**ELECTRONIC ACCESS POLICY**

Subject: Electronic Devices, Internet & E-mail Use Ref: Administration Code: 12

Date Approved: June 27th, 2017 Motion No.: 303/27/06/17 Replaces: 047/08/02/11

The County of Northern Lights believes that operational efficiencies, including timely access to information, employee productivity, and customer service improvements, can be achieved through the proper use of tools such as the internet and electronic mail.

Electronic devices, e-mail and internet are valuable tools to assist users in performing the legitimate work of the County of Northern Lights. It is important that such "tools" be utilized in a professional and responsible manner. This Policy outlines the appropriate use of these 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 the County and its resources at risk.

The County of Northern Lights intends to minimize risks due to the potential for misuse and abuse of these technologies by setting out Guidelines governing staff access to the electronic mail and the internet.

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 County resources.

Chief Elected Official

Chief Administrative Officer

## PROCEDURE

## 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 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 Northern Lights 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 Administrative Department as per the County Organizational Chart, who have responsibility for Information Systems; or the Information Systems Support Contractor hired by the County – currently PCIT.
- **Security Loopholes** means a vulnerability in software, 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 RESPONSIBLITIES:

**Chief Administrative Officer** is responsible for:

- Ensuring all Directors/Managers are aware of this policy and any subsequent revisions;
- Ensuring compliance with this policy and any discipline deemed necessary.

**Directors/Managers** are responsible for:

- Ensuring all applicable supervisors are aware of this policy and any subsequent revisions;

- Ensuring compliance with this policy and any disciplinary action deemed necessary;
- Determining the need for and permitting an authorized user to access and use the Internet and/ or e-mail (internal and/ or external) through the County's computer systems provided such access is restricted to County business purposes only;
- Arranging for training for authorized users
- Denying, amending or revoking access by any authorized user and regarding any computer or group of computers;

**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.
- Consulting with Information Systems Personnel if any doubts while using Corporate Resources

**1. Access to and use of the Internet and Electronic Mail**

The County provides access to the Internet and electronic mail to its users who comply with this Internet Use Policy.
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;
- Copying of corporate software is prohibited;

- Unauthorized attempts to bypass Data Protection Schemes or uncover Security loopholes are prohibited (hacking);
- 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 shall not be done without consulting Information Systems Personnel and following all requirements in the County's Procurement of Goods and Services Policy.
- 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 the Disposal of Surplus Items Policy.
- Bring Your Own Device – BYOD – Procedure (Schedule "A") establishes the guidelines to use personally-owned mobile devices in the workplace.

**2. General Guidelines for Use of Electronic Mail and the Internet**

- 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.
- The internet is not only a resource, but a community inhabited by a wide range of users, therefore, extra care is required when distributing or accessing information.
- Virus checking practices remain in effect. Any file you execute or download or acquire from any remote source must be virus scanned on your local drive immediately. users should not assume that automatic virus checking will be performed during the actual download.
- Any viruses found must be reported immediately to the Information Systems Personnel. Anti-virus programs shall not be disabled by a user. Only business related documents may be downloaded directly to the network. Anything else (including but not limited to; personal documents, applications, utilities, video/ audio clips, screen savers, games and software) must not be downloaded.
- Apply sound judgment to the Internet sites you access since these are tracked and regularly monitored by the Information Systems Personnel. As part of the management of this system, the software keeps a log of what is accessed and by whom.
- Users are to refrain from disclosing their access codes/ passwords to anyone and will be responsible for any use of their accounts by others to whom access has been given. It is recommended that users change their passwords periodically to prevent unauthorized use of their accounts.
- Individuals are not to send personal e-mails from the County e-mail address.
- Many organizations on the internet have their own guidelines about what you may or may not do when you access the information on their computer systems. Please act responsibly when you access these systems. Make sure you understand and apply their guidelines for use.
- Each Internet user will respect other users in their use of all Internet services, and will

not inappropriately forward electronic messages received by them without the permission of the original author.

- Guidelines concerning Conflict of Interest and Confidentiality apply to all usage of the internet. Employees duties shall be conducted in such a manner that stakeholder confidence and trust in the integrity, objectivity, and professionalism of the County are preserved or enhanced.
- 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 acceptable 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.
- 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.

