using this facility.

From time to time, there may be a need for a member of staff to communicate with another member of staff using a personal, non-council issued, mobile device. If this is the case, information exchanged should be kept to a minimum and should not be sensitive in nature.

Under no circumstances should a member of staff use a personal, non-council issued mobile device to communicate with a service user.

PROTECT YOUR EMAIL ACCOUNT AND MOBILE DEVICE AGAINST UNAUTHORISED USE

Authorised email users are given a user ID and password for a network account which provides access to email. Mobile devices issued to staff, which provide access to messaging services, require a password to be entered before they can be used. **You must** maintain security of our email systems and your mobile device by:

- choosing a password that can't be guessed
- not telling your password to anyone else
- changing your password every 30 days, or sooner if you suspect someone else may know it
- not letting anyone else use your account or mobile device
- not using anyone else's account
- not leaving your PC unlocked or unattended when you are signed into the council network
- do not leave your mobile device unattended.

If someone else needs to access your email account (for example, a job share partner or deputy), **you must** use 'delegate permissions', rather than giving them your account name and password. You can find out how to do this by accessing the Help pages on Outlook. Read our guidance on managing your passwords.

Email Security

VIRUSES

Viruses are harmful programs that spread by copying themselves from computer to computer. They are a serious threat to our systems and often use email or messaging services to spread rapidly across the Internet.

You must not open any files, messages or attachments unless the council issued PC, laptop, tablet or mobile device you are using is protected by up-to-date council-approved virus protection/security software. You must make sure that your device is up-to-date by connecting to the council network at least once every 30 days, or if using a council iPhone, regularly connecting to WiFi and updating the software.

Contact the CGI IT Service Desk if you have any doubts about whether you are protected.

Internet email is checked for viruses as it leaves or enters our network. If a message to you is infected, or if the system cannot check it, it will be quarantined and you will be informed. Infected messages will not be released from quarantine. If the message has been quarantined for other reasons you will need to read the instructions included in the notification sent to you carefully. **You must not** ask for messages to be released from quarantine unless you have checked with the sender that the message is genuine. Although these measures are highly effective, **you should** still be cautious about opening files attached to messages or links within messages, particularly where:

- they come from an address or telephone number you don't recognise
- the message does not make sense, refers to previous correspondence that you have never seen or is not business-like.

If you have doubts about whether an attached file or link is safe, check with the sender if they are known to you, and the CGI IT Service Desk for advice.

SPAM

Spam is the nickname for unsolicited marketing messages received by email and text, and its volume or content can cause problems to our network or fill up space on your device. If you can tell that a message is spam from its subject title or sender details, you can right-click on it and select "Block Sender". This will also move it to your Junk folder. Please **do not** reply to it, even to opt-out of receiving more email or messages, as this can confirm to the sender that the message has been read, encouraging you to receive even more spam emails or messages.

Spam may be sent directly to the 'Junk' folder in your email account's Inbox. **You should** check this folder regularly to determine if there are inappropriate messages in it that **should be** reported, or if there are legitimate business messages that have been sent to this folder in error.

Email Security

If you have a concern about a particular message which appears to be SPAM, you can report it to spamreport@glasgow.gov.uk .

If the amount of spam you receive is interfering with your duties, report it to the CGI IT Service Desk on extension **74000.**

CYBERCRIME

Cybercrime is a growing threat for everyone who uses email and messaging services. **You must** always make sure that any email requests or messages you receive are genuine and where possible, verify the sender before you complete anything the email or message asks you to do. This is especially important if the email or message asks you for financial details or personal information.

Three forms of cybercrime in particular are on the increase – **Phishing, Spear Phishing and Ransomware**.

PHISHING

Phishing is a type of fraudulent email or message request which attempts to obtain funds from us or gain access to information which **may result** in a crime being committed.

If the email or message you have received asks you to send personal information or complete a financial transaction and this is not normally part of your usual procedures, **you must** phone the sender of the email or message using separate contact details. That is, **don't use** the contact details contained in the email or message. **You can** use the telephone directory on Connect to search for the sender's details (if internal) or the BT telephone directory or similar (if external).

Never contact any telephone number detailed in the email or message you have received to call the sender as this **may not** be genuine and could mislead you.

