WHITEHORSE
CITY COUNCIL

IT ACCEPTABLE USE POLICY

Reviewed 2021

1. PURPOSE

The Information Technology Acceptable Use Policy is to provide guidance for all Councillors, council employees and users of the council's information technology resources. The purpose of this policy is to ensure:

- The acceptable and appropriate use of Council's Email and Internet systems;
- The acceptable and appropriate use of Council's Collaboration systems (including MS Teams and Zoom);
- Adherence to procedures for core IT processes;
- The provision of reliable and uninterrupted Information Technology services;
- The integrity and validity of data;
- The protection of all Council's information technology assets including data, software and hardware.

2. SCOPE

The Internet is recognised by government and business organisations as a commonly used and valuable information resource. It provides information on a wide variety of subjects that may be useful to Council officers.

This document describes the access methods, services available, and the user and management responsibilities when using the Internet, Electronic Mail (email) and Collaboration facilities within Council. Employees who have access to the Internet have an obligation to use their access in a responsible and informed way. Managers and supervisors have a responsibility to ensure the Internet is used appropriately within their department.

All Council policies, procedures and requirements with regard to ethical and appropriate behaviour, fraud, risk management and records management apply to the use of the Internet, Electronic Mail and Collaboration systems. The provisions of the Local Government Act regarding the use and confidentiality of Council information, apply to all employees and all other system users.

This policy applies to all users of Councils information systems including Councillors, employees, contractors, casual employees and work experience students.

3. POLICY

3.1. Electronic Mail (Email) and Collaboration Systems

Corresponding via email and collaboration systems is common across the organisation. It is important to remember that the use of email and collaboration systems should, wherever possible, be restricted to business use (like Council's telephone system). Offensive material should not be instigated by Council users and if received, should be deleted immediately. Further, such material should not be forwarded to any internal or external correspondents.

3.1.1. Ownership & Storage

Authorised users are responsible for information or information systems accessed via their username or login and therefore it is important to maintain security of your login password. Passwords should never be shared. It should be noted that all electronic files, emails, data, and accounts on Whitehorse IT systems should be presumed to be the property of Council.

All incoming and outgoing email messages and chat sessions can be monitored by the IT department and information (including content and contact details) may be kept on file.

Messages that concern matters of policy and official communication between Council, individuals and other organisations should be placed on the appropriate electronic file within Content Manager - Council's electronic document management system.

Electronic mail and chat sessions may be subject to Freedom of Information and Privacy rules and therefore, individual employees are responsible for anything they write. Email has the same legal status as traditional written correspondence, so employees must apply the same business rules and protocols for email correspondence.

The email system is not designed to and should not be used as a file management system and as such, Whitehorse Information Technology, in conjunction with the IT Steering Committee, reserves the right to impose mailbox size quotas as and when and at what limits it deems necessary.

3.1.2. Acceptable Use and Etiquette

Employees should remember that body language, facial expressions and vocal inflections DO NOT travel with electronic mail or chat messages and be aware in composing messages, that their contents have the potential to be misconstrued by the recipient. The following directions and guidelines in email etiquette are provided for using Council's email and chat services:

3.1.3. When Sending email or chats

- Regardless of the recipient, act in a professional and courteous manner. Be discreet in what you send. Avoid gossip and personal comments. Avoid sarcasm or irony.
- Once an email or chat has been sent, the sender loses control of what happens to that email or chat, for example whether it is on-sent or who will have future access to view it. Employees must therefore assume that emails or chats sent are not private and may be freely available in the public domain.
- Where possible, use the 'To' field to indicate 'for action' and 'Cc' to indicate 'for information'.
- Use mixed case in email messages. DO NOT use uppercase only.
- Always proof read and spell check messages before sending them.
- Keep your email and chat messages brief and to the point. DO NOT clutter other people's email and chat accounts with unnecessary messages.
- Never forward offensive material to others within or external to the organisation, this includes jokes and video clips. If you receive offensive material, delete it immediately and reply to the sender asking to refrain from sending inappropriate material – see attached addendum for an example of reply content.
- Avoid using coloured or graphical backgrounds, large graphics or illegible fonts.
- Use shortcuts, hyperlinks or Content Manager references to large documents rather than attaching them as files. This will reduce duplication on the email server.
- Where possible, consider using expiry dates for messages sent to multiple users.
- Immediacy of transmission does not always translate into immediacy of receipt. Where a response is required immediately or the matter is urgent, it might be advisable to consider using other means of communication.