**3. Unacceptable Internet Use**

- 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.
    - Under any circumstances, use the internet for illegal purposes, to gather information to support illegal activities, or to make a personal profit.
    - Upload or download information or software in violation of copyright laws
    - Engage in any communication that is obscene, defamatory, offensive or in violation of County policies on harassment;

- The use of computing resources for electronic "snooping" i.e. to satisfy idle curiosity about the affairs of others, with no legitimate business reason for obtaining access to the files or communications of others is not acceptable.

- Sending, forwarding, redistributing or replying to "chain letters" or doing anything that results in County e-mail addresses receiving spam (i.e. junk mail) messages or solicitations.

- 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 users" should be sent via e-mail only when all Employees have a significant need to know the information.

- 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. (see attached "E-mail best practices")

- Retention of non-transitory email records shall be as described in the "Records Retention Bylaw".

- 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.P (Freedom of Information and Protection of Privacy) signature is required when sending external e-mail:
    - County logo
    - Your name
    - Job title, County of Northern Lights
    - Address, phone number, fax number
    - Website: www.countyofnorthernlights.com
    - *"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".*

**4. Monitoring and Consequences of Violations**

The County reserves the right to capture, access and review all information transmitted or received. Staff should have no expectations of privacy using our system. Authorized employees may need to view your email for legitimate business purposes, and others may inadvertently view your messages. Periodic monitoring will occur to ensure compliance with this policy. All system users are expected to exercise sound judgement.

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 which may include revocation of internet privileges, discipline, or where appropriate, termination of employment as per the Progressive Discipline Policy.

**5. Laptops, Tablets and Smart Phones – Corporate Electronic Devices**

- Laptops, tablets, smartphones and any other electronic devices used for the County of Northern Lights must adhere to the Electronic Access Policy.

- VPN access may be made available to office users that require network access outside the office. This request will be made to the Information Systems Personnel.

- Devices are kept on our persons, are removed from company locations on daily basis, and are in danger of being lost or stolen, therefore all County of Northern Lights Corporate Devices must be password protected.

- Never leave a portable laptop / tablet in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave it in plain sight. If you must leave our laptop/ tablet in a vehicle, the best place is in a locked trunk. If you don't have a trunk, cover it up and lock the doors.

- It is the responsibility of the County of Northern Lights users to ensure that their laptop / tablet or Smart phone is given the same consideration as a user's on-site computer. When connected to the County's network from inside / outside our office, it is the responsibility of the authorized user to adhere to this policy in its entirety and to ensure that family members, colleagues and the public do not gain access to the County network.

- Corporate Electronic Devices and Corporate Software are to be returned to the County of Northern Lights upon termination of employment with the County.

- Corporate Electronic Devices assigned to Elected Officials are provided under the County Remuneration Policy and may be made available to Elected Officials at the end of their term.

**6. Virtual Private Networking**

- Remote access to any County computer or hardware is prohibited unless authorized. Any employees or outside parties granted access to the County's computer systems are responsible to ensure that their remote access connection is given the same considerations as the local user's onsite connection to the County of Northern Lights network. Any violation of any of the County's policies will result in a loss of remote access privileges.

- Computers and / or computer systems remotely accessing the County of Northern Lights computers, computer systems or computer networks must have some type of up-to-date and functioning firewall software or firewall hardware in place and running.

- 
- to have VPN access must first be pre-approved by County Information Systems Personnel to ensure compliancy with County of Northern Lights security from viruses, SPAM and electronic attacks.

- Authorized users of VPN are responsible to ensure family members do not violate any County of Northern Lights policies, do not perform illegal activities, and do not use the access for outside business interests. Authorized users should ensure that VPN access is restricted and inaccessible to family members. The authorized user bears responsibility for the consequences should the VPN access be misused.

- All users of the County Corporate Electronic Devices or remote access are required to read and sign acknowledgement of this policy. Employees will be provided this policy at commencement of employment and will be provided with the required Corporate Electronic Devices and allowed access once the policy has been read and acknowledged.

# COUNTY OF NORTHERN LIGHTS
# ELECTRONIC ACCESS POLICY – BYOD PROCEDURES
# SCHEDULE "A"

## Purpose and Intent:

- Outline device options and terms and conditions, for allowing employees to use personally owned mobile devices in the workplace;
- Clarify the eligibility to obtain a corporate-issued mobile device or the exact limits regarding reimbursement for a personally-owned mobile device; and
- Outline supported device types, service levels, reimbursement, acceptable use and security requirements.