SPEAR PHISHING

Spear phishing is a specific form of phishing which targets individual officers, usually those who work closely with our finances, but any member of staff could be a target. They receive an email or other type of message which they think has come directly from a council or ALEO senior officer, such as the Chief Executive or a Director, asking for an urgent payment to be made, or for information on how to make an urgent payment. Staff receiving these emails and messages might believe they have received a genuine request as the email address or contact details, and signatures look legitimate. Again, **you must** phone the sender of the email or message using separate contact details. That is, **don't use** the contact details contained in the email or message. **You can** use the telephone directory on Connect to search for the sender's details

RANSOMWARE

Emails sent with the intention of committing a crime may contain encryption software,

known as **ransomware**, in an attachment or through a link. This is malicious software that scrambles the data on your computer and asks for payment to restore your data to its original state (although there is no guarantee that this will actually happen).

Ransomware has been around for a few years, but generally there has been a significant increase in these types of cyber-attacks, particularly against public organisations, such as schools and other local government departments. If the ransomware is contained in an attachment, a victim will see an email addressed to them, which appears legitimate. They will open the email and may open its attachment as it appears to be relevant to the content and of interest. However, this attachment contains the malicious ransomware code and by opening the attachment the ransomware code is activated.

Alternatively, the email might contain a legitimate looking URL link, but when a victim clicks on it, they are directed to a website that infects their computer with this malicious software.

We must all be aware of how to recognise a phishing, spear phishing or ransomware email or message, and what **we must do** if we get one.

What to do

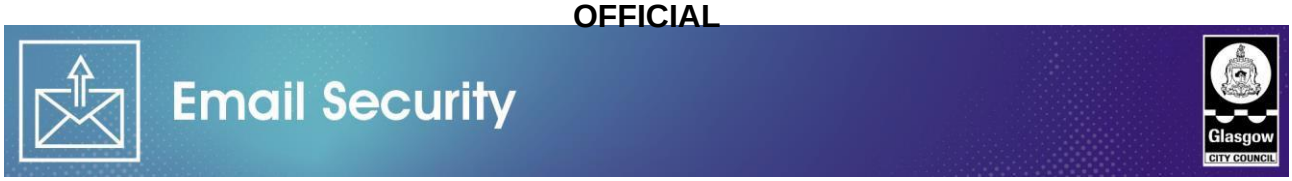
- Be wary of all unexpected emails, embedded links and attachments that you receive.
- Be aware of the titles of email attachments which are incentives to get you to open them, such as 'you will never guess who I met on holiday!'
- If you receive an urgent, or unusual, email payment request you **must not** process it, nor open any attachments or click on any URLs within the email unless you have actually spoken directly to the person who sent you the email and confirmed it was a genuine request.
- If you are in any doubt and think the email is of a suspicious nature - please email Internal Audit at integrity@glasgow.gov.uk immediately.
- If you have clicked on something in the email and activated the ransomware you must contact the CGI Service Desk immediately on 74000.

PERSONAL FRAUD

Where individuals rather than the council are the target of fraud, for example, if you are asked to provide your personal bank account details or to assist in the illegal transfer of funds, **you must** report this to your line manager and to Trading Standards (CATS), who work with Police Scotland on this issue, by email to ts.enquiries@glasgow.gov.uk or phone **0141 287 1061.**

HOAXES

If you receive a warning of a security threat from someone other than the CGI IT Service Desk, **do not** pass it on to your colleagues, as it may be a hoax, or the advice may not be appropriate for our systems. Instead, report it to CGI IT Service Desk.



OFFENSIVE MESSAGES

If you receive an offensive message, notify your line manager, who may decide to contact the CGI IT Service Desk for further advice.

EMAIL ENCRYPTION

The council has implemented a facility called Transport Layer Security (TLS) which means that all emails sent from the Council's email domain to another government domain, including the NHS and Police, will automatically be encrypted, and therefore be secure, while in transit between the organisations.

Emails sent to other domains will also be encrypted in transit if the recipient's domain also has TLS switched on. As a guide, all the main Internet Service Providers (ISP) tend to have TLS switched on by default, but if you intend sending sensitive information and you are unsure if it will be encrypted in transit, contact the intended recipient before you send the email and ask them to check with their ISP if TLS is enabled.

SECURE EMAIL TOOL

The council also has a Secure Email tool which is available to all staff through the council email system.

If you want to send sensitive information Secure Email allows you to encrypt your message. The recipient receives an email requiring them to click on a link to register with the service in order to retrieve the email.

If you are sending sensitive information and the Internet Service Provider of the person you are sending the email to has TLS switched on you **will not** need to use Secure Email as TLS will automatically encrypt the email.

Support material for the use of Secure Email can be found here.

