(I) Digital Information Councillors' Code of Practice

Introduction

The purpose of this Digital Information Councillors' Code of Practice is to ensure the effective protection and proper usage of digital information systems for all aspects of Council activity.

The Digital Information Councillors' Code of Practice assists in maintaining systems at operational level, ensuring cyber security risks are minimised and protecting the Council reputation.

Key aspects to be mindful of on use, sharing and protection of digital information include:

- Confidentiality
- Data Protection
- Transparency
- Cyber Security
- Ethical Use
- Prevention of Damage to Reputation

Contraventions of the Digital Information Councillors' Code of Practice could seriously disrupt the operation of the Council, and any breaches will be treated seriously.

Breaches of cyber security, Data Protection Act 2018, and General Data Protection Regulation (GDPR) could lead to significant financial penalties and losses.

Contents

1) Email Usage and Phishing Protection
2) Use of Council Mobile Devices
3) Data Protection and Management
4) Password and Second Factor Authentication
5) Cyber Security
6) Council Data Networks
7) Cyber Incident Response
8) Social Media
9) Printing
10) Use of Artificial Intelligence
11) Breach to Code
12) Acknowledgement and Acceptance

1) Email Usage and Phishing Protection

- Douglas City Council email accounts must only be used for Council related activities.
- Councillors must not use the Council allocated email address for services or communications that related to personal, business or commercial purposes not related to the Council activities.
- Non-Council business related email addresses may be blocked at any time without notification and the Council will not be liable for any failure of delivery of a personal related email.
- If an email account shows a high number of SPAM emails being received. Consideration should be given to unsubscribing to services they may have subscribed to in the past.
- Councillors must take care when receiving emails, only clicking on links and attachments from trusted sources, if there is any doubt contact Digital & Information Services for advice and assistance.
- The Council's e-mail system must not be used to send illegal or inappropriate material.
- General Data Protection Regulations and Freedom of Information Legislation apply to all emails on the Douglas City Council system. Emails will be managed in line with Councils Document Retention Schedule and Policy.
- Global distribution lists should be used appropriately. Councillors should take care to consider their audience before using the Reply All option to ensure their target recipients are correct.
- Confidential material sent by e-mail should be so marked but sent only with caution and care must be taken to ensure emails are not sent in error.
- Emails must be sent in accordance with the Data Protection Act 2018. Personal and sensitive data must be protected appropriately. Outlook 365 users are to use Outlook encryption where required and available.
- Councillors should use official email addresses to communication to Council staff.

Councillors must not communicate to staff regarding Council related business on Non-Corporate Communication Channels (NCCC's). This includes the use of their own or staff NCCC's.

Such NCCC's applications include but are not limited to:

i. Gmail
ii. Hotmail
iii. Manxnet
iv. Whatsapp
v. Facebook Messenger
vi. Snapchat
vii. Apple Imessage
viii. SMS/Text

Record keeping: if any significant information is received by staff via a NCCC's this information should be copied, forwarded or noted on a Council system i.e. @douglas.gov.im email.

The use of NCCC's impacts the Council ability to adhere to Subject Access Requests, Freedom of Information requests and its data retention policy.

The use of NCCC's impacts the ability of the recipients to identify if the sender is valid and not a security risk.

- The Council retains the right to access, monitor and view all emails sent and received by the email system. This right is exercised solely through Digital & Information Services on the instructions of the Chief Executive Officer or Head of Digital & Information Services.
- An external protection system is used to automatically filter and classify all incoming and outgoing emails. A notification email is sent to users on a daily basis on any emails held in quarantine. Email attachments which are deemed to be high risk will be rerouted to DCC administrators for review. Some email addresses are blocked to protect the system. This may apply to incoming and outgoing files as required by safety rules in force at any given time.
- Emails should only be released from quarantine if the Councillor believes the email is safe, from a known and expected source. Releasing an unknown email from an unknown source may seriously endanger Council systems.
- If a Councillor is concerned that genuine emails are being blocked, they should contact the Digital Service Desk and the sender can be added to an allowed and approved senders list if deemed safe.