3.1.4. Workplace Representatives

Employees who are nominated by a Union to be employee delegates will be afforded reasonable time to attend to employee representation duties. Employee representatives may access Council's email system to communicate with other employees with the prior approval of the Manager Organisational Development and in accordance with this Policy.

3.1.5. Good Housekeeping Practices

- Check email daily. Respond to messages promptly. Give a brief acknowledgment if a full response cannot be provided initially.

- Delete unwanted messages immediately and regularly empty the Deleted Items folder.
- Keep messages remaining in electronic mailboxes to a minimum.
- If messages are Council related, catalogue them into Content Manager and then delete them.
- If you detach an attachment to the network or Content Manager, delete the email or at least clear the attachment from it.
- Employees should not use alternative systems to store or manage their business documents containing personal information eg. Email folders, shared (network) drives, portable storage devices, local drives because they lack the required records management function.

3.1.6. Web Based Email Access

Access to selected web-based email services is permitted for reasonable and necessary personal use. Whitehorse City Council related business communications, transactions, files, data and proprietary information are not to be sent, stored or transacted via these services.

Permitted web-based email services include Microsoft Hotmail/Outlook365, Gmail, Yahoo, Bigpond and Optusnet services.

3.1.7. Distribution Lists

The use of council-wide distribution lists (i.e. Everyone Whitehorse, Civic Centre) are only for use by nominated staff when the email is Council related and relevant to the majority of the group. Distribution lists are not to be used for soliciting, campaigning or engaging in fund-raising for any organisation, person, charity or other body without the prior permission of your Director. There are facilities available through the Council Intranet for listing items that are for sale.

Note that there are alternative ways to communicate various messages:

Message	**Method or channel**
Site specific messaging	Email user group for that worksite
Staff leave, higher duties, backfill positions	Auto reply, Out of Office on Outlook, update status in Interaction Desktop
Staff departure, acknowledging their service; or introducing new people	The Loop, CEO update or local email group and intranet
Shout outs for great performance or internal promotion of campaigns or events	The Loop, CEO update or local email group and intranet
Babies, weddings, pets, significant achievements outside work	Local email group or The Loop
Social events, coffee vans, footy tipping, social club	The Loop, intranet or local email group

Please remember, and remind your staff, that there are alternative ways to communicate various messages:

Message	Method or channel
Site specific messaging	Email user group for that worksite
Staff leave, higher duties, backfill positions	Auto reply/Out of Office on Outlook, update status in Interaction app
Staff departure, acknowledging their service; or introducing new people	The Loop, CEO update (email smc@whitehorse...) or local email group and intranet. Send content to smc@whitehorse.... And we will share it.
Shout outs for great performance or internal promotion of campaigns or events	The Loop, intranet or CEO update. Send to smc@whitehorse...
Babies, weddings, pets, significant achievements outside work	Local email group or The Loop
Social events, coffee vans, footy tipping, social club	The Loop, intranet or local email group

3.1.8. Unacceptable Practices

The practices as listed in Appendix 1 are considered to be unacceptable.

3.1.9. Email Protocol

Established procedures regarding the signing of official correspondence also apply to email. Employees should NOT forward any official correspondence via electronic mail unless delegated to do so as stated in the Council delegation manual.

All care should be taken to ensure that external email messages are addressed correctly. Messages should also identify where they contain personal opinions. Employees should refer to Council's Correspondence policy for guidelines for how to prepare an official email message.

Employees should not knowingly delete any correspondence that could, at some time in the future, be used as evidence in any potential legal proceedings.

It should be noted that the email system is a communication tool provided by Council to carry out Council business (not personal business). Professional ethics and the Employee Conduct & Contract of Employment Policies require that personal messages be kept to a minimum.

Council permits occasional, reasonable personal use, but this shall not be excessive and all communications shall comply fully with this policy.

3.1.10. Virtual Meeting Etiquette

When participating in virtual meetings please be mindful of whether video is appropriate and necessary. When video is used please consider presentation, lighting, the background and background noise. As a general rule, please behave as you would in a face-to-face meeting. Sound muting should be carefully managed to ensure the best meeting experience. When representing Whitehorse at external meetings, please ensure the corporate virtual background is used.

3.1.11. Large File Attachments

The transfer of very large files via email can affect the performance of the Council computer network with larger files consuming more bandwidth and taking longer to transmit across the network. This can have a major effect on other systems running on the network.

A degree of caution should also be exercised when sending files within email messages, to ensure that confidential or unrelated files are not inadvertently sent. It is recommended to use the Council's approved secure file transfer methods for transmitting large files. The IT Service Desk can provide further information on software and methods available.

