



POLICY NO. 3.14

September 8, 2015

TITLE: INTERNET AND EMAIL USE POLICY

POLICY STATEMENT:

Many of our employees have access to the internet as well as email capabilities. The County recognizes that these capabilities extend beyond the limitations of the workplace so this policy has been established regarding appropriate use of corporate internet and email systems.

The computer network is the property of Westlock County and is to be used for legitimate business purposes. Employees are provided access to the computer network to assist them in the performance of their jobs. All users have a responsibility to use Westlock County's computer resources and the internet in a professional, lawful, and ethical manner.

PURPOSE:

To clarify acceptable use of internet and email systems at Westlock County.

DEFINITIONS:

County means the municipal corporation of Westlock County.

Employee means an employee of Westlock County. This includes all employee groups listed in section 1 of Westlock's Personnel Policy, Policy No. 3.01.

IT Department means the company contracted by Westlock County to provide IT services.

User means someone given access to the County's electronic systems.

1. APPLICATION:

1.1. This policy applies to employees of the County as well as individuals and organizations that are given access to Westlock County's electronic systems.

2. GENERAL GUIDELINES ON INTERNET ACCOUNTS:

2.1. With respect to account setup and network administration, department managers and/or supervisors are responsible for identifying and recommending internet access levels for staff members in their department and forwarding that information to the IT Department.

2.2. All user names and passwords for County owned and operated devices must be supplied to the IT Department.

2.3. In the event that an employee loses, forgets, or believes that his/her password has become compromised, the employee must inform the IT Department immediately. The IT Department will then confirm the username, reset the password, and inform the employee of the changes made and the procedure for changing the password.

3. GENERAL GUIDELINES ON ACCEPTABLE INTERNET USE:

3.1. Employees may only use the County's internet system to complete their job duties during work hours. Permissible, acceptable and appropriate internet-related work activities include:

- a)** Researching, accumulating, and disseminating any information related to the accomplishment of the employee's assigned responsibilities, during work hours or overtime;
- b)** Collaboration and communicating with other employees, business partners, and customers, according to the individual's assigned job duties and responsibilities;
- c)** Conducting professional development activities, such as news groups, chat sessions, discussion groups, posting to bulletin boards, web seminars, as they relate to meeting the employee's job requirements.
 - i.** In instances where the personal opinions of the user are expressed, a disclaimer must be included asserting that such opinions are not necessarily those of the County.

3.2. Users may use the County's internet system for non-County related research, internet browsing and communication during breaks or non-working hours, provided that all aspects of this policy are adhered to.

4. GENERAL GUIDELINES ON UNACCEPTABLE INTERNET USE:

4.1. Internet use shall comply with all federal and provincial laws, and the County's other policies.

4.2. Inappropriate and unacceptable use includes, but is not limited to:

- a)** Copying, destroying or altering any data, documentation, or other information that belongs to the County or any other business entity without authorization;
- b)** Downloading unreasonably large files that may hinder network performance. All employees must use the internet in such a way that does not interfere with others' usage;
- c)** Engaging in online commercial activities, including offering services or products for sale or soliciting services or products from online providers;
- d)** Engaging in an activity that could compromise the security of the County's host servers or computers. Any and all passwords must not be disclosed to, or shared with others;
- e)** Engaging in any fundraising activity, endorsing any products or services, or participating in any political activity unless authorized to do so as part of completing one's assigned job duties and responsibilities;
- f)** Any individual internet usage that violates any of the policies and procedures of the accessed information's source network;
- g)** Accessing social media forums during work time, including but not limited to chat lines, Facebook, Twitter, MSN, and personal emails;
- h)** Allowing unauthorized parties or third parties to access the County's network and resources;
- i)** Usage for illegal or potentially illegal purposes;

- j) Accessing, downloading, or printing any content that exceeds the bounds of good taste and moral values such as pornography or anything that contravenes human rights legislation;
- k) Engaging in any other activity which would in any way bring discredit, disrepute, or litigation upon the County.

5. SECURITY:

5.1. Passwords must not be disclosed to others. Any and all internet accounts are to be accessed only by their assigned users.