PROTECTIVE MARKING

Protective Marking is a tool that is used in conjunction with Outlook, the council email system, to add a label to your message. It is used by the user to classify the email depending upon the nature of the content and its level of sensitivity. This visual classification is regardless of whether the email is being sent internally or externally and is used to determine what level of protection must be applied to the document to maintain its confidentiality, integrity and availability.

To make it easy to apply Protective Marking, the council uses a tool within Outlook. This allows you to mark your email and any attachments simply and quickly. More information about Protective Marking can be found here.

Email Security

Contact your Service/ALEO Information Risk Owner (SAIRO) or CGI IT Service Desk for advice on handling confidential information. The list of SAIROs (Information Security Board representatives) can be found on Connect here.

You must not send personal data (information relating to an identifiable living individual) to or from your private/home email address. You can reply to a citizen's own email address, preferably using a secure method (unless from the content of their message they expect you to reply by the same unsecure process and have given consent). The standard council email footer sets out the conditions under which the email has been sent.

If you are in any doubt, please speak to your line manager, SAIRO or the CGI IT Service Desk.

SENSITIVE INFORMATION, EMAIL AND MESSAGING SERVICES

General good practice when using email is to keep sensitive information to a minimum.

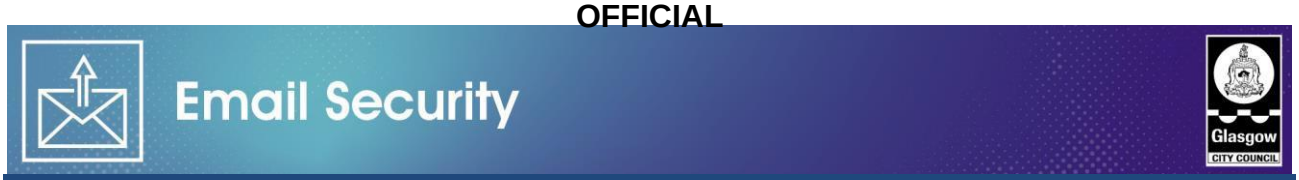
You must not under any circumstances send sensitive information to colleagues, third parties or customers using other messaging services – as these are not considered to be secure. Therefore, you must avoid naming individuals, listing addresses, contact details and case information in other message types.

AUTO-FORWARD EMAIL FUNCTION

You must not set up the auto-forward function or use Outlook's Out-of-Office Assistant to automatically forward your email to an external email address, such as your own personal, non-work account. This process can affect the efficiency and security of our email system by:

- **causing email looping** - for example, if you auto-forward messages to a mailbox that becomes full or breaks down, then you get error messages in response. Your auto-forward will then send the error messages back to the broken account and you will then receive another round of error messages back in return. This process will keep happening.

- **auto-forwarding** means that you are not able to assess whether an email message contains sensitive or personal data before you send it on. Our Information Security Policy prohibits you from sending such information across the Internet (email systems) without sending it securely, such as encrypting it. There is a serious risk that someone may send you confidential information, expecting it to stay inside our council IT system. If you use the auto forward email function you are then sending it outside our secure IT network without encrypting it.



8. Email, messaging services and the law

PORNOGRAPHY

Storing or sending images that contain child abuse or exploitation is a serious criminal offence. If you have received or suspect you have received images that contain child abuse or exploitation by email or other messaging services, you **must** report it immediately to your line manager and to Internal Audit, who will advise on how to proceed. **Do not** attempt to investigate further without the approval of Internal Audit, who can be contacted at:

Head of Audit and Inspection
City Chambers
Glasgow,
G2 1DU
Phone **0141 287 4053**

Storing or sending adult pornography or links to such material from a work email account or mobile device is also prohibited. Further information can be found in the Council Code of Conduct and the Acceptable Use of IT Policy.

DEROGATORY AND DEFAMATORY STATEMENTS AND INCITEMENT TO HATRED

Both you and the council may be liable for prosecution or other legal action if your email or message contains derogatory, defamatory, offensive, racist, libelous, or slanderous statements, or if it could be seen as inciting hatred against a particular group or individual. Use of email or messaging services to bully or harass anyone is prohibited and any incidents of bullying or harassment may result in disciplinary action in terms of the relevant policies.

