Acceptable Use Policy

Sign Off

	Name, Title, Department	Signature	Date
Prepared by	Ricky Ng (DoIT, IT Division)		Sept-Oct 2024
Reviewed by	Deputy Chief Executive		Oct 2024
Approved by	Full Council		11 Dec 2024

This policy is owned by Information Technology Division, any changes and/or adjustments to this policy shall be made, reviewed, and approved by Information Technology Division.

Consumer Council Document Library Access Right

Access Party
All Users of Consumer Council

Revision History

Version Date	Version Number	Description of changes	Author
11 Dec 2024	1.0	N/A	Protiviti / ITD
30 Jun 2025	1.1	General • Change of Titles: Updated all references from “Division Head” to “Director”. • Renaming of OGCIO: Changed all references from “OGCIO” to “DPO”. • Renaming of AGDEIT: Changed all references from “AGDEIT” to “Committee on Digital Economy and Information Technology (DEIT)”. Paragraph 17.10: • Permitted the use of Council-authorised instant messaging applications for transmitting classified information, provided the requirements outlined in the Information Classification and Protection Standard are followed.	Protiviti / ITD

Table of Contents

1 Scope

This policy applies to all individuals, IT assets and services within or have access to the Consumer Council's IT network infrastructure. The individual includes all staff, contractors, third parties and any other individuals who access, handle or manage network resources.

IT assets refer to IT systems and other information/equipment including paper documents. The IT systems include all information systems managed by the Consumer Council, including servers, network devices, workstations and applications.

2 Statement of Responsibility

IT Division

2.1 IT Division is responsible to review and update this policy with the assistance of Directors.

Directors

2.2 Directors shall assist IT Division to review and update this policy based on the business needs.

Users (Staff, Contractors, Third Parties)

2.3 Users are individuals or groups who require access to the data, information, programs, and systems for their jobs, perform or receive a service.

2.4 Users must agree to comply with this policy before accessing Council's IT network infrastructure and responsible for their own actions and act responsibly and professionally.

3 Acceptable Use

3.1 Information assets and data must be used only for business needs with the purpose of executing Consumer Council related tasks.

3.2 Users must only access and use those information assets and data for which they have been authorized.

3.3 Users must only use Council's authorized IT assets to store Consumer Council information.

3.4 Users will cooperate fully with all requests from IT Division with respect to updating software on Council's IT Systems.

3.5 Users are responsible for protecting the confidentiality, integrity and availability of the information assets and data under their procession.

3.6 Users are required to report a lost or stolen IT assets and data immediately to IT helpdesk and Directors.

4 Prohibited Activities

Users are prohibited to perform the followings:

4.1 Take part in any activities to bypass IT systems security controls.

4.2 Use IT assets and data in a manner that unnecessarily takes up capacity, weakens the performance of the IT systems or poses a security threat.

4.3 Conduct personal matters on Council-owned devices at any time.

4.4 Download image, video or files which do not have a business purpose to Council-owned devices, e.g. watching movies, playing games, etc.

4.5 Install, plug in or use peripheral devices such as modems, memory cards or other devices for storing data (e.g. USB flash drives) without explicit permission by Director of IT.

4.6 Disable any standard software installed on IT systems.

4.7 Connect non-Council authorized devices to Council's IT network.

4.8 Install software or program code on IT systems without explicit and formal permission by Director of IT.

4.9 Use Council's resources for unlawful, criminal, offensive, obscene, defamatory, fraudulent, deceptive, harmful, threatening or objectionable behavior or in a manner which would violate the rights of others.

4.10 Auto-forwarding or transfer Council's e-mail/message to non-Council's e-mail accounts or non-Council authorized devices.

4.11 Use of Council's email to misrepresent personal opinions as those of Consumer Council.

4.12 Use of Council's email for performing any activities (e.g. performing membership registration) unrelated to Council's operations or business.

4.13 Use of Council's IT assets to create, transmit, forward, post or store material of

inappropriate or illegal content.

4.14 Using non-Council authorized instant messaging applications for transferring sensitive information.

4.15 Use of social media (e.g. Facebook, Twitter and LinkedIn) on Council's/Council's managed devices for non-business purpose.

5 Return of Assets Upon Termination of Contract

5.1 IT assets and data in physical and electronic form (e.g. documents, manuals, equipment, hardware and software) provided to the users by the Council remain the property of the Council and must be returned when the contract agreement ceases. Similarly, any information assets and data received from the Council's external stakeholders in connection with the users' work must be returned to the Council.