This procedure applies to all County employees as well as contractors, consultants and volunteers, including resident members of committees, authorized by the department they report to participate in the Bring Your Own Device (BYOD) program.

Authorized employees and external contractors are eligible to bring personally-owned mobile devices into the workplace to access their County email, calendar, contacts and other systems (see ***DEVICE OPTIONS AND EXPECTATIONS OF USE*** Page 4).

***RELATED POLICIES AND PROCEDURES***

BYOD participants are reminded that they are also subject to the following corporate policies and procedures:

- Electronic Access Policy;
- Social Media Policy;
- Freedom of Information and Protection of Privacy Act.

It is the responsibility of all BYOD program participants to read the policies and ask for clarification from their manager/supervisor of any information not understood.

## Definitions for the purposes of this procedure:

**"BRING YOUR OWN DEVICE" (BYOD)** means a program whereby employees, contractors, consultants, volunteers and members of committees utilize personally-owned mobile devices to access County systems such as email and networks.

**"BYOD User"**

**"Reimbursed BYOD User"** means an employee or external contractor who is a participant in the BYOD program who is required to carry a mobile device for business purposes and who is reimbursed by the County for personally-owned mobile device expenses.

**"Non-Reimbursed BYOD User"** means an employee or external contractor who chooses to utilize their personally-owned mobile device to access systems such as County email and County networks for occasional convenience use and who is not reimbursed by the County for personally-owned mobile device expenses.

**"Corporate-issued Mobile Device"** means a device owned by the County and issued to eligible employees or external contractors for the purpose of conducting County business.

**"Employee"** means all County staff.

**"External Contractor"** includes contractors, consultants, members of committees, and other volunteers acting on behalf of the County. While not considered employees, the above are expected to conduct themselves in accordance with established County policies, as amended from time to time.

**"Mobile Devices"** include cell phones, smartphones, tablets, iPod and laptops.

**"Mobile Device Management"** (MDM) means a software system that enables the County to manage mobile devices connected to the County's network. Functionality includes: provisioning, securing, monitoring, and the ability to remotely wipe devices.

**"Personally-owned Mobile Device"** means a device that is owned by an employee or external contractor and brought into the workplace to access systems such as County email and County networks.

**"Reimbursement"** means a monthly or bi-weekly (as required) non-taxable allowance paid to an employee or external contractor who is eligible for a corporate- issued mobile device but is using a personally-owned mobile device. Reimbursements are an automatic, recurring, fixed-amount payment toward monthly service provider fees deposited into employee payroll accounts monthly or bi-weekly (as required). Individuals who are not on the County's payroll system are reimbursed through invoice through accounts payable.

**"Virtual Private Network"** (VPN) means a computer or mobile device used to send and receive data across shared or public networks securely, as if by a private network, with all the functionality, security and policies of a private network.

## Procedure:

### *ADMINISTRATION*

Information Systems Personnel, as defined in the Electronic Access Policy, are responsible for management of the County's BYOD program. The Information Systems Manager or designate, has authority for allowing or disallowing devices into the BYOD program.
The County may alter the features of the BYOD service and/or cancel the program at any time, with appropriate communication to affected BYOD users.

### *CORPORATE RECORDS*

The County, through the Records Retention Bylaw is committed to establishing and maintaining record keeping practices that meet its legislative, accountability, and business obligations. Employees are responsible for complying with the Records Retention Bylaw and are encouraged to contact the County FOIPP Coordinator (Executive Assistant) prior to permanently deleting information related to County business.

### *ACCOUNTABILITY*

Directors are accountable for:

- ensuring all applicable Managers/Supervisors are aware of this procedure and of any subsequent revisions; and
- ensuring compliance with this procedure and any discipline deemed necessary

Managers and Supervisors are accountable for:

- ensuring BYOD users in their respective work units are aware of this procedure and any related policies and procedures, as well as any subsequent revisions;
- ensuring applicable BYOD users are trained on this procedure and any related policies and procedures, as well as any subsequent revisions, with respect to their specific job function;
- ensuring applicable BYOD users comply with this procedure and follow any related policies and procedures;
- authorizing "BYOD User Agreement" and "Reimbursement Request for BYOD Device" forms; and
- ensuring reimbursement does not continue if a reimbursed BYOD user no longer meets the reimbursement criteria (e.g. moves to another position in the County) by notifying the County's payroll office.