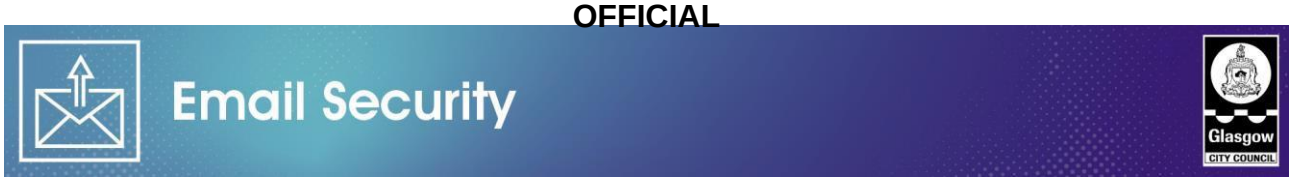
PERSONAL INFORMATION

The Data Protection Act 2018 contains rules on how we should handle any personal information entrusted to us. Breaching data protection rules is a very serious matter. Further information is available by phoning the Customer Care team phone **0141 287 0900**, from Legal Services, or on Connect click here.

FREEDOM OF INFORMATION

Glasgow City Council is a public authority, and therefore, in compliance with the Freedom of Information (Scotland) Act 2002 the council may have to release information to the public within 20 days of a request being made. This can include correspondence through emails and other message types, and also chat functionality.

It is therefore important for all staff to file emails properly and regularly in order to access information efficiently and when needed. You should regularly delete emails and other messages which are no longer required. Similarly, systems used to send other messages **must include** a suitable method for retrieval if required.



If you are going to be absent for more than one day, please **make sure** that any FOI requests in your absence will be dealt with promptly. You can use delegate permissions in Outlook to let a colleague deal with your email, or you can use the auto forward function to send your email messages onto a colleague's internal email address. Instructions on these methods can be found in the Help pages in Outlook.

USING EMAILS OR MESSAGES FOR MARKETING OR NOTIFICATION

These activities are principally governed and regulated by data protection law and the Privacy and Electronic Communications Regulations 2003 (amended 2011). Section 11 of the Data Protection Act refers to direct marketing as 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'. The Information Commissioners Office (ICO) regards direct marketing as covering a wide range of activities that apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals.

Although some activities undertaken by the council **may not** directly fall within the Privacy and Electronic Communications Regulations 2003 (amended 2011), sending appointment reminders, for example, by email or message could potentially fall within the regulations, and require the standards outlined in this guidance document to be followed.

Where citizens and service users are the intended recipients of a communication via email or message, the consent of the individual **must be** obtained and recorded **before** this method of communication commences. The message **must also** make it clear that it has been sent from Glasgow City Council.

It is good practice to make recipients of this type of service aware of their responsibility to inform the council of any change to their contact information and of the potential risks of communicating with them by less secure methods. Citizens and service users must be given the opportunity to decline use of this method of communication, and any message itself **must contain** a point of contact or method by which the recipient can opt out of future messages.

These requests **must be** recorded and actioned.

All message types stored on council systems and equipment are subject to the same data protection and Freedom of Information obligations as other information. Council staff **must therefore** make sure these aspects are fully considered and risk assessed before using a messaging service.

EMAIL MESSAGE AND MAILBOX SIZE

The council email system **is not** intended to be a document management system and large mailboxes slow the system down for all users. Please delete messages you no longer need and **do not** store attachments in your mailbox - store them within your file plan area in our Electronic Document and Records Management System (EDRMS).

Email Security

You should keep your email messages and attachments as small as possible, preferably below 1Mb (megabyte). Best practice, where possible, is that you send an EDRMS link to your colleague or other member of staff advising where to find the document and other relevant information. This is particularly helpful for emails sent within a single team and where all team members have access to the same file plan area in EDRMS. Image files in certain formats are very large, for example, TIFF or BMP format.

Where possible, **you should** send image files in more suitable formats, such as JPEG and GIF. If you need help on how to do this contact the CGI IT Service Desk.

There is a size limit of 30Mb (megabytes) on messages to and from the Internet. Messages larger than that **cannot** be sent.

In Outlook you will experience poor performance if your folders contain large numbers of items. To help avoid this you should carefully manage the number of items you have stored in your frequently used (core) folders such as the Inbox, Calendar, Contacts and Sent Items. CGI and Microsoft recommend that you maintain a maximum of 3,000 items in these core folders. For other folders, CGI recommends that the number of items does not exceed 5,000 to maintain an acceptable performance level.

CHAT

The content of online chat discussions, such as those stored in MS Teams, 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.

