Wheatland County

INFORMATION, SECURITY, AND TECHNOLOGY POLICY SECTION

TABLE OF CONTENTS

SECTION 4.1 – OVERVIEW AND COMMITMENT **PAGE**

SECTION 4.2 – ACCEPTABLE USE AND INDIVIDUAL RESPONSIBILITIES

Policy Name:	Policy Overview
Policy Number:	4.1.1
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	November 16, 2021
Date Last Reviewed:	November 16, 2021

PURPOSE

The purpose of the policy is to outline the Information, Security, and Technology Policies for Wheatland County. These policies will act to consolidate related Information Technology policies into categories for ease of use by employees and approved third parties.

The policy categories are:

- 4.1 – Overview and Commitment
- 4.2 – Acceptable Use and Individual Responsibility
- 4.3 – Asset Management Policy

The policy will:

- Provide guidelines and use requirements to all users with access to Information Services.
- Increase user understanding and adherence to policies to help protect both the employees and the organization from potential harm that may arise from misuse of information, documents, and data/technology.
- Outline the expectations set by the organization for all employees who access information, documents, or data, or those who are requesting assistance or using Information Technology assets.
- Adhere to all laws and regulations (Federal and Provincial).
- Ensure the integrity and the quality of information, documents, data, and technology infrastructure.

DEFINITIONS

“Employee/s” unless otherwise stated, includes full-time, part-time, seasonal employee/s, elected officials, contractors, approved third party vendors, and service providers.

“Information Services” encompasses the support, delivery and sustainment of technology, software, information, and human skills, that directly or indirectly produces, manipulates, supports or stores information in digital or physical mediums. This information is utilized by the organization to assist in its decisions, records and organizational efficiency.

Policy Name:	Organizational Commitment
Policy Number:	4.1.2
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

ORGANIZATIONAL COMMITMENT

Information Technology (IT) Services commits to providing effective Information Technology software, hardware and support. Additionally, it commits to provide the means of robust information management in the form of digital and physical media such as databases, information management tools, files and records, as required by Wheatland County employees.

Information governance is the partnership in which IT Services and Enterprise Content Management collaborates to ensure a cohesive set of procedures, policies and tools can be used to better the flow of information. This partnership commits to working towards transparency, security, and business automation ultimately resulting in available, user-friendly services for residents and employees of Wheatland County.

IT Services policies, through Enterprise Content Management, will protect information, documents, and data throughout its lifecycle. This includes, but is not limited to, official business information, retention schedule, naming conventions, and conversion and transition from physical to digital information.

This policy will act to provide a foundation for the automation of business workflows while ensuring the availability of technology that is mobile. These functions will allow Wheatland County employees to effectively work on-site or remotely.

The availability and protection of information, documents, and data is a partnership between IT Services and the employees of Wheatland County. This policy provides guidance on how to access and use technology and information, documents, and data necessary to their functional responsibility as well as how to secure information, documents, and data against internal or external threats.

MANAGEMENT COMMITMENT

Management encourages the on-going improvement of technology and business automation that supports employees in fulfilling their obligations for the betterment of service to Wheatland County residents. Moreover, the continuous improvement of Information Services is paramount in maintaining efficient and effective communication between Wheatland County, its employees, and residents.

IT Services' will promote, support, and ensure compliance of policies outlining the implementation of procedures that work towards the security of digital information, documents, and data. Additionally, IT Services will advance technology and improve service levels to reduce risk and liability of data breaches or loss of information, documents, or data. Finally, IT Services will assist employees in the identification of data sets, ensuring they have a single point of access for information which allows them to make decisions based on complete and accurate business information.

DEFINITIONS

"Enterprise Content Management" is a discipline; a set of defined processes, strategies and tools that enables a business to effectively obtain, organize, store and deliver critical information to its employees, business stakeholders and customers.

REFERENCES

- ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO 15489-1:2016 Information and Document – Records Management Part I: Concepts and Principles
- CAN/CGSB 72-34:2017 Electronic Records as Documentary Evidence

Policy Name:	Overview
Policy Number:	4.2.1
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

This policy exists to provide an overarching user guideline to employees with access to Wheatland County's Information Technology. Guidelines surrounding acceptable use and individual responsibility will protect the organization and its employees from potential harm from misuse of the County's Information Technology systems and/or information, documents, or data.

This policy will:

- Protect employees and residents of Wheatland County.
- Clearly outline expectations of employees when using information, documents, or data and technology assets.
- Adhere to laws and regulations (Federal and Provincial).
- Maintain the integrity and quality of the Information Technology infrastructure.

POLICY

When accessing the information, documents, or data and technology infrastructure, employees must adhere to this policy. This policy applies to both in-house and remote access of the technology infrastructure.

On an annual basis, employees are required to read the Information, Security and Technology Policy Section 4.2 and all its policies and sign the "ACCEPTABLE USE AND INDIVIDUAL RESPONSIBILITY POLCY AGREEMENT FORM."

Information Services covered by this policy include, but are not limited to:

- Data network,

- Desks and desktop computers,
- Remote access,
- Removable storage,
- Mobile devices (e.g. cellphones, tablets, etc.),
- E-mail,
- Instant messaging,
- Information security,
- Application and software installations, and
- Internet.

Unacceptable use includes, but is not limited to:

- Emailing, texting, or messaging inappropriate messages about another employee or resident of the County or the County itself,
- Intentionally downloading, receiving, archiving or distributing materials that are offensive, pornographic, sexually explicit, etc.,
- Downloading pirated software or data (e.g., movies or books) or streaming from pirated sites,
- Using Tor, the dark web, downloading torrents, or using any non-sanctioned VPN or proxy services,
- Knowingly disabling or overloading the technology infrastructure,
- Overusing internet bandwidth for personal use by uploading or downloading multiple, simultaneous large files,
- Downloading or uploading files that may contain viruses, malware, ransomware, etc.,
- Circumventing technology infrastructure security, and
- Adding personal / non-authorized networking equipment, storage devices, computers, or mobile devices to the private or internal networks of the County.

This policy applies to all County employees, council, contractors, and approved third parties.

