



POLICY – HR 31

USE OF TECHNOLOGY

APPROVAL DATE:	2013-05-15	CROSS-REFERENCE:	
RESPONSIBILITY:	Administration		
APPROVER:	Council	APPENDICES:	
REVISION DATE (s):	2018-08-13; 2021-12-13	REVIEW DATE:	2025

POLICY STATEMENT

To establish the rules governing the use of the Village of Marwayne's information technology resources.

BACKGROUND

The purpose of this policy is to govern the use of internet, email, computers, applications and mobile devices owned by the Village of Marwayne.

OBJECTIVE

To ensure that information technology resources are being used in a manner that is appropriate and protects the privacy and best interests of the Village of Marwayne.



DEFINITIONS

CAO is the Chief Administrative Officer for the Village of Marwayne in the Province of Alberta.

Employee is a full-time permanent Employee, Councillor, Volunteer or Contractor of the Village of Marwayne in the Province of Alberta.

Employer is the Village of Marwayne in the Province of Alberta.

FOIP is the Freedom of Information and Protection of Privacy Act, as amended from time to time.

Information Technology (IT) Resources is all hardware, software, documentation, programs, information, data, and devices that are owned or provided by the Village of Marwayne.

Village is the Village of Marwayne in the Province of Alberta.

GUIDING PRINCIPLES

This policy applies to all Village of Marwayne Employees, whether at the office or offsite, and is subject to the terms set forth below:

- The Village is the exclusive owner and has complete control over all email messages sent, received, forwarded, deleted, or in draft format, from a Village of Marwayne email account.
- The use and disclosure of email messages is covered under the provisions of FOIP.
- The use of IT Resources is restricted to Village business only. Limited, occasional and/or incidental use of IT Resources is acceptable provided that the privilege is not used excessively or abused.
- Personal and/or confidential information is not guaranteed to remain private or confidential if shared using the Village's IT Resources.
- Information that is sensitive or confidential in nature should only be shared using the Village's IT Resources if such information has been encrypted or password protected.
- Employees are responsible for all actions associated with their use of Village IT Resources. This includes any actions that are carried out under their username and/or login credentials.



- Employees should ensure their passwords are updated regularly to prevent any misuse of Village IT Resources.
- Inappropriate use of email includes but is not limited to:
 - Messages that contain information which is, or may be, offensive;
 - Messages that contain information which is, or may be, derogatory, defamatory, or threatening in nature;
 - Messages that contain information which is, or may be, illegal, or for a purpose that contravenes any of the Village's bylaws, policies or laws in the Province of Alberta;
 - Messages that reflect personal opinions or bias of individuals, employees, groups or Village practices, policies, bylaws, etc.;
 - Messages related to the operation of an Employee's personal business; and
 - Chain, spam, marketing, etc. messages.
- The Village requires that Employees conduct themselves professionally, honestly and appropriately when utilizing IT Resources and respect all copyrights, software licensing rules, intellectual property rights, and privacy laws.
- The Village reserves the right to blacklist or block, as the case may be, any internet site or program that it deems to be inappropriate or affecting the Village's network performance.
- All IT Resources that are not owned by the Village must connect only to wireless networks designated for public use.
- In the event Village IT Resources are lost or stolen, the CAO must be notified immediately. The CAO will then inform the Village's IT Resource contractor to disable the associated device(s).
- Where practical, files that contain information considered private or confidential under FOIP must not be stored on mobile devices such as notebook computers, tablets, phones and USB keys or on third-party off-site servers. When private or confidential information must be stored on these devices, the device must be protected by a password or encryption.
- Information considered as private or confidential by FOIP must not be posted to the Village's website or any other publicly accessible service or platform, unless prior approval has been received or granted by the CAO.
- The master copy of all corporate records and files must be located on Village IT Resources, not on third party off site servers.



- The following activities are prohibited at any time using the Village's IT Resources:
 - Intentionally sending files or messages containing programs designed to disrupt other systems (commonly known as viruses);
 - Accessing another computer system without authorization inside or outside of the Village's network (commonly known as hacking);
 - Intentionally possessing, using, or transmitting unauthorized material, in violation of copyright restrictions;
 - Installation of software in violation of software licensing and piracy restrictions;
 - Creating, viewing, storing, printing or re-distributing unlawful or potentially offensive material or information, on any computer system accessed through the Village's network (this includes sexually explicit, obscene, or other potentially offensive material); and
 - Disclosing personal or confidential information outside of the organization.
- Any personal expenses incurred on Village IT Resources must be reimbursed to the Village by the user. This includes applications purchased or expenses incurred on all IT Resources, including mobile and/or handheld devices.
- Some employees may need to use personally-owned cell phones to conduct Village of Marwayne business. In such cases, the Village will reimburse the Employee whom is required to use their personal cell phone for work purposes, subject to the following conditions:
 - The CAO must first authorize the Employee to use their personal cell phone for conducting Village business; and
 - The Employee is responsible for submitting the invoice page of their cell phone bill for reimbursement.
- Authorized IT Resource users are responsible for reimbursing the Village for the full costs of damaged, lost, or stolen cell phones and related accessories if they were damaged, lost, or stolen due to user negligence or neglect.



- **Consequences of Non-Compliance**

- All employees and elected officials should be aware that the Village's computer system creates records of every Internet site visited and every e-mail message sent, received, forwarded, etc. If abuse of the Village's IT Resources is suspected, the CAO may request an audit of the suspected employee's usage of the system. The CAO must approve this request in writing before IT contractors perform an investigation under the direction of the CAO.
- Details of the investigation, including any evidence, will be held in strict confidence and will only be shared on a limited need-to-know basis. If the investigation reveals that a compromise or breach of policy or legislation has occurred, it is the responsibility of the CAO to determine if disciplinary action is required.
- Failure to comply with this policy may result in disciplinary action, up to and including, termination of employment or contract.

ROLES & RESPONSIBILITIES

ROLE/TASK	TITLE (s) OF PERSON RESPONSIBLE
HANDLING INQUIRIES & COMMUNICATING POLICY	Chief Administrative Officer
MONITORING REVIEWS AND REVISIONS	Administrative Assistant