5.2. Employees shall not attempt to obtain anyone else's account password.

5.3. Users are required to take all necessary precautions to prevent unauthorized access to internet services.

5.4. If a user has reason to believe his/her password has been compromised, the user must inform the IT Department immediately. Users are required to take all necessary precautions to prevent unauthorized access to County internet systems or County databases.

5.5. All internet users must comply with the following:

- a) Personal files or data downloaded from the internet may not be stored on the County's PC hard drives or network file servers.
- b) Video and sound files must not be downloaded from the internet unless their use has been authorized for the purposes of conducting appropriate business on behalf of the County.
- c) Users must refrain from any online practices or procedures that would expose the network resources to virus attacks, spyware, adware, malware, or hackers, or other such attacks.
- d) Users are responsible for familiarizing themselves with the procedures for downloading and protecting information in a secure manner, as well as for identifying and avoiding any online material deemed sensitive, private, and/or copyrighted.

- e) Users must conduct themselves in a professional manner at all times, especially while participating in collaborative activities, and must not disclose confidential County information or intellectual capital to unauthorized third parties.

6. ACCESS, MONITORING AND FILTERING:

6.1. Westlock County reserves the right to access, monitor, search, review and track any internet activity or other information that is stored on any County-issued computers, laptops or other devices.

6.2. Specifically, the County:

- a) Uses monitoring software for the purpose of enforcing acceptable use policies. Monitoring software blocks access to certain web sites which the County has deemed access to be a contravention of these policies;
- b) Uses filtering software to restrict access to websites the County has deemed unsuitable for business use. Where activities that conflict with the law or this policy are discovered, the County may retrieve internet usage records concerning those activities and used to document any wrongdoing;
- c) Reports any unlawful use to the Police and takes appropriate action up to and including termination if a violation of County policy is found;
- d) May review any activities using the County's hardware, software, equipment, and accounts to access the internet;
- e) Users' use of the County's internet resources implies the users consent to web monitoring for security purposes;

6.3. All users covered by this policy and related policies should have no expectation of privacy in their internet sessions while using the County's internet connection and/or using County-owned devices for accessing the internet.

7. EMAIL:

7.1. All employees who use the County's internet and email systems will be required to adhere to this policy when communicating with customers, clients, or any third party on behalf of the County.

7.2. Employees are expected to ensure that all communications employees send as agents of the County will be created using a consistently high level of professionalism and attention to detail.

7.3. Here are some general rules for emails:

- a)** Email communications must be polite, and begin with an appropriate greeting such as “Hello”, “Dear”, or “Good morning” and maintain an appropriate tone throughout an email;
- b)** Ensure that all messages use appropriate language;
- c)** Proofread your emails before sending them;
- d)** Ensure the accuracy of all factual information sent in email messages;
- e)** Use an appropriate and professional tone in the creation of email messages. It is often very difficult to determine when a person is using humour, sarcasm, or irony in an email. Please note that emails that include humour may be misunderstood and the effects could negatively impact our business;
- f)** At all times, please avoid sending messages using all capital letters as this is the written version of shouting, and may be taken as offensive;
- g)** Keep messages short, simple, clear and concise;
- h)** Emails should be sent only to those that require the information and you should refrain from sending unnecessary emails or mass emails;
- i)** Remember that when you send an email, it creates a permanent electronic record. Whatever is written in your email, including content and form will be on the record for a long time. Ensure that all messages sent are appropriate, and accurate in their content;
- j)** While it’s common to use short-hand for personal notes, it is unacceptable for business communication. Standard abbreviations such as “Mrs.”, “Mr.” will continue to be acceptable; however, the use of popular abbreviations such as LOL, ROFL, BRB, smiley faces, and emoticons is unacceptable, other than in intra-office communications;

- k) Ensure that all messages are sent only to the intended recipients. Avoid sending messages to parties that are not directly affected by the contents of the message;
- l) Ensure that all messages include a completed, appropriate and accurate subject heading in the subject line. Ensure that the subject line is relevant to the topic, clearly stating the purpose of the email;
- m) Avoid sending confidential information via email and ensure that all emails are appropriately encrypted;
- n) Avoid using email to send large attachments and only open attachments from known senders;
- o) Check your email frequently;
- p) Archive all messages that are older than 3 months. All County mailboxes have a space of 2GB. If employee mailboxes become full, it is responsibility of the employee reducing the space used.

