POLICY MANUAL

Legal References:	Policy department: Information Systems
Cross References: • Policy L7 - Personnel Policy • Policy C21 - Disposal of Assets Policy • Policy P1 - Records and Information Management • AD IS-1 – Shared Network Drives • AD IS-2 – Corporate-issued Mobile Device • AD IS-3 – BYOD Mobile Device	Policy Number: R1
Adoption Date: • December 8, 2003 Resolution 12/1042/2003 Revision Date: • April 18, 2006 #04/499/2006 • May 9, 2016 - #CM20160509.1022 • Nov 7, 2016 - #CM20161107.1013 • May 31, 2018 - CAO Approval Form	Policy Title: Electronic Devices, E-mail and Internet Use Review Date: May 2021

POLICY PURPOSE:
To establish a Policy for the use of Electronic Devices, e-mail and internet in the workplace.

Electronic Devices, e-mail and internet are valuable tools to assist Users in performing the legitimate work of the County of Grande Prairie No. 1. It is important that such “tools” be utilized in a professional and responsible manner. This Policy outlines the appropriate use of these Corporate Resources by identifying responsibilities, requirements and providing guidance for the use of Electronic Devices, Internet and E-mail. Specific guidelines are required to safeguard systems from potential viruses and other hazards which place Corporate Resources at risk.

This Policy applies to all County employees, council members, contractors, temporary help and agents or representatives acting on behalf of the County authorized to use Corporate Resources.

DEFINITIONS:

- **Bring Your Own Device – BYOD** – Procedure (Schedule "A") establishes the guidelines to use personally-owned Mobile Devices in the workplace.
- **Corporate Electronic Device** means a device owned by the County and issued or reimbursed to eligible Users for the purpose of conducting County business. A device that accomplishes its purpose electronically; includes but not limited to any laptops, desktop computers, tablets, smart phones, cellular, land line phones, and audio/visual equipment.
- **Corporate Networks** means a network owned and provided by the County.
- **Corporate Resources** means any item owned and provided by the County.
- **Corporate Software** means software owned and provided by the County**.**
- **County** means the municipality of the County of Grande Prairie No. 1 having jurisdiction under the Municipal Government Act and other applicable legislation.
- **Data Protection Schemes** means the process of safeguarding important information from corruption and/or loss.
- **Electronic Devices** means a device that accomplishes its purpose electronically; includes but not limited to any laptops, desktop computers, tablets, smart phones, cellular, land line phones, and audio/visual equipment.
- **Information Systems Personnel** means any Employees under the umbrella of the Information Systems unit of, Corporate Services Department as per the County Organizational Chart.
- **Security Loopholes** means a vulnerability in software, typically in the operating system, that enables an attacker to compromise the system.
- **User(s)** means all County employees, council members, contractors, temporary help and agents or representatives acting on behalf of the County authorized to use Corporate Resources.

ROLES AND RESPONSIBILITIES:

Chief Administrative Officer is responsible for:

- Ensuring all directors are aware of this Policy and any subsequent revisions;
- Ensuring compliance with this Policy and any discipline deemed necessary.

Directors are responsible for:

- Ensuring all applicable managers/supervisors are aware of this Policy and any subsequent revisions;
- Ensuring compliance with this Policy and any disciplinary action deemed necessary.

Department Managers/Supervisors are responsible for:

- Ensuring Users in their respective work units are aware of this Policy and any related policies and procedures, as well as any subsequent revisions;
- Ensuring Users are trained on this Policy and any related policies and procedures, as well as any subsequent revisions, with respect to their specific job function;
- Ensuring Users comply with this Policy and follow any related policies and procedures, as well as any subsequent revisions.

Users are responsible for:

- Complying with this Policy and asking for clarification if any of the information is not understood from their immediate supervisor or Information Systems personnel;
- Advising Information Systems personnel of any loss or change of Corporate Resources or Users.
- Consult with Information Systems personnel if any doubts while using Corporate Resources

POLICY STATEMENT AND GUIDELINES:

All equipment and software programs, information and data installed or created on Corporate Electronic Devices belong to the County. This includes all programs, documents, spreadsheets, databases, and methods or techniques, developed using Corporate Resources while employed or retained by the County.

- Only software authorized by the County can be used in Corporate Electronic Devices;
- Installation of software, shall be done under the direction of Information Systems personnel;
- Configuration changes to hardware / software is prohibited;
- Corporate Electronic Devices should not leave the County property without authorized permission from the User's immediate County supervisor;
- Copying of Corporate Software is prohibited;
- Unauthorized attempts to bypass Data Protection Schemes or uncover Security Loopholes are prohibited;
- Knowingly or carelessly performing an act that will interfere with normal operation of the Corporate Electronic Devices or Corporate Networks is prohibited;
- Ordering or purchasing Corporate Electronic Devices or Corporate Software should not be done without consulting Information Systems Personnel;
  Corporate Electronic Devices which are no longer useful for business operations shall be returned to Information Systems personnel to be disposed of in accordance with Policy C21, Disposal of Assets Policy;

Network access ID passphrase (password)

- A network access ID passphrase must be confidential to each user and not be shared amongst users (excepting Information Systems personnel when required to upgrade systems, after which user should immediately change password);
- Users are accountable for all activities that occur under their network access ID;
- Users are responsible for immediately reporting any known or suspected compromise of their network access ID passphrase to Information Systems personnel;
- Passphrase should not be left where someone else can find them;
- Passphrase guidelines shall be adhered to.