All BYOD program participants are accountable for:

- familiarizing themselves with this procedure and asking for clarification of any information not understood from their Department Manager or Supervisor; and
- advising the County of any loss or change of a personally-owned mobile device.

## *DEVICE OPTIONS AND EXPECTATIONS OF USE*

Eligible employees have two options for using mobile devices in the workplace:

- Corporate-Issued mobile device
- Bring Your Own Device (BYOD)

### Corporate-Issued Mobile Device (see procedure for complete information)

Employees required to carry a mobile device as part of their job duties may choose a Corporate issued mobile device, with costs covered by the County.

Eligibility for a Corporate-issued mobile device will be limited to employees:

- who spend the majority of their working time away from the office;
- whose job duties are in public safety, requiring immediate or emergency response, unless otherwise provided;
- whose job duties support 24x7 business infrastructure and systems; or
- who are required to respond promptly to urgent business related email or communication needs;
- Other reason – where a business case has been approved by the Director or Manager (further justification must be supplied).

Corporate-issued mobile devices are to be used primarily for County business use and related activities, with a limited amount of personal use.

Acceptable personal use is defined as reasonable and limited personal communication, and occasional use of apps, personal long distance calls are not included.

### Bring Your Own Device (BYOD)

Employees who choose to use a personally-owned mobile device in lieu of a Corporate-issued mobile device are eligible to receive reimbursement (Reimbursed BYOD Device User).

Employees will not be able to return their Corporate–issued mobile device if that device is still under active contract.

A Reimbursed BYOD User must agree to use their device primarily for County business use and related activities during regular business hours.

Business use is defined as activities that directly or indirectly support the business of the County (e.g. business-related email, calendars, contacts, documents, applications, phone calls, etc.).

All employees may choose to bring Personally-owned mobile devices into the workplace for occasional access to County systems such as Internet, email, calendar and contacts, with manager approval. In this case, no Reimbursement will be made, as this is deemed primarily "convenience use" (Non-Reimbursed BYOD User).

### *REIMBURSEMENT AND ADDITIONAL EXPENSES*

Reimbursements will be provided to reimbursed BYOD Users in the form of an automatic, recurring, non-taxable payment deposited into the Employee's payroll account on each regular pay period. Additional legitimate business-related mobile expenses may be reimbursed on an occasional basis if approved by the Director or Manager.

Rates are subject to change with proper notice (via email or staff Intranet) to the reimbursed BYOD user, rate changes will be applied automatically on the date agreed on, and reimbursed BYOD user has the choice to withdraw from the program.

The County is not responsible for charges resulting from personal voice or data overages, roaming, long distance charges, etc. that are not additional legitimate business-related expenses. Employees are advised that downloading and/or synchronizing corporate email, calendars and contacts will result in increased data volumes being sent to their devices. Employees are responsible for consulting with their wireless service provider to ensure that their data plan is sized accordingly.

Employees will not be compensated for purchasing, insuring, maintaining, servicing or replacing their personally-owned device.

### *APPROVAL PROCESS*

To request to be enrolled in the BYOD program, employees must complete a "BYOD Employee Agreement" form and submit it to their Supervisor for processing. This form must be signed by the employee and approved by their Director or Manager. Reimbursed BYOD Users must also complete a "Reimbursement Request for BYOD Device" form, which must be signed and approved by their Director or Manager.

### *ACCESS PROVIDED*

Approved BYOD users may synchronize their County email, calendar and contacts to/from their personally-owned mobile devices. Network access may be provided where technology permits. Access and security will be controlled via MDM, VPN or a similar access control system. This may require the installation of supporting software on the BYOD user's device.

***DEVICE SUPPORT***

Support of BYOD devices will be limited to device setup and "reasonable effort" resolution of connectivity issues and access to County related applications ("apps"). Any other support issues are the responsibility of the device owner, in consultation with their wireless service provider. Prior to obtaining support from a third-party service provider (e.g. when returning, repairing or upgrading their device), BYOD users must contact Information Systems personnel to disconnect their device and ensure that County related data is removed.
In all cases, when dealing with third-party service providers, device owners are responsible for ensuring that County-related data is not exposed.