7.4. Not adhering to any of the items in 7.3 may lead to disciplinary action as non-adherence could result in:

- a) Miscommunications;
- b) Inability to complete work tasks;
- c) The County being viewed by the public and other organizations as unprofessional;
- d) Damage to the County's reputation;
- e) Lost business;
- f) Failure in the County upholding its obligations under Alberta's *Freedom of Information and Protection of Privacy Act*.

8. SOCIAL NETWORKING SITES AND BLOGS:

8.1. The use of social networking sites, such as Facebook, Twitter, MySpace, and Friendster, and personal blogs is unacceptable during work time.

- 8.2.** The uses of social media sites and blogs for personal use are only permissible in accordance with 3.2.
- 8.3.** The use of social networking sites and blogs are subject to the same limitations and acceptable use rules provided for under this policy.
- 8.4.** The abuse of personal internet use on these sites using either County owned equipment or personal internet access devices during normal working hours will be subject to disciplinary action, up to and including termination of employment.
- 8.5.** The County reserves the right to deny access or usage of any of these social networking sites if it is deemed that employees are not abiding by this policy.

9. BUSINESS INFORMATION:

- 9.1.** The organization retains ownership rights to all forms of intellectual property created by employees using County equipment and County electronic systems, regardless of the time, intent or location of the intellectual property's creation.
- 9.2.** Employees shall not divulge, disclose, provide or disseminate business information to any third party not employed by the County at any time, unless prior authorization is obtained.
- 9.3.** Users must not use the County's business information for any purpose other than its reasonable use in the normal performance of employment duties for the County.

10. COUNTY OWNED PROPERTY:

- 10.1.** All County business is intended to be performed using County owned property, including, but not limited to, computers, telephones, smartphones, letterhead, notebooks, etc.
- 10.2.** All information contained in, created or transmitted by County owned property or County operated property is the property of Westlock County and not the property of the user.

11. EMPLOYEE-OWNED PROPERTY:

- 11.1.** Employees are prohibited from using personally owned equipment or property for the creation, transmission or storage of County business information, unless authorized to do so.
- 11.2.** In the event that an employee creates, stores or transmits County business information on personally owned property, such as on a laptop or a smartphone, the information will remain the express property of the County.

12. RETIREMENT, LAYOFF OR TERMINATION:

- 12.1.** Upon retirement, layoff, or termination of employment, employees must promptly return, without duplicating or summarizing, any and all material in their possession pertaining to the County's business including, but not limited to, all customer lists, physical property, documents, keys, electronic information storage media, manuals, letters, notes and reports.
- 12.2.** Upon conclusion of an employee's employment with the County, Human Resources will provide notification to the IT Department immediately to ensure the removal of the former employee's access to the County's email and internet resources. This is an important measure in protecting the safety and integrity of our resources.
- 12.3.** In the event that a device containing business information is password protected, the employee will be required to provide the correct username and password for the device.

13. COMPLIANCE:

- 13.1.** Employees will be expected to sign an Internet & Email Use agreement.
- 13.2.** Pursuant to Policy No. 3.01, section 18, violations of this policy may result in one or more of the following:
 - a)** Temporary or permanent revoking of access to the County's internet resources and/or other IT resources;
 - b)** Temporary or permanent revoking of County devices;

- c) Disciplinary action up to and including suspension or termination of employment;
- d) Legal action according to Provincial or Federal laws.

14. DISCLAIMER:

- 14.1. The County does not accept responsibility for any loss or damage suffered by employees as a result of employees using the County's internet connection for personal use.
- 14.2. The County is not responsible for the accuracy of information found on the internet. Users are responsible for any material that they access, download, or share through the internet.

15. CLIENT, VISITOR, AND EMPLOYEE PRIVACY:

- 15.1. Employees are strictly forbidden from posting sensitive, derogatory, malicious, inflammatory or personal information regarding our clients, visitors and employees on social networking sites and/or the internet in general during work time or personal time.
- 15.2. Employees are strictly prohibited from taking photographs of clients, visitors or employees on County premises for either personal or professional reasons, unless they have received prior authorization in writing to do so.
- 15.3. Employees are strictly prohibited from posting photographs of other employees, clients or visitors on the internet, unless authorized in writing to do so.

MOTION: _____

DATE: _____

Peter Kelly
Chief Administrative Officer