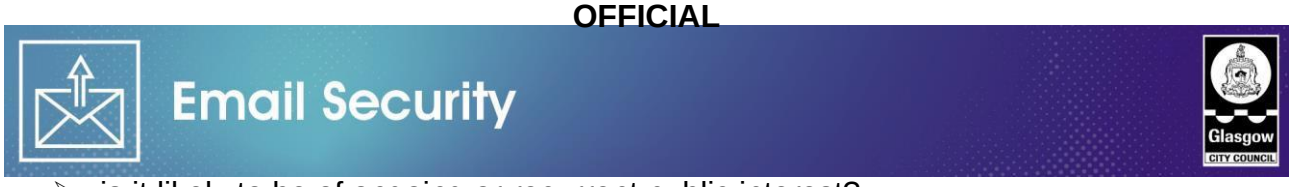
RETENTION, DISPOSAL AND ARCHIVING

To make sure that our email system **does not** fill up with old, unwanted messages, **you must** delete messages that you no longer need as soon as possible. **This must** be in line with our Records Retention and Disposal Schedule (RRDS) which you can find on Connect here.

If the email contains material information about a council activity or decision, you should move it to an appropriate folder in your file plan area of EDRMS. If your ALEO does not currently use EDRMS you should save it in a networked central drive. This removes the email from the system but still allows you to access it when you need to. **Please note that you should move the email before it is archived so that other members of your team can access it in EDRMS as necessary.**

In line with our RRDS consider the following when deciding if your email is an official record and should be kept:

- is the email required as evidence of the day-to-day operation of council services?
- is it required for legal purposes (for example, related to a contract)?
- does any legislation or official regulation govern how long it must be kept?



- is it likely to be of ongoing or recurrent public interest?
- does it record a decision or action which isn't recorded elsewhere?

Previously read messages of other types take up space on mobile devices and can affect their performance. Therefore, if you have a council mobile device and you receive messages **you should** get into the habit of regularly deleting these from your phone. Texts and other types of short messages are intended for brief and convenient communication.

They **must not** be used for sending sensitive information and it is anticipated that a requirement for retaining any information they contain will be by exception. In rare cases where the content of a message requires to be retained for one of the above reasons, the content **should be** noted and transferred to proper storage.

BULK EMAILING and MESSAGING

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 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 messaging applications can be used to achieve this. For larger distribution lists, contact the CGI IT Service Desk for assistance.

PERSONAL EMAILS AND MESSAGES

Personal use of email and messaging services is permitted in certain circumstances, as described in our Acceptable Use of IT Policy which can be found on Connect click here.

This policy describes when email and messaging services can be used for personal purposes. It also sets out a number of cases where the personal use of email and messaging is **not permitted** on our networks. Any personal use of email or messaging **must also** comply with these guidelines.

Personal emails and messages remain records held by the council and may therefore be accessed by management when necessary and may be disclosed under Freedom of Information and/or Data Protection laws. If you would not want someone outside the council to read the email or message, think very carefully about whether you should be sending it at all. Council email or messaging services should also **not be** used for personal purposes where views expressed might lead the recipient to incorrectly believe that the views expressed are those of the council, or council reputation may be damaged.

USE OF BUSINESS EMAIL ADDRESS

Your business email address should **only be used to subscribe to mailing lists and services that are relevant to your work.** You should not use your business email address for subscriptions 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.

YOUR PROFILE PHOTOGRAPH IN EMAIL AND OTHER APPLICATIONS

A profile photo for employees has become more common in emails and other applications as staff find it useful to be able to see who it is they are communicating with. This trend is due, in part, to the extensive use of profile pictures in social media.

All images uploaded to Email, and other Messaging Services are visible externally.

In the council email system, you can choose to add either a **profile picture** or a **copy of the corporate identity** for the organisation you work for – such as the Glasgow Marque or the GCHSCP logo.

If you choose to add a profile picture you are giving your consent for this to be viewed out-with the council network. Your profile picture should be **portrait and professional**, a passport style head and shoulders image of yourself. Images of anything else other than the approved logos must not be used. The use of illustration, clip art or cartoons and so on are not appropriate.

We encourage staff to take a responsible approach to this, as you are representing the council.

There is no requirement to add a profile picture if you choose not to do so.

9. Further guidance and information

For further guidance on information security, you should complete the Information Security course on GOLD. This course **must be** completed, each year, by every member of the council family to comply with core policies.

The course is monitored, and you will be reminded if you have not taken it for that year. Please speak to your line manager if you need an alternative format of the course or more information.

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

.