In the event that an approved third party or a contractor is permitted to access Wheatland County's Information Services they will be provided with a copy of this policy and the accompanying ""ACCEPTABLE USE AND INDIVIDUAL RESPONSIBILITY POLICY AGREEMENT FORM." Any third party or contractor found violating this policy will be investigated and may be found in breach of their contract.

All employees will be required to read and sign the “Information Technology Policy Form” to be provided with access to the technology infrastructure, information, documents, and data.

New and returning employees will read the policy and sign the “Information Technology Policy Form” to be provided with access to the technology infrastructure, information, documents, and data.

A synopsis of each Acceptable Use and Individual Responsibility item is listed below:

- The **“Clean Desk and Clear Screen”** policy outlines the responsibility of employees working on County property to keep their desk clear, ensure the lock up of hardcopy information, documents, or data and the locking of computer screens when exiting offices or workspaces.
- The **“Email”** policy outlines how corporate email accounts are to be used. This policy also includes a list of activities employees cannot use email for.
- The **“Internet usage”** policy outlines acceptable use of the internet by employees or approved third parties. The primary purpose of the internet is to assist in locating information (e.g. addresses, information on organizations, and using approved cloud services, etc.).
- The **“Instant Messaging”** policy outlines how employees can use instant messaging within the organization.
- The **“Remote Access”** policy outlines how employees can work remotely and their responsibility in accessing and protecting the organization's information, documents, and data.
- The **“Removable Storage”** policy outlines what is considered removable storage and that any information, documents, or data held on a removable storage device to be encrypted prior to being removed from the facilities.
- The **“Password”** policy outlines password requirements and how to create strong passwords for accessing the technology infrastructure, applications, software, and protect information, documents, or data from being illegally accessed either internally or externally.
- The **“Individual Responsibility to Information Security”** policy outlines the role employees have regarding information security. This is a partnership between IT Services and employees to ensure that all information, documents, and data are held and handled securely.
- The **“Software Downloading & Installation”** policy outlines IT requirements on how employees can make requests to have software or applications installed on their desktop computer, tablets, or other mobile devices. All software and application downloads are to be approved and downloaded by IT Services.

- The **“Mobile Device”** policy outlines IT requirements on how employees request access to use personal cellphone or request a corporate cellphone. Employees require supervisor and IT Services approval.
- The **“Third-Party Access, Non-Disclosure, and Responsibility”** policy outlines services and access provided to approved third parties. This includes a Non-Disclosure Agreement (NDA).
- The **“Acceptable Use and Individual Responsibility Agreement Form”** will require annual review and sign-off by employees to acknowledge that they agree to follow the Wheatland County Acceptable Use policies.

REFERENCES

- Addendum to Policy 4.2 – Acceptable Use and Individual Responsibility Policy Agreement Form.

Policy Name:	Organizational Commitment
Policy Number:	4.1.2
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to establish requirements for maintaining a "clean desk" and a "clear screen." A "clean desk" is a desk that is free of visible or easily accessible sensitive or critical information. A "clear screen" is the digital version of a clean desk, in that your computer screen is not left showing sensitive or critical information when you are not present.

Sensitive/critical information such as personal passwords, personal or employee salary information, or business documents that are deemed confidential must be secured in locked areas. This information must be kept out of reach and sight while offices are unattended, or when any third parties or other employees are in the office. Risks of security breaches (e.g., loss, missing or stolen information, documents, or data) is, therefore, minimized.

POLICY

The goal of the Clean Desk and Clear Screen Policy is to improve the security, privacy, and confidentiality of the organization.

This policy applies to all spaces where County information can be accessed such as offices, desktops, mobile devices, removable storage devices, software, offsite/onsite shared or personal workspaces (when working from home), or offices.

Employees and contractors must ensure that all sensitive and confidential information, documents, or data, whether digital, paper, removable storage media, or hardware is properly secured and protected from unauthorized view by employees, visitors, third-party vendors, or contractors.

To minimize risk of unauthorized access, loss, theft and damage to information, documents, data, hardware, and software, all county devices or devices approved for

“Bring Your Own Device” (BYOD) must always be software locked, whereby a password or pin is required to re-access the device.

Instructions

Windows PC: *Windows Key + L key to lock a Windows PC.

Mobile Devices: Mobile devices can be locked by turning the screen off. Re-entry to the mobile device must be secured by a password or pin.

Offices: Offices or desks where drawers or cabinets house sensitive or confidential information should always be locked, and keys supplied to authorized employees only.

This policy applies to employees, approved third parties, and contractors when working on Wheatland County-owned premises, remotely, or in other locations owned or operated by the organization (e.g., fire halls, maintenance shops, water treatment plants, etc.).

Policy Name:	Email
Policy Number:	4.2.3
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of the policy is to set out the acceptable use of Wheatland County corporate electronic mail (email).

POLICY

Email is an integral part of conducting business for the organization and has become the primary method of communication between both internal stakeholders and external organizations. The misuse or abuse of email can negatively impact the organization, its employees, its third-party vendors, or its contractors. This misuse or abuse can result in reduced productivity for those involved or a negative representation of the organization.

Employees or contractors that have been provided Wheatland County emails are to use corporate email only where the use supports the goals and objectives of the organization.

Employees should be aware that e-mails are subject to FOIP requests.

When employees, third-party vendors, and contractors are using corporate email they must ensure they:

- Comply with current legislation (Federal and Provincial),
- Use corporate email in an acceptable manner, and in adherence with Human Resources Policy Section - 6.1 Code of Conduct, and
- Not create unnecessary business risk to the organization by misuse of corporate email.

Unacceptable Use:

- Users must not post, transmit, or otherwise distribute materials which is unlawful, harassing, libelous, discriminatory, defamatory, racial, profane, abusive, threatening, harmful, vulgar, obscene, sexually suggestive, hateful, invasive of another's privacy, or otherwise objectionable,

- Users must not distribute or provide access to information, documents or data which is protected by copyright or other intellectual property rights, without attribution/permission to the rights of the holder(s),
- Posting, transmitting, or otherwise distributing messages constituting "spam" including unsolicited non-work related e-mail messages, phishing emails, malware distribution, inappropriate postings to news groups, false commercial messages, junk mail, and chain mail,
- Distributing confidential information, documents, or data belonging to the organization without appropriate authorization and applicable redaction, or providing access to personal information, as defined in the Access to Information and Privacy Act, except in accordance with proper authorization under that legislation,
- Engaging in any activity which, regardless of the purpose, constitutes appropriation of another person's identity,
- Communication in support of partisan political purposes including, but not limited to statements, opinions, or solicitations,
- Users must not indicate affiliation with the organization without appropriate authorization, and
- Conducting personal and/or personal external business (enterprise) over County supplied email.

REFERENCES

- Human Resources Policy Section 6.1
- Government of Canada, *Access to Information Act*
- Government of Canada, *Privacy Act*

Policy Name:	Internet
Policy Number:	4.2.4
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to provide Wheatland County employees guidance on acceptable use of the internet. This policy will outline the impact that inappropriate use of the internet can have on shared technology resources and to provide clarity on related security matters.

POLICY

The internet is a valuable tool that is made available to employees to assist in fulfilling their functional responsibilities and obligations to the organization.

To ensure that policies are followed, and to ensure the highest level of security possible, the County will monitor internet traffic and browsing history while logged into the network. Websites that are deemed as a high security threat (e.g., pornography, pirating, or gambling) will automatically be blocked. In some cases, frequency of attempting to access these types of websites may be reported to IT Services.

Acceptable Use:

- Employees must ensure they use the internet in an acceptable manner in adherence with Human Resources Policy Section - 6.1 Code of Conduct,
- To accomplish job responsibilities and the core responsibilities or goals of the organization,
- To communicate with work-related professional contacts,
- To improve familiarity with the range and depth of the information on the internet,
- To pursue personal development through learning,

- To distribute and make available information to employees with approved internet tools,
- Using the internet for personal use, namely during breaks, and within reason, provided that such use does not interfere with the performance of regular duties, obligations, or breach business professionalism, and
- Within the constraints of any mobile data plan.

Unacceptable Use:

- Conducting illegal activities that includes copying and sending confidential or proprietary information or software that is protected by copyright and other laws protecting intellectual property, and maliciously or knowingly spreading viruses or malware. Illegal activities may be reported to the RCMP for investigation,
- Accessing websites supporting hate, pornography, gambling, excessive shopping or auctions, investments or stock trading, gaming, espionage and terrorism, theft, or drugs, unless accessing such sites is a requirement of your job responsibilities and such access is authorized by management,
- Transmitting, sharing, or downloading material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic, or obscene, and
- Participating in activities regarding the preparation or distribution of content that could damage the County's image or reputation.

REFERENCES

- Human Resources Policy Section – 6.1 Code of Conduct

Policy Name:	Instant Messaging
Policy Number:	4.2.5
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to set out the acceptable use of corporate instant messaging.

POLICY

Employees are provided the use of Wheatland County supplied internal chat systems and mobile text messaging (SMS) capabilities to facilitate instant messaging between individuals within, and outside of, the organization in a secure way.

Wheatland County will provide employees with access to secure instant messaging platforms approved by the County to protect the business information being shared amongst staff. Instant messaging clients that exist outside of Wheatland County approved applications may not provide sufficient authentication of the parties involved in the conversation, resulting in a risk exposure to Wheatland County employees. When using non-County approved applications, employees may not be assured that they are communicating with who they think they are (the individual may not be who they are claiming to be) or in a secure manner. For this reason, it is encouraged that Wheatland County employees only utilize County-approved instant messaging platforms when discussing County-related business.

Employees are not permitted to download Facebook Messenger, Yahoo! Messenger, AOL Instant Messenger, MSN Messenger, Google Talk, etc. on any corporate-owned device or use any non-County approved instant messaging services for business communication. If any messaging software is discovered on a corporate device, it will be automatically deleted by IT Services and disciplinary action may be taken.

The exception to this policy is if an approved/trusted third party hosts a virtual meeting and needs to use their own software such as GoToMeeting, Zoom, etc. or the role permits the use of other tools such as Facebook, Instagram, and Twitter instant messaging for corporate communications to the public.

Employees should be aware that instant messages and conversation threads regarding any Wheatland County business, regardless of the service, are subject to FOIP.

Acceptable Use:

- Instant messaging services must be used in an acceptable manner, and in adherence to Human Resources Policy Section - 6.1 Code of Conduct, and
- As outlined as an acceptable use in Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.

Unacceptable Use:

- Communications consisting of non-public or confidential information,
- Communications utilized in such a manner as to qualify as "excessive personal use" and that interfere with the functional responsibilities, tasks, and projects of employees, and
- As outlined as unacceptable in Sections Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.

REFERENCES

- Human Resources Policy Section 6.1 – Code of Conduct
- Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4

Policy Name:	Remote Access
Policy Number:	4.2.6
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to outline the responsibilities of Wheatland County employees when remotely connecting to the technology infrastructure of the County.

POLICY

Wheatland County employees are only permitted to perform County business via remote access upon authorization by IT Services.

Remote access allows employees to connect with computer desktops, cloud applications/services, or servers from alternative locations using corporate laptops, personal computers, smart phones, tablets, etc.

When remotely accessing the County’s network, employees will use a VPN (Virtual Private Network) gateway sanctioned by IT Services with an authentication code provided to users at the time of signup. When connecting remotely from any device in this manner, employees will have the same access rights as if they were in the office and, therefore, it is important to ensure their location and devices are secure.

All County policies apply to employees when working remotely and accessing Wheatland County computer desktops, servers, or cloud applications/services.

Failure of employees to adhere to this policy will result in remote access rights being revoked by IT Services and other disciplinary action as applicable.

Policy Name:	Removable Storage Devices
Policy Number:	4.2.7
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of the policy is to minimize and mitigate the potential loss of information, documents, or data removed from Wheatland County facilities on removable storage devices. Removable storage devices limit the County’s ability to control its location, thus making its access a risk. Additionally, this policy will act to reduce the risk of acquiring malware infections on the County’s technology infrastructure using removable storage devices.

POLICY

This policy applies to all removable storage devices that employees use to download information, documents, and data from the technology infrastructure and County buildings.

Removable storage devices are defined as “a portable readable and/or writable device (or mediums) by which end users can transport information between computers.”