***SECURITY***

Safeguarding the County's corporate data and the personal information of its staff and clients is of paramount importance. Any BYOD device being used to access/store corporate and personal data must comply with the security and authentication requirements of the County.

**Employees in the BYOD program must:**

- agree to safeguard the confidentiality of County-related data on their personally-owned mobile device at all times, and exercise caution when transferring sensitive business data to/from their device;

- agree to keep their personally-owned mobile device current with software updates as released by the manufacturer and/or wireless service provider;

- agree not to "jailbreak" or "root" their device (i.e. install software that allows the user to bypass standard built-in security features and controls). "Jail broken" personally owned mobile devices will be removed from the BYOD program immediately and may be remotely wiped (a remote wipe is immediate and irreversible. Any data on the mobile device that has not been backed-up or synchronized will be lost.);

- agree to allow Information Systems personnel to enforce standard security policies on their personally-owned mobile devices to safeguard the County's data and network;

- agree to being blocked from accessing certain websites or apps (e.g. those that are prohibited) while connected to the corporate network;

- agree to use only County configured and approved VPN client software or private cloud server for accessing the County's network;

- agree to immediately report any loss or theft of their personally-owned mobile device to their Director or Manager and to Information Systems personnel;

- agree to back-up the personal contents of their personally owned mobile device to their home computer or an authorized external data storage service to prevent data loss. The County is not responsible for any personal emails, appointments, contact names, images or other content lost due to the provision of this service;

- ensure that County email, files, etc. are not compromised if a device-owner shares their device with other individuals or family members. When in doubt, device-owners are advised not to share their device;

- agree that the County may remotely wipe/erase the entire contents of their personally-owned mobile device (i.e. reset it to factory default settings) in case of theft, loss, suspension or termination of employment, virus or malware, security breach (the County deems that information is being, or may be, at risk of misappropriation or other misuse), at the request of the device owner, for any other legitimate reason arising out of administrative, legal, or criminal proceedings, or if the County reasonably considers that such remote wipe/erase is necessary to ensure the confidentiality of County-related data;

- not allow third-party service providers control of or access to their device until it has been decommissioned and County data removed by Information Technology.

Information Systems personnel will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and dealt with in accordance with this procedure. The applicable device will be removed from the program immediately.

### *DEVICE & DATA OWNERSHIP*

Personally-owned mobile devices enrolled in the BYOD program remain the sole property of the owner. All County data, documents, information and work products created, received, transmitted, synchronized or downloaded by BYOD program devices remain the sole property of the County.

### *COUNTY ACCESS TO PERSONALLY-OWNED DEVICES*

The County will request and the owner of the personally-owned mobile device will provide access to personally-owned mobile devices as needed, to assist with the installation of software, for compliance verification or to respond to legitimate discovery requests arising out of administrative or legal proceedings (applicable only if the device-owner downloads County email/attachments/documents to their personal device). IT staff may also require access to the device when assisting device-owners with technical support issues.

While providing service, Information Systems personnel will make reasonable efforts to access only the parts of the personally-owned mobile device necessary to deliver support. However, should

Information Systems personnel view content on a user's device that is in their opinion criminal or illegal, it will be investigated in accordance with the County Electronic Access Policy.

Users may decline to provide access to their personally-owned mobile device by opting-out of the BYOD program.

### *DEVICE LOSS OR THEFT*

In the event of loss or theft of a BYOD device, employee shall notify the Information Systems personnel immediately. Information Systems personnel may remotely wipe the device to remove any corporate data. The County is not responsible for replacement costs related to loss or theft of personally-owned mobile devices.

### *REPLACING OR WITHDRAWING DEVICES*

Employee who wishes to replace their BYOD device, or who wishes to withdraw from the BYOD program, shall advise and consult with Information Systems personnel so that the device can be safely decommissioned from the County's system. It is the user's responsibility to ensure that all County data is wiped from a device prior to selling, trading, gifting, or discarding it and/or returning it to a third-party wireless provider.

### *EMPLOYEE DEPARTURE*

When any BYOD user discontinues employment with the County, or chooses to withdraw from the BYOD program, access to County systems will be terminated and the BYOD user shall remove all County-related data immediately from the personally-owned mobile device. If the BYOD user does not satisfy the County that all County-related data is removed from the personally-owned mobile device, the County may be remotely wiped from the personally-owned mobile device. It is the user's responsibility to ensure that the wipe was successful and that all County-related data is removed from any devices or external storage services to which County data may have been stored or replicated.

### *COMPLIANCE*

Any County employee who violates this procedure will be subject to appropriate disciplinary action, up to and including termination of employment. The County is authorized to immediately withdraw information systems access and initiate an investigation, in accordance with the Electronic Access Policy, should abuse of any aspect of this procedure be suspected.

The County is authorized to immediately withdraw the access of other authorized BYOD users should abuse of any aspect of this procedure be suspected.

### *APPENDICES:*

A - Form, Bring Your Own Device, Employee Agreement
B - Form, Reimbursement Request for BYOD Devices
C - Reimbursement Rate Schedule

Date:

# MEMO TO FILE

***RE: Payment to _____ for Personal Cell Phone Usage***

This letter is written as confirmation that the County of Northern Lights, the "County", and _____, a County employee, have agreed that the County will make a monthly payment to the employee for using his/her personal cellular phone to conduct County business.

This payment is for use only and does not make the County responsible for any loss or damages due to fire, theft, etc. as the cellular phone remains the employee's property. The employee has read and acknowledges the County of Northern Lights Electronic Access Policy and BYOD procedures.

The payment has been set at $50.00 per month until this agreement is amended or _____'s employment with the County is terminated.

Read and agreed to this _____ day of _____, 20_____.

_____ _____

Supervisor Employee:

Date:

To: Vicki Hudema
Accounts Payable Clerk

From: Josh Hunter
Manager of Finance

**REQUEST FOR CHEQUE TO BE ISSUED**

Please issue a cheque to:

Payment for: January – March _____ Phone Reimbursement

Code: 2-XX-XX-XX-217

Amount: $150.00

Due: March 31, _____

_____
Josh Hunter, CMA

Schedule "B"

County of Northern Lights

Electronic Access Policy

**Electronic Access Use Agreement**

I certify that I have read, understood and agree to the terms set forth in the County of Northern Lights Electronic Access Policy.

I further certify that I have received a copy of this policy.

I acknowledge that using the County`s systems is a privilege that may be revoked at the sole discretion of the County for any reason, and that it automatically terminates when I leave the employment of the County.

_____ _____

Signature Date

_____

Name (Please Print)

Schedule ``C``

County of Northern Lights

Electronic Access Policy

**Virtual Private Networking Use Agreement**

I certify that I have read, understand and agree to the terms set forth in the County of Northern Lights Electronic Access Policy, in particular, Clause 6 of the Electronic Access Policy which lays out guidelines and procedures for Virtual Private Networking.

I further certify that I have received a copy of this policy.

I acknowledge that using the County`s systems is a privilege that may be revoked at the sole discretion of the County for any reason, and that it automatically terminates when I leave the employment of the County.

_____ _____

Employee Signature Date

_____

Name (Please Print)

_____ _____

Manager Signature Date

_____

Name (Please Print)

Schedule ``D``

County of Northern Lights

Electronic Access Policy

**Laptop, Tablet and Smart Phone Agreement**

I certify that I have read, understand and agree to the terms set forth in the County of Northern Lights Electronic Access Policy, in particular, Clause 5 of the Electronic Access Policy which lays out the guidelines and procedures for Laptop, Tablet and Smart Phone.

I further certify that I have received a copy of this policy.

I acknowledge that using the County`s systems is a privilege that may be revoked at the sole discretion of the County for any reason, and that it automatically terminates when I leave the employment of the County.

_____ _____

Employee Signature Date

_____

Name (Please Print)

_____ _____

Manager Signature Date

_____

Name (Please Print)

County of Northern Lights

Electronic Access Policy

## Email Best Practices

Email has rapidly become the standard by which business communicates. This poses a number of significant communication challenges because of its text based nature. To obtain the most effectiveness from this resource, these best practices are provided and are expected to be utilized when using e-mail to communicate on behalf of the County of Northern Lights. All users should regularly self-evaluate their use of email to ensure they are using it in an optimally effective manner.