2) Use of Mobile Devices

- All mobile devices issued by Douglas City Council will have mobile device management software installed on them where applicable.
- To prevent unauthorised access, the security and safekeeping of portable and other equipment used is the responsibility of the Councillor using it. If a Council device is lost or stolen, it must be reported to Digital & Information Services immediately.
- Reasonable and appropriate personal use of Council equipment is permitted. Inappropriate use of any equipment provided is not permitted - for clarity, this would include access to, or storage of, pornographic material, use of gambling sites, illegal activities, disreputable sites, or anything that may bring the Council or individual into disrepute.
- Member may use their own equipment i.e. smartphone, laptop, PCs to access web base services provided by the Council, such as Email and First Agenda, this equipment must have up to date security and virus protection. The Councillor is responsible for the security and operation of these devices.
- Councillors must ensure Council data cannot be viewed by non authorised persons at any time or by CCTV when in a public place.
- Only use Council devices where it is safe and legal to do so.
- Douglas City Council reserve the right to charge for the cost of damage if due to repeated or reckless behaviour.

3) Data Protection and Management

- Members are Data Controllers in their own right and are responsible for ensuring adherence to General Data Protection Regulations, the Data Protection Act 2018.
- The Council acts as the Data Processor for the provision of the Council services including @douglas.gov.im email and First Agenda systems.
- Members must act in accordance with the Freedom of Information Act 2015.
- As a condition of use, Members consent to the Council as Data Processor to if required examine of the use and content of all data/information processed and/or stored by the Member on the Council's systems as required.

4) Passwords & Second Factor Authentication

Councillors are advised to always use strong passwords following the National Centre for Cyber Security guidance:

The password system should comprise of:

- Three random word format to be used for creating the passwords.
- Password minimum of 12 characters.
- Password required to include at least one non alpha character.

Passwords comprising of personal and family information i.e., names, dates, hobbies, favourite things or information obtainable from social media are not to be used.

- The user account will lock out after 3 unsuccessful log-in attempts.
- Councillors are responsible for the security of their password which they should not divulge to anyone else.
- Online applications will enforce their own password rules, these accounts will be managed by the Councillor in accordance with those rules.
- If suspected that a password may have been compromised or someone else knows the password a password reset request must be made.

Second Factor Authentication is to be used wherever available. This is where sign in credentials are associated with a second device or application that the user always has with them. This is to ensure online access has the appropriate protection for online services. This applies to the provision of services such as: Microsoft Office365 email and First Agenda (From April 2025).

5) Cyber Security

- Councillors are advised to take care when accessing websites and act to minimise threats to their system.
- Threats include Malware which is malicious software which may be inadvertently download onto your device and ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting it. A criminal group will then demand a ransom in exchange for decryption.
- General advice and guidance and be found on the National Cyber Security Centre website at https://www.ncsc.gov.uk
- If there are concerns Councillors should notify the Digital & Information Services immediately.

6) Council Data Networks

- Access to the Council's internet network, both wired and wireless (Wi-Fi) is provided for Council purposes only. Limited personal use is permitted on Council provided devices during office hours.
- Access to and usage of the Council's internal networking services is restricted to authorised devices only. This includes the wireless network "Mac Auth". Where available the Council public Wi-Fi can be used by personal devices.
- Monitoring and control systems are in place and will be used by Digital & Information Services to manage the performance and security of the Councils network.

7) Cyber Incident Response

In the event of a suspect Cyber Security Incident involving Council systems please ensure this is reported as soon as possible to the Digital Services Team who will follow a planned response appropriate for the incident detailed in the Cyber Incident Response Plan.

This may include:

- Locking a user account.
- Removing the user's pc or device from the Councils network.
- Blocking access to any server or application.
- Removing access to systems.
- Removing access to the whole network.

8) Social Media

Guidance received from the Information Commissioner states Councillors must make clear on any social media accounts that the account belongs to an individual or if they are operated and owned by the Council.

All communications through the internet and social media with reference to Douglas City Council must not bring the Council into disrepute.