Types of removable/portable storage devices include:

- Flash drives (USB sticks/thumb drives, SD cards),
- Devices with imbedded storage such as IoT devices, MP3 players, cameras, “Fitbits”, and mobile phones,
- Removable or internal hard drives or Solid-State Drives (SSD), and
- Optical disks such as CD’s, DVD’s, and BlueRay disks.

Prior to sharing information, documents, or data on a removable storage device with other organizations or with each other, it is preferred that employees use approved secure/encrypted cloud storage and sharing systems such as Laserfiche, OneDrive or

SharePoint, whereby employees and IT Services have control over access, security, and permissions to the information.

If a portable storage device must be used, all removable storage devices being sent to other organizations with any non-public information must be encrypted and protected with a secure password[1]. Employees are responsible for the information, documents, or data on the removable storage device.

Lost or stolen removable storage devices are to be reported immediately to IT Services. Depending on the type of information, documents, or data on the removable storage device and whether the device is encrypted, could be considered a data breach.

Employees are prohibited from connecting any portable storage device into a corporate computer if employees are unaware of its origin and/or the origin is untrusted. If a storage device origin is unknown or untrusted, employees must turn in the device to IT Services or Records Management for safe discovery and retrieval of information.

The information, documents, or data on the removable storage device can only be shared with the individual identified as the device recipient. Sharing the information, documents, or data with anybody else is in violation of the Information, Security, and Technology Policy.

Retrieval of a file, applicable to any records retention, that originates on a portable storage device must be saved in an appropriate file server or Laserfiche for proper retention. The device is to be cleared of its original information.

PROCEDURE

[1] Turning on Device Encryption:
https://tech.wayne.edu/kb/security/computer-device-security/26186

Policy Name:	User Accounts and Passwords
Policy Number:	4.2.8
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to set requirements for maintaining secure accounts and passwords for access into mobile devices, systems, servers, applications, or cloud services under Wheatland County's corporate domain.

POLICY

The organization recognizes that information, documents, data, and anything else that can be considered corporate resources, are valuable. It is important that access to these resources is limited to those individuals within the organization who have a legitimate reason for access and are approved as such. The County must also protect information from being illegally accessed, either internally or externally, by parties not approved for access.

The creation of passwords or pins provides authorized access through accounts to devices, networks, application, and software. Passwords combined with additional security measures such as multi-factor authentication significantly limits the possibility of others gaining access to data held on internal or external sources should the password be breached.

Passwords must:

- Be changed as soon as possible upon issuance for the first use,
- Be securely transmitted to individuals by administrators,
- Never be shared with another individual,
- Never be requested from one employee of another employee,

- Never to be written down and then left in a location easily accessible to others in an open or unlocked location,
- Not be stored in a web browser’s password manager in any publicly accessible PC but can be stored in a secure password management system,
- Never be stored in Word, Excel, or any other unencrypted file on a computer, mobile device, or network, and
- Enable or use multi-factor authentication where possible, or required.

Accounts may be locked out after multiple attempts to login with an incorrect password. The number of attempts allowed is dependent on the application or software.

Systems and applications may request passwords to be changed, and new passwords must comprise of upper-case characters, lower-case characters, numbers, and symbols. It must not include usernames, first name or last names of the account holder, and have a level of length and sophistication that cannot be easily guessed.

Compromised passwords or user accounts must be reported to IT Services and the breached password must be replaced with a new password as soon as possible.

If an account is shared (i.e., group/service accounts), and where more than one user is able to access the same account, passwords are to be changed when any user that had access to that account leaves the organization. This procedure must be done at the earliest opportunity by the manager of the group sharing the account, and then the password redistributed to the group securely. When a user (employee, contractor, or vendor) leaves the organization, a request must be sent by Human Resources or the supervisor of the user to have accounts to various systems disabled for security reasons.

Employees found intentionally attempting to gain access to accounts or secure data (hacking, sharing account information without approval, or holding for ransom any account or data) without Human Resources and/or Senior Management approval may be grounds for immediate termination.

Policy Name:	Personal Responsibility to Information Security and Access
Policy Number:	4.2.9
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

This policy outlines employee responsibilities regarding security of information, documents, and data.

POLICY

Employees have a responsibility to maintain confidentiality and protect information of documents and data stored on technology, desks, in filing cabinets and other physical file storage facilities.

As a function of their role, employees are granted access to information, documents, and data. This access allows employees the right to:

- Access only to information, documents, and data for which there is a business need and to carry out job responsibilities, and
- Disseminate information, documents, or data to others who have a need-to-know and have the approval to view or edit such information.

Employees are required to:

- Report file access privileges that are incorrect to IT Services,
- Report any actual or suspected vulnerabilities in the confidentiality or integrity of the technology infrastructure or filing systems to IT Services,
- Report suspected breaches in the information, documents, or data,
- Not disable firewalls and/or anti-virus and/or security technologies etc.,
- Not leave confidential files outside a secure space,
- Protect access to accounts and passwords,

- Accept responsibility for user accounts,
- Maintain confidentiality of information, documents, and data,
- Complete assigned information security training and maintain knowledge about information security as it pertains to passwords, files, account access, phishing scams, social engineering, malware, and zero day/ransomware, etc., how they occur, and how to avoid security breaches and apply learnings to daily use of the County's technology and information with extreme diligence,
- Perform all responsibilities necessary to protect information, documents, or data when transferring information, documents, or data to a removable storage device or cloud storage service,
- Maintain physical security of personal assigned access badges, any assigned fobs, keys, access codes to facilities, alarm codes, technology, assets, consumable resources, and vehicles,
- Help ensure no unauthorized persons enter the County secured areas without permission or through access assignment by administration, who provide access to facilities based on the level of temporary access required,
- Ensure visitors (with visitor access granted) have visitor badges and are always accompanied while in secure areas of the County's facilities, and
- Ensure visitors with re-entry capabilities such as contractors have signed the Non-Disclosure Agreement and third-party access agreement at the time of contract signing and have been granted a re-entry visitor badge for each day they are required to be onsite.

Policy Name:	Software and Installations
Policy Number:	4.2.10
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

This policy outlines permitted downloading and installing of software by employees on corporate devices.