Email should adhere to the following basic principles:

1. Professionalism: using proper email language conveys a professional image.
2. Efficiency: emails that get to the point are much more effective than poorly worded emails.
3. Protection from liability: colleague awareness of email risks will protect the County from costly legal action.

- **Use the TO field for people who are expected to act on your message**
    - Send messages only to relevant people who must be involved in the specific communication. Avoid the temptation to over-distribute.
- **Use the CC field as an FYI only**
    - An individual identified in the CC (copy) field on an email should not be expected to take action as a result of this message.
- **Use the BCC (blind carbon copy) with caution**
    - Use the BCC field for sending an email to a large group of people.
    - Make sure when using BCC that your intentions are proper. To send BCC copies to others as a way of talking behind someone's back is inconsiderate.
- **Use the SUBJECT field**
    - Keep the Subject field relevant with a brief clear description of the message.
- **Use a salutation/greeting**
    - An email is a form of business communication and should present a professional image. Use of a courteous greeting at the beginning of the email for external communications is a must.
- **Be concise and to the point**
    - Long, rambling messages tend to be ignored and deleted. They also stand a greater chance of being misunderstood.
- **Use proper spelling, grammar and punctuation**

- Improper spelling, grammar and punctuation present a poor impression of the County. Emails with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. Use spell check.
- LOL, TTYL, etc are not proper grammar and should be limited to use in text messages and not at any time used in business emails.

- **Do not write in CAPITALS**
  - WRITING IN CAPITALS APPEARS AS IF YOU ARE SHOUTING.
- **Answer all questions, and pre-empt further questions**
  - If you do not read and answer all the questions in the original email, you will receive further emails regarding the unanswered questions, which will not only waste your time and other's time, but also creates considerable frustration.
- **Answer swiftly**
  - As a general rule, an email should be replied to within 24 hours and preferably within the same working day. Even if you do not have the time to compose a full response, a quick message to acknowledge receipt and set expectations for a more detailed response is always welcome.
- **Read the email before you send it**
  - A lot of people don't bother to read an email before they send it out, as can be seen from the many spelling and grammar mistakes contained in emails. Apart from this, reading your email through the eyes of the recipient will help you send a more effective message and avoid misunderstandings.
- **Watch your tone**
  - The written form lacks the subtle nuances of in-person conversation. Avoid humour, sarcasm and irony unless you are absolutely certain the recipient will understand your meaning.
  - When there is a misunderstanding by email, don't hesitate to pick up the telephone to work things out.
- **Avoid using the confirm receipt feature unless it is absolutely necessary**
  - Not all systems support it, and not all recipients appreciate these notifications.
- **Forwarding and Redirecting**
  - A message that has been forwarded or re-directed a number of times will likely have sections by different authors. Be careful that the entire message you are forwarding is "appropriate" for all the new receivers.
  - Keep in mind that messages that you send to others can be forwarded. If you feel your message should not be forwarded, specify that in the email.
- **Do not "reply all"**
  - Make sure if you are replying to all, that everyone in the email actually requires, or should receive a reply.
- **Don't send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks**
  - Sending, or even forwarding just one defamatory or offensive remark in an email could result in you and the County facing a lawsuit.

- **Security**
  - Always assume anything you send or receive via email is not secure. Ask yourself would this email cause you or the County concerns if it were to be posted on the front page of the paper?
  - Do not open a message that seems suspect
  - Do not click on links if you are not sure of their source. If you are not expecting a link or an attachment from a known email contact, there is no harm in calling to determine if it is in fact from them.
  - Never disclose anything confidential such as your password, or credit card number in an email message.
  - If you suspect your email has been compromised in any way, contact Information Systems Personnel immediately.
- **Manage your email effectively**
  - Try to schedule daily visits to your inbox. Scheduling them, rather than checking on a reactive basis, will ensure that you use your time more efficiently.
  - After taking any action needed, either file the message in an appropriate folder or delete it. Do not maintain a long list of messages in your inbox.
  - Remember to regularly delete your sent messages, and deleted messages.

**Remember if you are sending an email on behalf of the County you are expected to treat it the same as any other business correspondence.**