Internet Use

- Internet access is provided to Users for research or system support purposes relevant to the County's business;
- Immediate supervisor, at their discretion, may choose to block internet access for specific Users;
- Corporately provided internet access and e-mail are Corporate Resources and are not to be used for purposes other than as allowed by this Policy or the Chief Administrative Officer's discretion. Occasional personal use of the internet and e-mail is authorized within reasonable limits as long as it does not interfere with or conflict with business use or performance of duties and should occur during non-working hours;
- Under no conditions is the internet to be used to access sites that are generally viewed as inappropriate;
- Users shall not knowingly:
  - Visit internet sites that contain obscene, pornographic, hateful, offensive or otherwise objectionable content;
  - Send or willingly receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person or group of persons.
- Users shall not, under any circumstances, use the internet for illegal purposes, to gather information to support illegal activities, or to make a personal profit;
- Downloading of non-executable files for business use is permitted. These would include reports, Adobe "PDF" files, spreadsheets, information flyers, etc. Users must ensure the source is reliable as a virus can be introduced to the Corporate Networks through spreadsheets and other documents. Users are encouraged to consult with Information Systems personnel if they have any doubts while using County Resources.

E-mail Use

- E-mail must not be used in a manner that is likely to cause Corporate Network congestion or significantly hamper the ability of others to access and use the system. Messages destined for "all Employees" should be sent via e-mail only when all Employees have a significant need to know the information and has been approved by the Chief Administrative Officer;

- E-mail records are like any other records that are created to correspond with the public and has the potential of information being released the same as any other document in the custody and control of the County. As a result, professional business practices shall be adhered to in respect to the creation and content of e-mail records. Retention of non-transitory email records shall be as defined in the Records and Information Management Policy P1 and the Corporate Records Structure;
- Use only business-like language and do not express personal opinions about individuals or situations, unless it is a specific task or requirement as part of your position or job function;
- If there is a need to include confidential information, mark your text as “confidential”.
- In general, do not include any text or information that would not be suitable or could not be “made public”;
- F.O.I.P. (Freedom of Information and Protection of Privacy) Signature is required when sending external e-mail:

  Your name
  Job Title, department (if not already stated in Job title)
  County of Grande Prairie
  Phone: (Your phone Number) Fax (Your Fax number)
  Website: www.countygp.ab.ca (Our Website address)
  Address: 10001 – 84 Avenue, Clairmont AB T8X 5B2
  This communication is intended for the use of the recipient to which it is addressed, and may contain confidential, personal, and or privilege information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error, or subsequent reply, should be deleted or destroyed

Management of Users

A network access ID is a unique personal identifier which is used as username for various services provided by the County.

- Request is placed by immediate supervisor, using the appropriate process;
- Termination or change is placed by immediate supervisor, using the appropriate process;
- Upon termination or transfer, all e-mail and folders are to be turned over to the immediate supervisor by Information Systems personnel;
- No information is to be deleted or otherwise made inaccessible or non-functional regardless of storage medium. All information remains the property of the County.

CONFIDENTIALITY:

The use and interpretation of all County Policies and schedules will comply with all aspects of the Freedom of Information and Protection of Privacy Act (FOIP). Any breaches of the FOIP Act will be subject to disciplinary action. Corporate Electronic Devices and Corporate Networks are the responsibility of the County Information Systems Personnel. The Information Systems personnel, therefore, reserves the right to inspect any and all files stored in private areas of the Corporate Networks in order to ensure compliance with this Policy.

All information accessed on County information systems is for internal use only unless disclosure of specific information to the public is permitted under the *Freedom of Information and Protection of Privacy Act* (F.O.I.P), *the Municipal Government Act* (MGA) or any other prevailing law or legislation.

RECORDS MANAGEMENT REQUIREMENTS:

All documentation will be filed in accordance with the Records and Information Management Policy and to comply with the *Municipal Government Act* (MGA), *Freedom of Information & Protection of Privacy Act* (FOIP) and any other applicable legislation, regulation, or act.

NON COMPLIANCE AND SANCTIONS:

Consequences of non-compliance with this Policy may result in the potential for legal challenges and/or penalties to the County, its elected officials and/or Employees.

Consequences to Employees for non-compliance of this Policy and its schedules shall include corrective action up to and including dismissal. According to Policy L7 – Personnel Policy (Corrective Action and Dismissal).

Consequences to all other Users for non-compliance of this Policy and its schedules shall include corrective action as per the CAO and/or Council.

Immediate supervisor is responsible for their respective Users' use of the internet and email. The immediate supervisor will co-ordinate with Human Resources any disciplinary action as a result of not complying with this Policy in accordance with, Policy L7 – Personnel Policy (Corrective Action and Dismissal)

The Chief Administrative Officer must approve any exceptions to the Policy in writing.

POLICY AUTHORITY:

The Chief Administrative Officer has the authority to amend the related Schedules of Policy R1 from time to time to keep current, enforceable and compliant with statutes and legislation in the Province of Alberta. Any changes that are made to Policy are to be approved by Council.