POLICY

Installation of unauthorized software accessed on the Internet or uploaded from a removable storage device can introduce serious, fast-spreading security vulnerabilities. Unauthorized software, even those seemingly provided by reputable vendors and trusted companies, can introduce viruses and Trojan programs that aid attempts to illegally obtain or hold for ransom, sensitive, proprietary, data, and confidential information documents.

Protecting the organization's technology infrastructure, information, documents, and data from unauthorized access and guarding against information, documents, or data breaches or loss is of paramount importance.

Employees are not permitted to download or install unapproved software. If software is required for the use of conducting day-to-day business, a request must be initiated to IT Services to review the software's integrity and approve or deny its use. Once it is approved for use, the software will be available on the software library and subsequent installs can happen with a request to IT Services.

IT Services will automatically delete any unapproved software found on desktop computers or portable devices.

Software acquired through illegal means will not be approved for install. Software or files such as torrents, TOR, VPN Masking, Block Chain, Dark Web applications, worms, malware, keyloggers, cracked software, or other obscure software shall not be installed or used on Wheatland County corporate networks or storage devices for any reason, unless required and approved as necessary for duties of particular roles, such as law enforcement or data investigation.

Software or cloud solutions must be accompanied by a valid purchase agreement and licence. IT Services holds the right to reject any software or cloud solutions purchased or subscribed to that has not been reviewed and approved by IT Services and/or does not meet internal software/solution selection criteria.

Policy Name:	Mobile Devices
Policy Number:	4.2.11
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

Wheatland County grants, securely and at its discretion, certain employees the ability to use mobile devices for the purposes of conducting County business. It may also grant the privilege of using an approved personal device in lieu of being provided an additional County owned device, approved at the discretion of management.

POLICY

This policy applies to any corporate owned mobile device or Bring Your Own Device (BYOD) that has been approved for business use, and any other County device that is allowed to enter or leave County facilities and used in personal or in public locations.

The County policies extend to the device that has left the premises, including the networks it connects to, the location, and potential access to the device by non-Wheatland County parties.

To be granted the ability to use a mobile device to conduct County business, additional approval and agreement forms are required.

For domain connected laptops, and/or corporate phones, the Mobile Device Approval Form (Addendum to Information, Security, and Technology Policy Section 4.2.11), and the Corporate Device Agreement Form (Addendum to Information, Security, and Technology Policy Section 4.2.11.2) are required.

For BYOD Android or Apple mobile phones and/or tablets, Mobile Device Approval Form (Addendum to Information, Security, and Technology Policy Section 4.2.11) and BYOD Device Agreement Form (Addendum to Information, Security, and Technology Policy Section 4.2.11.1) are required.

REFERENCES

- Information, Security, and Technology Policy Section 4.2.11
- Information, Security, and Technology Policy Section 4.2.11.2
- Information, Security, and Technology Policy Section 4.2.11.1
- Addendum to Policy 4.2.11 – Mobile Devices – Mobile Device Approval Form

DEFINITIONS

“BYOD” or “Bring Your Own Device” is a personal mobile device that has also been authorized and setup securely with a corporate profile for County business use.

Policy Name:	Mobile Device – Bring Your Own Device (BYOD)
Policy Number:	4.2.11.1
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The County grants, at its discretion, certain employees the privilege of opting to use personal smartphones and/or tablets at work for the purposes of County business. The Bring Your Own Device (BYOD) option is available instead of being provided a County-owned device.

POLICY

This policy is intended to protect the security and integrity of Wheatland County's data and technology infrastructure. Limitations to the ability to use the BYOD program may occur due to unforeseen variations in compatible devices, the device does not meet security standards, or depending on job-related risks, put unnecessary risk on the integrity of the device etc.

County employees must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network through a mobile device management system.

Management reserves the right to revoke this privilege at any time if users do not abide by the policies and procedures outlined below, or if their device no longer meets current security standards. If BYOD access is revoked, IT Services may remove its software and data off the personal device and may require an employee to use a County owned device for the continued operation in an employee's role.

Acceptable Use:

- Acceptable *business use* is defined as an activity that directly or indirectly supports the business of the County,
- Acceptable *personal use* is defined as reasonable and limited personal communication that namely occurs during beaks and within reason, provided that

such use does not interfere with the performance of regular duties, obligations, or breach business professionalism,

- Employees may be blocked from accessing certain websites on the corporate profile of the phone or during business hours,
- Devices may not be used at any time to:
  - Store or transmit illicit materials,
  - Represent the County in a negative way,
  - Transmit proprietary information belonging to the County to another company on non-business-related activity,
  - Engage in outside business activities while on company hours,
  - Used in an acceptable manner in adherence to Human Resources Policy Section - 6.1 Code of Conduct, and
  - As outlined as acceptable in Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.
- Any application not downloaded through a trusted authority such as Google Play, Apple's App Store/iTunes, or Microsoft Store is implicitly not allowed; any application that could be deemed a security threat, hacking, explicit, or otherwise are not appropriate in a business setting,
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, VPN, remote desktop, authentication, productivity applications, and any other applications that are posted on the company portal, and
- Wheatland County has a **zero-tolerance** policy for distracted driving, such as texting or emailing while driving. Those who operate Wheatland County-owned vehicles or those who are operating a personal vehicle for the purpose of conducting Wheatland County business must abide by the *Alberta Traffic Safety Act* and ensure devices are in hands-free mode while talking or navigating.

Devices and Support:

- Smartphones and/or tablets are allowed, granted they are up to date and meet minimum operating system requirements, storage, and device security standard.
- Connectivity and company installed application issues are supported by IT Services; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Before accessing the network, devices must be enrolled into our device management program for provisioning and configuration of standard apps, such as enrollment profiles, network settings, office productivity software, and security tools.

Reimbursement:

- The County will contribute $50.00 per pay period equating **to a maximum of $100.00 per month**, towards the cost of the mobile device plan. The County does not reimburse costs of the mobile device itself or accessories.
- All contributions towards the cost of the mobile device plan by the County will be considered a taxable benefit.
- The company will not reimburse employees for the following charges:
    - Roaming,
    - Phone or data plan overages,
    - Accessories, or
    - Damaged or hardware replacements.
- Any damages to the device while on County business are at the risk and expense of the employee.

Security:

- To prevent unauthorized access, devices are required to have at the very least, a strong 6 (six) digit pin in order to access the company network.
- The device must lock itself if it is idle for more than 5 minutes.
- After 5 failed login attempts, the device will lock. To regain access, IT Services must be contacted.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network. Attempting to do so will remove the employee from the BYOD plan.
- Employees are automatically prevented from downloading, installing, and using any app that is not authorized by a trusted provider within the work profile ecosystem.
- Smartphones and tablets that are not on the company's list of supported devices are deemed unfit for corporate use and are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT Services and automatically enforced.
- The employee's device may be remotely wiped (factory reset – entire phone data deleted) if:
    - The device is lost,
    - IT detects a data/security breach such as a virus originating from the device or similar threat to the security of the company's data and technology infrastructure, or

    - The employee is acting in a way that threatens the security or public integrity of the County.

- The employee's device will have Wheatland County applications, email, and data removed (wiped) from the device if:
    - The employee's employment has been terminated, or
    - The employee's role changes where applications or Wheatland data is no longer required. Personal data, images, and videos will not be removed.

Risks/Liabilities/Disclaimers

- While IT Services will take every precaution to prevent employee personal data from being lost in the event that it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, pictures, data, contacts, etc.
- In the unlikely event a device is completely wiped, the County is not responsible for any lost data.
- Employees should be aware that communication regarding any County business, regardless of the medium, are subject to FOIP requests.
- It is recommended to not use SMS/instant messaging for decisions or discussions of any substantial County business, whereby the message/s would be considered a business record. If SMS was used, in the event of a FOIP request, it is the responsibility of employees to submit unaltered screenshots of any County related discussions, decisions or transactions conducted through SMS related to that request or face a fine up to $10,000 per Section 92 of the *FOIP Act*.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to IT Services within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- Employees are always expected to use devices in an ethical manner and adhere to the County's Acceptable Use Policy.
- The County reserves the right to publish your personal phone number in the internal company contact directories. This number, while stored in Office365, will not be given out to any third party for non-County related business.
- Employees are personally liable for all costs associated with their device.
- Employees assume full liability for risks including, but not limited to, physical damage, the partial or complete loss of company and personal data due to physical damage, an operating system crash, errors, bugs, viruses, malware, device data wipe, and/or other software or hardware failures, or programming errors that render the device unusable.

- The County reserves the right to take appropriate disciplinary action up to, and including, termination for noncompliance with this policy.

Your Privacy

IT Services cannot see the following on your device:	**IT Services can see the following on your device:**
• Call and web history • Location • Email and text messages • Contacts • Passwords • Calendar • Camera / Images / Files	• Model • Serial Number, IMEI • Operating System • Corporate Application Names • Owner • Device name

REFERENCES

- Office of the Information and Privacy Commissioner of Alberta – BYOD https://www.oipc.ab.ca/resources/subjects/bring-your-own-device.aspx
- Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.
- Government of Alberta, *FOIP Act*
- Government of Alberta, *Traffic Safety Act*
- Addendum to Policy 4.2.11.1 – BYOD Device Use Agreement Form

DEFINITIONS

“BYOD” or “Bring Your Own Device” is a personal mobile device that has also been authorized and setup for County business use.

Policy Name:	Mobile Device – Corporate (County Issued)
Policy Number:	4.2.11.2
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

Wheatland County grants, at its discretion, certain employees the use of Wheatland County smartphones, tablets and/or laptops for the purposes of conducting County business. This policy outlines the expectations of employees when using mobile corporate devices.

POLICY

This policy is intended to protect the security and integrity of Wheatland County's data and technology infrastructure.

County employees must agree to the terms and conditions set forth in this policy to be permitted to use mobile corporate devices.

Management reserves the right to revoke this privilege at any time if users do not abide by the policies and procedures outlined below, or if their device or use does not meet current security standards.

Acceptable Use:

- The company defines *acceptable business use* as activities that directly or indirectly support the business of Wheatland County.
- The company defines *acceptable personal use* on company time as reasonable and during breaks or off hours and limited to personal email communication or recreation, such as web surfing, streaming, reading, personal phone calls, or social media.
- Employees may be blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the County.
- Devices may not be used at any time to:
  - Store or transmit illicit materials,

  - Represent Wheatland County in a negative way,
  - Transmit proprietary information belonging to the County to another company on non-business-related activity,
  - Engage in outside business activities,
  - Used in an acceptable manner in adherence to Human Resources Policy Section - 6.1 Code of Conduct, or
  - As outlined as acceptable in Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, VPN, remote desktop, authentication, productivity applications, and any other applications that are posted on the company portal.
- Wheatland County has a **zero-tolerance** policy for distracted driving, such as texting or emailing while driving. Those who have access to a Wheatland County corporate device must abide by the *Alberta Traffic Safety Act* at all times while operating any motor vehicle, and ensure the device is in hands-free mode while talking on it or navigating with it.

Devices and Support:

- Before accessing the network, devices must be enrolled into the County's device management program as a corporate owned device for provisioning and configuration of standard apps, such as enrollment profiles, network settings, office productivity software, and security tools.
- Corporate devices are deployed with a standard manufacturer, operating system, and support. IT Services follows standard device replacement lifecycles and will replace or repair devices at its discretion.
- To ensure accountability to our financial standards, device models are deployed to employees based on risk and features required by role.

Security:

- To prevent unauthorized access, telephone devices are required to have at the very least, a strong 6 (six) digit pin in order to access the company network.
- The device must lock itself if it is idle for more than 5 minutes.
- After 5 failed login attempts, the device will lock. In order to regain access, IT Services must be contacted.
- Attempting to root (Android) or jailbreak (iOS) a corporate owned device may result in disciplinary action and removal of mobile device privileges.
- Employees are automatically prevented from downloading, installing, and using any application that is not authorized by a trusted provider.

- Employee’s access to company data is limited based on user profiles defined by IT Services and automatically enforced.
- The device may be wiped (factory reset – entire data deleted) if:
    - The device is lost,
    - IT detects a data/security breach such as a virus originating from the device or similar threat to the security of the company’s data and technology infrastructure,
    - The employee is acting in a way that threatens the security or public integrity of the County, or
    - The employee leaves the organization.
- The device will have Wheatland County applications, email, and data removed (wiped) from the device if:
    - The employee’s role or security requirements change where applications or access to certain Wheatland data is no longer required. Images and videos will not be removed.