6 User Account Responsibilities

6.1 The owner of the user account is its assigned individual, who is responsible for its use, and all activities performed through the user account. Therefore, users must not directly or indirectly, allow another person to use their access rights (i.e. user account and password) and they must not use another person's user account and password.

6.2 The use of shared accounts is forbidden unless explicitly reviewed, assessed and approved in accordance with User Access Management Procedure, shared account related activities must be logged and reviewed.

7 Password Responsibilities

7.1 Users must apply good security practices when selecting and using password by following Password Policy.

7.2 Password must not be disclosed to other persons, including management and IT personnel.

7.3 Password must not be written down.

7.4 Password must not be stored for automated system login (e.g. using auto-saved passwords of web browsers).

7.5 Where passwords need to be stored on computers, they must be protected by an access control program or encrypted with a robust encryption algorithm.

7.6 Password must not be distributed through the same channel on which the user account information is disclosed, unless delivery by hand, verify the receiver identity before

providing the password.

7.7 Passwords must be changed if there are indications that the passwords or the IT systems may have been compromised, in that case an incident must be reported by following the Incident Management Standard.

8 Classified Data

8.1 Data is restricted to individuals on a need-to-know basis only and different security measures must be implemented according to the classification level, users must follow the Information Classification and Protection Standard when handling data.

8.2 Unauthorized disclosure or modification of classified data may result in serious disciplinary actions.

8.3 Data shall be stored on secured workspace on Consumer Council's authorized systems (e.g. Microsoft OneDrive, Microsoft Teams, Microsoft Outlook).

9 Information Security Awareness

9.1 Staff must attend all regular security awareness trainings and complete the corresponding security awareness tests if requested.

10 Sharing of Endpoint Devices

10.1 Endpoint devices (e.g. desktop, laptop, mobile phone) which are provided to an authorized individual user shall not be shared with other persons.

11 Copyright

11.1 Users must not share, copy or transfer licensed software to other individuals or devices.

11.2 Users must not copy software or other original materials from other sources, and are liable for all consequences that could arise under the intellectual property law.

12 Taking Assets Off-site

12.1 IT assets, regardless of its form or storage media, shall not be taken off-site without prior explicit permission by Director of IT or Directors.

12.2 With permission granted, users are responsible for controlling the IT assets they take off-site.

13 Mobile Devices

13.1 Only Consumer Council-managed mobile devices and privately-owned devices with

Mobile Application Management (MAM) solution deployed are permitted to access Consumer Council's IT systems.

13.2 Upon staff termination, contract termination, or when required by Consumer Council, the mobile device will be wiped for security purposes. (Note: All data and applications will be removed upon termination. The devices installed with MAM will only remove Consumer Council's data and applications.)

13.3 Consumer Council is not responsible for any damage to personal mobile devices.

14 Using Removable Media

14.1 Users must not insert or connect any unauthorized removable media (e.g. USB memory sticks, portable hard disk, mobile phone, CD, DVD) to Council's IT systems. The use of removable media must be approved in accordance with the Endpoint Security Standard.

14.2 Removable media shall only be used where absolutely necessary.

14.3 If removable media is used, Users must check that:

- All removable media used shall be kept secure.
- Information stored on removable media shall be deleted when it becomes redundant.

15 Clear Desk and Screen Policy

15.1 Staff must remove all classified IT assets from the desk when they are away from their desk to prevent unauthorized access.

15.2 Such IT assets must be stored in a secure manner according to the Information Classification and Protection Standard to prevent unauthorized access.

15.3 Users must lock their endpoint devices when they are away to prevent unauthorized access.

15.4 Classified IT assets must be immediately removed from meeting rooms, whiteboard, printers, fax and copy machine.

16 Use of Internet

16.1 Access to Internet through Council's network and/or using Council's Managed Devices shall be confined to business purposes.

16.2 All public Internet websites shall be presumed to be unsafe and users shall stay alert while accessing public internet website through Council's network and/or using Council's Managed Devices.

16.3 Users must consider information and data collected from the Internet as unreliable before verifying the source. Such information may be used for business purposes only after its authenticity and correctness have been verified on separate channel.

16.4 Users are responsible for all possible consequences arising from their unauthorized or inappropriate use of Internet services or content.

16.5 Direct Internet access through modems, mobile internet or other devices which circumvents Council's control is forbidden.

16.6 Access to inappropriate and insecure websites may be blocked for individual users, groups of users or all staff at the Council. If access to blocked website is required for business purpose, users shall request access by following Network Security Standard. Users must not try to bypass such restriction autonomously.

16.7 Users shall not connect Council's IT systems via public wireless hotspots (e.g. coffee shops, airports and hotel Wi-Fi). A Wi-Fi egg shall be used as an alternative for business trips.

17 E-mail and Other Message Exchange Methods

17.1 Messages and files containing Council's data must be exchanged through Council authorized methods, including Council's e-mail, Microsoft Teams, Microsoft OneDrive, designated shared drives, telephones, fax machines and Council authorized removable media.

17.2 Consumer Council's e-mail accounts are assigned on individual or group basis where the responsibility in account operation shall rest with the designated user or group. Each user (and each user within a group) is responsible for the actions performed on assigned e-mail account.

17.3 Users must only send messages containing true information and must not send spam messages. It is forbidden to send materials with disturbing, unpleasant, sexually explicit, rude, slanderous or any other unethical or illegal content.

17.4 Each e-mail message sent by the user must contain a disclaimer.

17.5 File Transfer Protocol (FTP) must not be used because it is not secure by nature.

17.6 User who received inappropriate content shall report it immediately to his/her Director,

or in case if any conflict or embarrassment may arise, report shall be lodged with a HR division representative.

17.7 Users who receive suspicious messages or attachments from Council's authorized method shall be reported to IT Division via cybersecurity_info@consumer.org.hk.

17.8 Users shall not click on links, download programs, or respond to suspicious e-mails and messages or emails and messages from unknown source.

17.9 Details of video calls and conference calls shall only be distributed to authorized persons.

17.10 Only Council's authorized instant messaging applications are allowed for transferring Council's classified information. The information must be transmitted according to the information protection requirements specified in Information Classification and Protection Standard.

17.11 Users may use instant messaging application for dissemination of Council's publicly available information, or basic and informal communications (e.g. contains no classified data or details) in response to external stakeholders' use of these messaging applications. This includes:

- Sending a copy of the Council's press release of a CHOICE article.
- A simple greeting (e.g. Have a good evening) or the Council's official seasonal greetings.
- Council's promotional or publicity messages with weblinks to Council's website or social media posts.
- Confirming a meeting time (e.g. Tuesday @3pm sounds good), or seeking confirmation on next steps (e.g. Yes/No response).

18 Use of Social Media

18.1 Authorized users are only allowed to use Council's social media accounts for business purposes, and are not permitted to use personal social media accounts for business purposes.

18.2 Authorized users are fully responsible for all posts and communications disseminated via Council's social media channels.

18.3 Authorized users shall not post or otherwise communicate any classified information.

18.4 Authorized users shall not comment on any issue relating to Council's legal matters.

18.5 Authorized users shall ensure all information posted using Council's social media accounts is accurate to the best of their knowledge and expertise. Users shall report, in writing, any known or perceived conflict of interest to his/her Director immediately.

18.6 Authorized users shall only post or otherwise communicate truthful information. When citation of quotes, statistics, standards, facts or third parties' opinions is required, only credible sources shall be relied upon.

18.7 Authorized users shall always be respectful of any personal and proprietary information, intellectual property and classified information, whether belonging to Consumer Council or otherwise, of which is acquired through employment or working with Consumer Council. Information sharing practices that govern all Consumer Council users under the Council's policies, procedures and guidelines shall also be applicable to all social media communications.

18.8 Authorized users shall ensure that all posts, information or information otherwise associated with them is presented in accordance with all legal requirements (i.e. copyright laws, fair use laws, proprietary laws, etc.).

18.9 Authorized users shall not portray Consumer Council or external stakeholders or users in a negative way.

18.10 Authorized users who use social media communication for solicitation and/or marketing purposes shall be approved by Director of Pubic Affair Division (PAD).

18.11 Any contacts from the media about Consumer Council and any of its products, users, partners, or otherwise should be referred to the Public Affairs Division.

19 Exemption

19.1 For situation arise where it is not possible to comply with the policy requirements, formal approval shall be obtained from the Director of IT or delegate(s).

19.2 All exceptions shall be protected by sufficient alternative security controls or processes to enforce the security and compliance.

20 Related Policy and Procedural Documentation

- Password Policy
- Incident Management Standard
- Information Classification and Protection Standard
- Endpoint Security Standard

21 Related Reference(s)

The policy is developed with reference to the following document(s):

- DPO S17 Baseline IT Security Policy
- DPO G3 IT Security Guidelines