Working together
to create the world's most liveable community

GENERAL IT USE POLICY

Approval Level:	EMT
Policy Type:	Organisation
Approval Date:	30/11/2021
Review cycle:	Four years
Review Date:	23/11/2025
Responsible Officer:	Manager Information Technology
Owner:	Information Management
Responsible Director:	Corporate Performance
Relevant Legislation/Authority:	*Privacy and Data Protection Act 2014* *Charter of Human Rights and Responsibilities Act 2006*
DOCSETID:	1739680

1. PURPOSE

1.1 The purpose of this policy is to outline expectations for the use of City Applications to perform City Functions at the City of Greater Bendigo including but not limited to:

- General use
- Email and messaging use
- Internet use

2. SCOPE

This policy applies to all Authorised Users.

3. DEFINITIONS

In this policy:

Authorised Users means employees, volunteers, students and contractors who use City Applications to perform City Functions.

City means The City of Greater Bendigo.

City Applications means the software systems used to perform City Functions.

City Functions means the activities undertaken by an Authorised User to meet organisational objectives.

Email means electronic mail which is the transmission of messages over communication networks.

Encryption means the process of converting data to an unrecognisable or "encrypted" form. It is commonly used to protect sensitive information so that only authorised parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the internet.

Messages/ing means a type of online chat which offers real-time text transmission.

Network means a digital telecommunications medium which allows the sharing of resources.

Pooled Device means a single device that is used by multiple Authorised Users sharing a common account.

4. POLICY

4.1 General Expectations of Authorised Users

(a) In addition to the expectations described in this policy, the general use of information technology, email and messaging and internet at the City must be in line with and/or adhere to:

- the City’s Employee Code of Conduct and;
- all other relevant City policies and procedures

(b) Maintain a professional standard when using and recording information in City Applications. Anything created or stored using City Applications may, and likely will, be reviewed by others including access by the public.

(c) Manage use of resources within the constraints built into the systems including disk space.

(d) Limited use of City Applications for incidental personal purposes is permitted.

(e) All software licence obligations are complied with and no unlicensed software is used.

(f) Only City Applications are authorised for installation on City supplied Windows based devices and must only be installed by Information Management.

(g) Anti virus software is installed on City supplied Windows based devices and is not to be disabled or circumvented.

(h) Access to City Applications is controlled through individual accounts and passwords. It is the responsibility of the Authorised User to protect the confidentiality of their account and password information. With the exception of approved Authorised Users of Pooled Devices, passwords should not be shared. Authorised Users will be held personally responsible for all activities conducted using their account.

(i) The establishment of a Pooled Device requires authorisation from the Unit Manager and the Manager of Information Technology. An individual will be nominated to be responsible for the maintenance, care and security of the Pooled Device.

(j) City Application access may be granted to third party non-employees on a case-by-case basis.

(k) Access to City Applications will be deactivated when an Authorised User's association with the City ceases. Furthermore, the City is under no obligation to store or forward the contents of an Authorised User's mailbox after the relationship with the City has ceased.

(l) Password changes will be enforced on a regular basis and may be initiated at any time at the discretion of Information Management.

4.2 Email and Messaging Use

(a) Authorised Users are responsible for mailbox management, including organisation and cleaning and operating with the allocated mailbox size limits implemented in the system.

(b) Normal standards of professional and personal courtesy and conduct are expected when representing the City via email and Messaging.

(c) Emails and Messages are corporate records and must be entered into City Applications where appropriate.

(d) An email signature in approved City format is to be included when sending external emails.

(e) Where an Authorised User has provided delegated access for the management of their email account to a third party, the Authorised User retains responsibility for all activities undertaken on behalf of their email account.

4.3 Internet Use

The use of City provided internet for streaming radio or video is to be used to perform City Functions only.

4.4 Monitoring, Review and Reporting

(a) The City implements relevant tools to manage and monitor a broad range of activities related to information technology, email and messaging and internet use.

(b) The City Applications used for Email and Messaging are logged, monitored and may be subject to review. This review may include, but is not limited to, reading by Information Management during the normal course of managing City Applications, review by the legal team, responding to Freedom of Information requests and access and/or investigations authorised by People and Culture.

(c) All inbound and outbound email is permanently archived. In addition, backup copies of Email and Messages exist. Deletion by Authorised Users does not delete Emails and Messages.

(d) All internet usage undertaken through the City's Network is logged. Unit Managers and Directors are provided with a monthly summary of each Authorised User's internet usage.

(e) Archival and backup copies of systems and information may exist, despite Authorised Account deletion.

5. ROLES AND RESPONSIBILITIES

5.1 Authorised Users

All Authorised Users are responsible for:

(a) Maintaining a secure and complex password, pin code, facial recognition or fingerprint to prevent unauthorised access and;

(b) Complying with the City's Employee Code of Conduct and all other relevant City policies and procedures

5.2 Information Management

Information Management is responsible for:

(a) Authorisation of the allocation and use of pooled devices;

(b) Distribution of usage reports to the appropriate Unit Manager/Director and;

(c) Invoicing to Authorised Users the costs associated to private use at the discretion of the appropriate Unit Manager/Director

5.3 Unit Managers / Directors

Unit Managers (or Directors as appropriate) are responsible for:

(a) Assessment and authorisation of the requirement for a Pooled Device

(b) Reviewing usage reports as provided by Information Management

6. RELATED DOCUMENTS

Employees are encouraged to access the related internal documents which are available on the intranet and/or external resources which are available as per the below.

These include:

- Appropriate Workplace Behaviour Policy (DOCSETID 1822685)
- City of Greater Bendigo Code of Conduct (DOCSETID 3603208)
- Customer Service Charter (DOCSETID ID 4051596)
- Flexibility at Work Policy (DOCSETID 4416636)
- Employee Mobile Device Policy (DOCSETID 3482760)
- Managing Misconduct Procedure (DOCSETID 2172947)
- Prevention of Sexual Harassment in the Workplace Policy (DOCSETID 4579152)
- Social Media Policy (DOCSETID 1863281)
- Privacy Policy (DOCSETID 4322695)

Further information or advice on this policy should be directed to Information Management.

7. HUMAN RIGHTS COMPATIBILITY

The implications of this policy have been assessed in accordance with the requirements of the Victorian Charter of Human Rights and Responsibilities.

8. ADMINISTRATIVE UPDATES

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this, such a change may be made administratively. Examples include a change to the name of a Business Unit, a change to the name of a Federal or State Government department, and a minor update to legislation which does not have a material impact. However, any change or update which materially alters this document must be made through consultation with the staff Consultative Committee and with the approval of EMT or where required, resolution of Council.

9. DOCUMENT HISTORY

Date Approved	Responsible Officer	Unit	Change Type	Version	Next Review Date
November, 2021	*DS*	*Information Management*	*Reviewing General IT use Policy and incorporating Email and Instant Messaging acceptable use policy and Internet policies.*	*3*	*November, 2025*