Be aware that Councillors are personally responsible for the content they publish on any platform of social media, whether it's published on a personal account or not. It's highly recommended that you never post or share anything online, or on any social media account, that you would not be comfortable saying or sharing in a public meeting.

This includes but is not limited to the following. You must not:

- Post inappropriate links or content.
- Agree or condone inappropriate comments that are offensive, discriminatory or bullying.
- Breach confidentially.

Understand what you can and can't post online, including legally

Councillors are personally responsible for the social media content they create, publish and share. Being a councillor will not prevent someone else pursuing legal action following the publication of an untrue statement. In such a situation, it is likely that you will be held personally liable.

Councillors should be mindful of the difference between fact and opinion. They also play a central role in preventing the spread of disinformation. Think twice before you press 'share' or 'retweet'!

On social media, Councillors should also keep in mind their responsibility in relation to confidential information, copyright, data protection, the pre-election period and exempt reports. Councillors are still subject to the Code of Conduct on social media where there is an explicit link between the content posted and council business or your role as Councillor. As a general rule, Councillors should demonstrate good conduct at all times and so their public engagement on social media falls within the scope of the Code of Conduct.

When posting to social media you should remember that:

- You are an elected representative of your Council.
- What you post can affect the reputation of your Council.
- Your Council is a corporate decision-making body – you can't, independently, make decisions for the Council on social media.
- Some issues and communications are best left to your Council's official social media channels, which are usually managed by officers.
- Having a single voice or message can be critical in some situations – for example, in the event of major flooding.

- You don't have to respond to or comment on everything on social media – and sometimes it's best not to.

Think before you press 'publish'! There is a simple test. If you would be reluctant to say something face-to-face to a group of strangers in the street, then you probably shouldn't say it on social media.

General Advice by the Local Government Association on Social Media can be found at An introduction to social media for councillors | Local Government Association

9) Printers

To support sustainability and NetZero aims, individual home printers are no longer provided. All documents are provided electronically. A PC and printer are available in the Members room and for exceptional large prints the Democratic Services team may be able to assist.

10) Use of AI Applications

Members are advised AI Chat for Chatbot functionality. includes Copilot, Bing Chat, ChatGPT, Google Bard.

This should not be used to:

- Upload, enter or provide confidential or sensitive information.
- Upload, enter or provide any data or text that is not either already in the public domain or intended to be in the public domain.
- Upload, enter or provide details of a resident or produce a letter or email on a specific matter.
- Upload, enter or provide a confidential email and ask it to suggest better wording.
- Upload or use it for anything that breaches the Councils obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Information automatically created by AI may not be correct and it is the responsibility of the user to ensure it in correct.

Information input to AI Chat functions may be reviewed by a human working for the application supplier i.e., someone outside of the Council.

Anyone using AI inappropriately or putting themselves or the Council at risk of reputational damage or legal challenge will be managed through the Council's existing Complaints about Councillors Procedures.

They can be used for:

- Drafting text.
- Generating ideas, text or artwork.
- Improving spreadsheets, charting the data and providing insights.

- Summarising large texts – provided they are in the public domain.
- Comparing two documents and indicating change or compliance – provided they are in the public domain.
- Obtaining feedback on a document – provided that document is intended to be in the public domain.
- Reviewing documents and suggesting improvements.
- Writing transcripts of audio files and suggesting summaries.
- Analysing survey results – provided that survey is intended to be published.
- Assist those with communication difficulties and reduce bias by suggesting more inclusive words in documents.

11) Breaches of Digital Information Code of Practice

Breach of email usage
▪ Raised with Chief Executive and the Leader of the Council.

Breach of mobile device usage
▪ Raised with Chief Executive and the Leader of the Council.

Breach of Internet usage
▪ Raised with Chief Executive and the Leader of the Council.

As each Councillor is the Data Controller in regard to Data Protection Regulations, they will be responsible to the Isle of Man Information Commissioner for any breaches regarding the Data Protection Act and Regulations.

12) Acknowledgement and Acceptance

I acknowledge receipt of this Councillors Digital Information Code of Practice, and I am familiar with its contents.

Signed:

Name:

Date: