# COUNCILLOR ICT ACCEPTABLE USE PROCEDURE

## 1.0 Purpose

The purpose of this procedure is to provide Councillors with clear guidance on the appropriate, safe, and legal way in which they can make use of information and Information and Communication Technology (ICT) equipment at City of Ballarat.

This procedure sets out the responsibilities and required behaviour of users of City of Ballarat's ICT services. It is essential for Councillors to understand how to use ICT services effectively and in line with print and editorial guidelines.

Councillors need to be aware of and comply with this procedure. This procedure will ensure use of computer and telecommunication equipment:

- Does not compromise the status, security or reliability of the Council computer network in any way
- Is provided within a secure environment
- Can be supported by City of Ballarat's Civic Support and ICT business units

Inappropriate use exposes City of Ballarat to risks including cyber-attacks, compromise of City of Ballarat's enterprise systems, and potential disruption to services.

## 2.0 Scope

This Councillor ICT Acceptable Use Procedure applies to the use of all City of Ballarat managed ICT equipment and software managed by City of Ballarat as well as by Councillors.

## 3.0 Procedure Statement

3.1. City of Ballarat's ICT systems and equipment must not be used for the creation, transmission, or deliberate reception of any images, data, or other material that is designed or likely to cause offence or distress, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, Councillors are expected to conduct themselves in an honest, courteous, and professional manner, and in line with the standards outlined in the City of Ballarat's Councillor Code of Conduct.

3.2. It is the responsibility of all Councillors to ensure that electronic devices, facilities, and the data which is accessed through them, are safe and secure. Electronic devices should be placed in an area where they are not likely to be damaged.

3.3. Deliberate activities with any of the following consequences (or potential consequences) are prohibited:

- Corrupting or destroying corporate data.
- Using systems in an unreasonable way that impacts service to others.
- Gaining access to systems that are unauthorised to use.

3.4. Councillors should treat unsolicited emails and the attachments and links contained within them with extreme caution, especially if the sender is unknown. Viruses and phishing attempts are often sent this way. If Councillors are not sure what an attachment or link is for,

or why someone has sent it to them, they should not open it and seek advice from the Civic Support team.

3.5. Councillors must not set up auto-forward rules to external addresses.

3.6. Any electronic device owned or provided by City of Ballarat is subject to the same conditions of use whether used at home or on Council property.

- Councillors should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations, keeping the ICT equipment locked and out of sight.

3.7. The ICT department will endeavour to provide all systems with secure access facilities.

- Where passwords or pin codes are used, Councillors will be able to set and change their own password or pin code whilst meeting the minimum complexity requirements.
- Councillors should not leave any electronic device unattended without either logging out or activating a password-protected lock screen.
- Attempting to remove or bypass any security access on any City of Ballarat electronic device is strictly forbidden.
- Passwords and PIN codes are issued for individual use only. They should not be shared or disclosed to anyone else (other than upon ceasing to hold office as per point 3.9). Councillors are required to protect their passwords and PIN codes against theft and possible misuse by others.
- Any Councillor who suspects or is made aware of a security breach must immediately alert both the Civic Support team and the ICT Service Desk, who will initiate investigation procedures in line with City of Ballarat's Security Incident Management Procedure. Depending on the breach scenario, investigations may be carried out jointly with City of Ballarat's Governance and Risk department. If warranted, the findings will be subsequently reported to City of Ballarat's Audit and Risk Committee and to any relevant Security Incident Reporting Scheme.

3.8. Access to read document archives will only be granted to City of Ballarat staff responsible for investigating system failure, system misuse, or as required or authorised by law, and information will only be accessed as necessary to repair or protect the systems or to investigate use that may be in contravention of this procedure.

- Document files, web browsing logs, email or voicemail messages may have to be accessed or disclosed as required or authorised by law, or during internal investigations if relevant to the issues being investigated.

3.9. When informed by the Chief Executive Officer that a Councillor has ceased to hold the office of a Councillor, the ICT department will deactivate the relevant account.

- Councillors who have ceased to hold the office of a Councillor must take responsibility to hand over all Council related information, either by forwarding them to Civic Support, or by copying them to a shared location.
- Councillors should ensure that any personal information stored in their OneDrive or elsewhere is deleted.
- All City of Ballarat devices need to be logged out of all personal accounts and mobile phones and iPads need to be restored back to factory settings. In the case where this isn't

done, exiting Councillors must provide Civic Support with their PIN codes and passwords so ICT can do this on their behalf.

3.10. Remote control software is used by authorised System Administrators from the ICT department to connect and take control of a computer remotely for ICT Service Desk support. ICT staff will not use this to connect to a computer without attempting to contact the user of the machine first.

- Remote access will not be used for other purposes.
- Councillors should not attempt to use any remote-control software, nor allow external users or support staff to use it without the express permission of the ICT department.

3.11. Access to the internet is primarily provided to enable Councillors to effectively perform their role. Reasonable personal use (excluding private work) is permitted, provided this does not interfere with the performance of duties or adversely affect system performance. City of Ballarat has discretion to determine what constitutes excessive use.

- The ICT department has the right to block inappropriate website access and globally ban access to any site as appropriate, without warning.
- City of Ballarat will not accept liability for personal legal action (e.g. libel) resulting from Councillor misuse of the internet.
- Access to file downloads will be restricted as necessary by the ICT department to ensure system security.
- City of Ballarat reserves the right, consistent with legislation, to monitor all internet access on any City of Ballarat device, including but not limited to email and web access. No Councillor should consider information sent/received through the internet as their private information.
- No Councillor may access, display, or download from internet sites that hold offensive material.
- Personal/staff identifiable data must not be published in any way on the internet without the express consent of each and every individual concerned.

3.12. All software for laptops must be purchased, installed, and configured by the ICT department. This includes all software packages, software upgrades, and add-ons, however minor. It also includes subscription services (free or otherwise), and any items downloaded from the internet. Under no circumstances should any software be purchased or installed without the explicit approval of the ICT department. The Civic Support team can arrange for the above approvals.

- Councillors must not violate license agreements by making illegal copies of City of Ballarat software. Doing so may be in breach of the law.
- Software not licensed to City of Ballarat must not be loaded onto City of Ballarat laptops. Software licensing will be arranged and recorded by the ICT department as part of the procurement and/or installation process.
- Councillors are not permitted to download software from the internet or install from a removable device to a laptop without authorisation from the ICT department. Any unlicensed software found on a City of Ballarat electronic device may be automatically deleted or disabled.

## 4.0 Supporting documents and references

### 4.1 Legislation

- *Privacy and Data Protection Act 2014*
- *Local Government Act 2020*
- *Gender Equality Act 2020*
- *Surveillance Devices Act 1999*

### 4.2 Definitions

| | |
|---|---|
| **Document archives** | Document archives is the storage of documents in a secure, long-term repository. This repository can be either physical or digital, and it is designed to protect the official documents from damage or destruction. |
| **Electronic devices** | Electronic devices include laptops, mobiles, tablets and any other smart devices. |

## 5.0 Administrative Updates

From time to time, circumstances may change leading to the need for minor administrative changes to this procedure. Where an update does not materially alter this procedure, such a change may be made administratively. Examples of minor administrative changes include changes to names of Council departments or positions, change to names of Federal or State Government departments or a minor amendment to legislation that does not have material impact. Where any change or update may materially change the intent of this procedure, it must be considered by Council.

## 6.0 Procedure owner

Executive Manager Information Communication and Technology.

## 7.0 Authorisation

Adopted by Ballarat City Council on 28 August 2024 (R138/24).