Risks/Liabilities/Disclaimers:

- While IT will take every precaution to prevent data from being lost in the event it must remote wipe a device, it is employees’ responsibility to take additional precautions, such as backing up email, pictures, data, contacts, etc.
- In the unlikely event that a device is completely wiped, the County is not responsible for any lost data.
- Employees should be aware that communication regarding any Wheatland County business, regardless of the medium, are subject to FOIP requests.
- It recommended to not use SMS/instant messaging for decisions or discussions of any substantial County business, whereby the message/s would be considered a business record.
- If SMS was used, and in the event of a FOIP request or investigation, it is the responsibility of employees to submit unaltered screenshots of any County related discussions, decisions or transactions conducted through SMS related to that request or face a fine up to $10,000 per Section 92 of the *FOIP Act*
- Corporate devices may be requested in the event of a FOIP request or investigation.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to IT Services within 24 hours.
- Employees are always expected to use devices in an ethical manner and adhere to the company’s Acceptable Use Policy as outlined above.

- Wheatland County reserves the right to publish phone numbers in the internal company contact directory and external contact publications.
- While Wheatland County assumes all liability in terms of damage to a device, frequent or careless damage to devices may result in removal of mobile device privileges.
- If a role requires extra care in reinforcing the casing of a device or the device itself must be a “tough” or “reinforced” device, this request must come from a supervisor and a GL Code provided for the additional costs to support the purchase requirement.
- Wheatland County reserves the right to take appropriate disciplinary action up to, and including, termination for noncompliance with this policy.
- Corporate owned devices must be returned to IT Services upon termination and personal images or information that may be stored on the device will be wiped. Wheatland County is not responsible for recovering personal information from a corporate device.

Your Privacy

IT Admin cannot see the following on your device:	**IT Admin can see the following on your device:**
• Call and web history	• Model
• Location	• Serial Number/IEMI
• Email and Text Messages	• Operating System
• Contacts	• Application Names
• Passwords	• Owner
• Calendar	• Device name
• Camera / Images / Files	• Levels of Security / Networks
	• Location (of lost device)

REFERENCES

- Information, Security, and Technology Policy Sections 4.2.3 & 4.2.4.
- Government of Alberta, *FOIP Act*
- Government of Alberta, *Traffic Safety Act*
- Addendum to Policy 4.2.11.2 – Corporate Mobile Device Use Agreement Form

DEFINITIONS

“Root / Jailbreak” means to perform a series of steps to override and gain access to the core operating system of the device such that the manufacturer’s built-in security features has been or can be overridden by any application or user.

Policy Name:	Third Party Access and Responsibility
Policy Number:	4.2.12
Policy Owner:	IT Services
Adopted Date:	March 23, 2021
Effective Date:	March 23, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to set out requirements for third-party vendors and contractors for accessing and protecting Wheatland County's facilities, information, systems, documents, and data. It outlines the responsibilities of engaging third-party services that require access to County systems and/or non-public information.

POLICY

When engaging with a third-party vendor or contractor that requires unattended access to one or more County facilities, its non-public information, and/or computer/information systems, the employees responsible for the County portion of the service contract must sign and have the third-party vendors or contractors sign the Confidentiality, Non-Disclosure and Third Party Access Agreement *(Addendum to 4.2.12)* before any unattended access will be granted to facilities, technology systems, files, or confidential information that they may be privy to while conducting business with the County.

Third-party vendors and contractors will be required to adopt, at minimum, corporate standards for information security controls, as well as abide by the Information, Security and Technology Policies, Acceptable Use, and Individual Responsibility policies.

Additional controls may also be required depending on vendor engagement such as:

- Robust and documented change control processes, including regular release management cycles,
- Vulnerability management, security patches/fixes, and changes to vendor internal IT assets to ensure they are up-to-date and protected,
- Controls to prevent changing, copying, or altering any code or its information or documentation belonging to the County without prior written permission or change approvals,

- Internal intrusion detection, prevention, and recovery controls that protect against malicious code and maintain all anti-virus software and signatures current and actively running to detect and remove malware from vendor systems accessing the County's systems,
- Tools or procedures that help protect third-party vendor or contractor's employees from downloading unauthorized programs onto the County's infrastructure without proper change approvals, and
- The ability to produce proof of liability insurance in the case of a data/information breach.

Third-party vendors or contractors shall implement a comprehensive and structured approach to protecting information, documents, or data accessed from the County, its facilities, documents, or technology systems.

Third-party vendors or contractors shall evaluate and monitor their exposure to security risks and other threats and take appropriate measures to address the associated risks to their facilities and information, documents, or data that belongs to the County.

Third parties shall use best practices for the exchange of information, for example, use secure managed file transfer services such as Cloud or SFTP services.

Consequences of non-compliance or data breach by a third-party vendor or contractor may be in breach of the agreement with the County and subsequently, a termination of the relationship or contract between the organization and the third-party vendor or contractor may occur, alongside any other consequential damages.

REFERENCES

- Addendum to Policy 4.2.12 – External Access, Confidentiality, and Non-Disclosure Acknowledgement Agreement Form
- Addendum to Policy 4.2.12 – Acceptable Use and Individual Responsibility Policy Agreement Form

Policy Name:	Asset Management Policy
Policy Number:	4.3
Policy Owner:	Chief Administrative Officer
Adopted Date:	January 12, 2021
Effective Date:	January 12, 2021
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to provide a commitment to asset management practices and to establish the philosophies and values that will guide the County as they develop a collaborative and consistent asset management system across the organization.

OBJECTIVE

Asset management practices is an iterative process that continuously improves and evolves. Applying asset management best practices will allow the County to:

- Obtain a holistic understanding of the state of infrastructure for the County's entire infrastructure portfolio;
- Develop unified and aligned goals to meet the needs of County residents;
- Increase confidence that the County budget is being focused where it is needed most; and
- Effectively solve complex interdisciplinary problems.

SCOPE

This policy applies to all physical and financial assets under the control of the County and includes, but is not limited to, Transportation, Water, Wastewater, Storm, Facilities, Information Technology, Fleet, and Fire Fighting assets.