3.1.12. Generic Email Addresses

Council's corporate email address is customer.service@whitehorse.vic.gov.au; emails to this address will be received by the Corporate Information department who will distribute the email to the appropriate officer.

Other mailboxes have been set up for specific purposes and the departments controlling these are responsible for the monitoring and processing of any email received as well as maintaining them in line with good housekeeping practices outlined in 3.1.5 above.

3.1.13. Email Signatures, Disclaimers and Informational Banners

Email signatures will be generated automatically based on data held in council's systems. These will be appended to all outgoing mail messages along with any disclaimers and marketing or informational banners as deemed appropriate by council's Corporate Services Division.

3.1.14. Policy Breaches

Any breach of this policy will be deemed to be serious and may result in disciplinary actions as set out in the relevant Human Resources Employment policies.

3.2. Internet Browsing

Internet browsing is an ideal method to access a broad range of information quickly. For all users, Internet browsing is to be used primarily for business purposes.

3.2.1. Authorised Access

All employees that have signed and returned this policy and the IT Security Policy acknowledgement form will get "Trusted" browsing access.

3.2.2. Unethical or Unacceptable Actions

Any activity that is unethical and unacceptable will be subject to disciplinary action in accordance with Council's Performance Management Policy. This may include losing access rights to the Council information systems or formal disciplinary measures in accordance with Council's Discipline policy

Unacceptable action may include but is not limited to that listed in Appendix 1.

3.2.3. Misuse

It is the responsibility of Managers and Supervisors to ensure that employees under their control are aware of how to use the Internet correctly. It is also the responsibility of each individual user to ensure that they have control over the use of their Internet access and keep their login password secure. Passwords should never be shared. Misuse of Council's internet services will be subject to disciplinary action in accordance with Council's Performance Management Policy.

Standards of behaviours outlined in the Employee Conduct Policy apply to all email, internet and collaboration usage.

Officers must ensure that any information or opinions obtained via the Internet be independently validated, as they are generally provided with no responsibility held by the originator and / or provider.

3.2.4. Use of Credit Cards

Business credit card transactions conducted through the Internet are to be made in accordance to Councils purchasing guidelines.

3.2.5. Subscriptions to Web Sites

Some Web Sites offer information and services to visitors in the form of subscriptions. Most often, subscriptions are free, but visitors are required to provide identification details to access these areas (usually name, company, position and email address).

Council officers may only subscribe to web sites that are related to their work. They must not subscribe to web sites for personal reasons. Employees wishing to use sites that require subscription / password access are to adhere to the following process:

- A record of the subscription is to be held by the department,
- Should the officer leave the organisation, the subscription should be transferred to another officer if required by the department otherwise the subscription must be cancelled. The officers' supervisor must action these tasks where applicable

3.2.6. Downloading Files

The following rules apply to the downloading of files from external sources, including electronic mail and the Internet.

- No games, movies or TV shows will be downloaded onto, or accessed from the Internet from any Council device and must not be saved on Council's file servers
- Pornographic or other material of an offensive nature is NOT to be searched for, downloaded or uploaded. This restriction includes but is not limited to such material in text, graphic, audio or video format. **Users are advised that the downloading of pornographic material from the Internet and / or distribution via electronic means may be a criminal offence and is prohibited by Council's Employee Conduct and Equal Opportunity and Human Rights Policies.**
- In some instances, offensive or inappropriate material may be inadvertently displayed when searching the Internet via advertising "pop-up" windows etc. Should any such "unsolicited" material be encountered, employees are advised to log out of the sites immediately and warn any other employees who may be affected.
- Employees are advised that content checking software may quarantine such material and bring it to the attention of the Information Technology department.
- Employees are reminded of international copyright and piracy laws and are strictly forbidden to copy any material onto Council systems that may breach these laws.
- No computer programs or executable (.exe) files are to be downloaded onto, or installed on any Council computer without the written permission of the Information Technology department.

3.3. Email and Internet Security

3.3.1. Scanning, Filtering and Blocking

Internet browsing, emails, chat sessions and downloads are subject to scanning, filtering and blocking processes conducted by automatic content filtering software. These processes aim to conserve Council resources, protect the network from cyber crime activities and prevent obscene, illegal or inappropriate activity.

This software is used to scan and detect viruses and prohibit inappropriate information from being exported or imported via email or the Internet. Such items, when detected, are automatically quarantined from the Council network and the Information Technology Service Desk is notified.

Council's filtering processes may automatically block websites that present a risk to council and/or are in breach of council policy. IT can also manually block problematic sites.

3.3.2. Quarantined Messages

Employees will be notified of any quarantined Email messages or Internet activity. Access to quarantined messages can be obtained by contacting the Information Technology department who may release them if deemed safe and appropriate to do so.

3.3.3. Monitoring, Auditing and Disclosure

The Information Technology department is authorised to and will monitor the use of communication and information devices to identify any breaches of policy or law. Records will be maintained to respond to valid requests for information pursuant to any legislation or audit. The records retained will include audit trails on Internet and email use.

In the event that an employee is suspected of breaching this policy their emails and Internet usage may be examined by the Information Technology department and action taken in line with Council's Performance Management Policy. All requests to obtain employee internet browsing history or access an employee's email must be approved by Information Technology through a People and Culture representative.

3.3.4. Viruses, Scams and Phishing

Email messages from unknown senders arrive from time to time – sometimes with file attachments and links. Exercise caution before opening attachments or clicking on links. If in any doubt, check with IT or just delete the item. Be aware too of 'Phishing' scams that purport in many cases to be from banks or utility companies may seek usernames, passwords and other personally identifiable information. Regardless of council's virus protection measures, it is always possible that newer virus strains may be able to penetrate virus scanning at the gateway or desktop.

3.3.5. Cyber Security Awareness

Regular Cyber Security Awareness Training will be conducted to enhance the security posture of the Council.

4. RESPONSIBILITIES

All managers are responsible for ensuring their employees are aware of, and comply with this policy.

It is the responsibility of the Information Technology department to ensure that any breaches of this policy are reported to relevant managers.

5. RELATED POLICIES & LEGISLATION

The following legislation relates to this policy:

- Spam Act 2003
- Equal Opportunity Act 2010
- Information Privacy Act 2000
- Privacy and Data Protection Act 2014
- Local Government (Democratic Reform) Act 2003
- Copyright Act 1968
- Electronic Transaction Act 2001

This Policy is implemented in conjunction with the following Council documents:

- Information Management Policy
- Information Security Policy
- Mobile Device Policy
- Employee Conduct Policy
- Performance Management Policy
- Equal Opportunity and Human Rights Policy
- Corporate Policy Manual
- Purchasing Policy
- Councillor and Employee Conduct Policy
- Privacy Policy
- Dispute Resolution Policy

INTERNAL USE ONLY

6. REVIEW

Responsible Manager: Director Corporate Services, Manager Information Technology
Date Adopted: July 2019 (Reviewed May 2021)

This policy has been reviewed for Human Rights Charter compliance.

7. APPENDICES

Appendix 1 – Inappropriate Activity

APPENDIX 1

INAPPROPRIATE ACTIVITY

"Inappropriate activity" includes, but is not limited to, any activity which:

- Interferes with the intended use of Internet resources. Such activities may include downloading large amounts of data for personal use affecting the performance of the Internet connection for all other users;
- Seeks to gain or gains unauthorised access to Internet resources;
- Uses or knowingly allows another to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises or representations;
- Without authorisation destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources;
- Without authorisation invades the privacy of individuals or entities that are creators, authors, users or subjects of the information resources;
- Transmits or causes to be transmitted communication that may be construed as harassment or disparagement of others based on the criteria of the anti-discrimination legislation and departmental policy;
- Violates any laws pertaining to the unauthorised use of computing resources or networks such as the Cybercrime Act (Federal) or the Crimes Act (Vic) or any other State, Commonwealth or International laws;
- Conducts a business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group or list members to use goods or services;
- Publishes on or over the network any information which violates or infringes upon the rights of any other person or group, including material of an abusive nature;
- Accesses or publishes on or over the network any information of an obscene or profane nature, or material likely to be sexually offensive to an average person or contrary to the generally accepted social standards for the use of a government facility;
- Involves participation in or facilitation of the services offered by commercial and/or online gambling and/or gaming sites or the equivalent mobile applications commonly referred to as 'apps'.
- Conducts political campaigning without prior approval of the Chief Executive;
- Harasses or bullies another person;
- Seeks or gains unauthorised access to any resource or entity;
- Vandalises the data of another user;
- Posts to a discussion group or other public forum personal communications without the author's consent;
- Has the potential to disrupt, interfere, or otherwise obstruct the work of other people by consuming large amounts of system resources including disk space, processor time and network bandwidth. Examples of activities likely to cause congestion include the emailing of chain letters or the broadcast of messages to lists or individuals, using tools which consume unnecessary network bandwidth.
- Severely degrades or disrupts equipment or system performance;
- Misrepresents him/herself or the Whitehorse City Council; or
- Attempts to read another person's protected files.