POLICY

Wheatland County shall adopt and apply asset management practices to provide effective financial and physical management of existing and future assets to ensure safe, reliable, and sustainable services to its residents. New methods will focus on incorporating the following principles into its existing management practices:

- **Aligned Organizational Goals:** Community needs, and Council goals will lead the organization goals at each level of the organization. Shortfalls and realities at each level of the organization will be communicated up to Council to ensure service level goals are achievable.

- **Data-Driven Decision Making**: The County will make decisions by analyzing service levels, risk, inventory, and condition needs. The cost to benefit ratios will be analyzed for new initiatives and prioritized in a manner that will maintain public confidence in how the County manages its infrastructure.

- **Consistency:** The County will develop a consistent and repeatable approach to asset management data collection and reporting to gain a holistic understanding of the County's state of infrastructure and service delivery.

- **Fiscally Responsible**: The County will consider the long-term projections of investment needs when developing annual budgets to ensure the services provided today are not compromising the fiscal sustainability of future generations.

- **Innovation and Continuous Improvement**: The County will continually incorporate asset management best practices into the organization and strive to develop new ways to improve service delivery and organizational efficiency.

DEFINITIONS

"Asset" is a physical component of a system that enables a service or services to be provided.

"Asset Management" is the process of making decisions about how infrastructure is used and cared for in a way that manages current and future needs, considers risks and opportunities, and makes the best use of resources.

"Asset Management System" is an interconnecting network of policies, people, practices, processes and software that enable asset management. An asset management system is not a software program.

"Risk" is exposure to the possibility of injury or loss of service and is always present. It is measured by multiplying the likelihood by the impact of an anticipated event.

"Levels of Service" describes the standard of outputs or objectives an organization intends to deliver to its customers. They typically relate to service attributes which includes but is not limited to quality, reliability, responsiveness, sustainability, timeliness, accessibility and cost.

"Lifecycle Strategies" is a list of activities that can be applied to an asset to reduce the lifecycle cost or meet a targeted level of service standard.

"Infrastructure" the body of in-service assets that are used to supply or support services to the County.

RESPONSIBILITIES

Key roles and responsibilities essential for establishing asset management policies, objectives, and practices are:

Council

- Review and adopt the asset management policy
- Prioritize and articulate community priorities

CAO & Executive Team

- Recommend this policy and any amendments for adoption by Council
- Be a visible champion for the implementation of asset management practices across the organization

Asset Management Specialist

- Develop an asset management framework that includes plans and procedures and incorporates the principles identified in the Asset Management Policy

Managers and Staff

- Participate and be open-minded to new methods of asset management principles and service delivery
- Ensure that any data entry into the plans is timely, accurate and reliable
- Approve the asset management plans

REFERENCES

Policies:

- Organizational Policy Section 1.1 – Vision
- Organizational Policy Section 1.2 – Mission Statement
- Organizational Policy Section 1.3 – Values
- Corporate & Financial Services Policy Section 2.2 – Tangible Capital Assets
- Corporate & Financial Services Policy Section 2.4.1 – Risk Control

Policy Name:	Information Management Policy
Policy Number:	4.4
Policy Owner:	Information Services
Adopted Date:	October 4, 2022
Effective Date:	October 4, 2022
Date Last Amended:	N/A
Date Last Reviewed:	N/A

PURPOSE

The purpose of this policy is to guide and direct the creation and management of information assets (records, information, and data) herein known as "information", regardless of the medium and to clarify the accountabilities of information users.

Information Services is committed to establishing, maintaining, and promoting information management best practices that meet industry standards, County needs, accountability requirements, and stakeholder expectations.

The benefit of compliance with this policy will be trusted information that is well described, stored in known endorsed locations and accessible to staff and residents where permission has been granted.

SCOPE

This policy applies to staff (full, part-time, hourly, and Seasonal), Council, and vendors, who create, receive or maintain information to support County business activities and programs.

POLICY

Information Services recognizes information, in any format or medium, as valuable assets to the County and is committed to achieving appropriate and ongoing management of this information.

Information Services is also committed to the principles and practices set out in the Canadian General Standards Board (CGSB), International Standards Organization (ISO), American Records Management Association (ARMA) and Association of Intelligent Information Management (AIIM) to implement, maintain, and promote fit-for-purpose information management policies, standards, and procedures. All information management practices will align with this policy, supporting standards, and procedures where they strategically align with County Practices.

GUIDELINES

The following are guidelines which are to be adhered to when creating or managing physical and digital documents or scanned images which are further described in our procedures and standards.
Signatures – Use the correct type of digital signature when signing or having documents signed.

In-House Scanning – Follow in-house scanning procedures from preparation to quality control.

Information Storage – Digital documents and scanned images are stored in the appropriate recognized storage site with complete metadata.

Destruction of Hardcopy – Upon completion of quality assurance of scanned images follow procedures for the destruction of hardcopy documents.

Disposition (Hardcopy, Digital Document and Scanned Images) Staff are to delete or shred copies of documents that have followed disposition procedures and met retention.

Signature Attestation – Staff to complete attestation prior to electronic signature use.

Freedom of Information and Protection of Privacy (FOIP) – Staff to understand and adhere to basic tenants of FOIP.

Hardcopy Filing – Staff to file hardcopy documents in the appropriate file, in the endorsed physical file location.

Scanner Settings – Staff to check scanner settings are reset to default settings after use if settings have been altered during scanning of the document.

ACCOUNTABILITY

Information Services is accountable to implement the mandate of this policy. Additionally, Information Services will ensure that information is held securely against internal and external threats and that the concept of “open by design and closed by exception” is enforced. Finally, the department is accountable to provide guidelines, standards, procedures, and training so that physical files, digital documents and scanned images are recognized as the official business records of the County.

Staff (Full-Time, Part-Time, Hourly, and Seasonal), Council and Vendors are accountable for maintaining County information which includes ensuring the security, accuracy, reliability, and availability of the information for all staff members, who require access to the information regardless of the medium.

Wheatland County as owner of all information received or created by the above are accountable to support Information Services in implementing the mandate of this policy.

REFERENCES

Standards

Departmental Folders > Information Services > Information Management > Documentation and Process > Policy > Standards

Procedures

Departmental Folders > Information Services > Information Management > Documentation and Process > Process and Procedure