



Haines Borough
Administrative Policy
Information Technology Resources Policy

Applicable to: *All Users of Borough Information Technology Resources excluding the library's public access system, which is governed by separate library policy*

Effective: *June 1, 2015*

Purpose

The Haines Borough ("Borough") provides users with a variety of Information Technology Resources ("Resources") that represent a significant investment on the part of the Borough. Use of these resources is regulated to ensure proper use and compliance with state and federal laws. Improper use can incur significant costs to the Borough through internet usage fees and virus/malware remediation.

Borough Resources include but are not limited to desktop computers, laptop computers, mobile devices, telephones, printers, fax/modems, application software, data files, email addresses, and access to local and wide area networks including the Internet. Violation of this policy and/or procedures may result in loss of use privileges and/or in disciplinary action, including suspension, demotion, or dismissal in accordance with borough code and the current Collective Bargaining Agreement.

Acknowledgement

All users of Borough Resources are required to read and acknowledge this policy. Please read this document carefully and keep it for reference. Sign the *Policy Acknowledgement Form* and return it to your supervisor or the Borough clerk. By signing your name on the Form and using the Borough's Resources, you are acknowledging that you have read, understand, and agree to this policy.

Contents

The following are included in this policy document:

- I. General Computer/Electronics Use
- II. Internet Use
- III. Electronic Mail (Email)
- IV. Social Networking
- V. Mobile Devices
- VI. Policy Acknowledgement Form

I. GENERAL COMPUTER / ELECTRONICS USE

DISCUSSION

The use of the Borough's Resources is primarily for the purpose of carrying out a user's Borough responsibilities. All electronic files, communications systems and all information transmitted, received or stored in these systems are Borough property. The Borough reserves the rights to observe, retrieve, print and read any communication, file, or other use of the system at any time, with or without a user's advance notice or consent. Such monitoring may include printing and reading all files, emails or other documents entering, leaving, or stored in Borough computer systems. Such access may occur during or after working hours by the Borough Manager or designee, or the employee's department manager. Accordingly, users should have no expectation of privacy in connection with the use, transmission, receipt, or storage of information in Borough computer and electronic equipment. Even when a file or communication is erased or deleted it may still be possible to recreate the communication; therefore, ultimate privacy of files and communications cannot be guaranteed to anyone. The Borough reserves the right to inspect any and all files in all areas, including individual hard drives and media in order to assure compliance with this policy.

Personal use of the Borough's Resources is similar to the use of an office telephone for personal calls. Incidental personal use is allowed as long as it does not interfere with the business of, or reflect poorly

on the Borough. The contents of all email messages and material stored on desktop computers must be in keeping with the standards of conduct appropriate to the workplace and to this policy and guidelines established herein.

POLICY

- A. **Use of Resources.** The Borough's Resources shall not be used during or outside of the user's work hours for other than Borough activities or incidental personal use (defined below). The Borough's systems shall not be used to gain unauthorized access to remote systems. Any willful act or omission that could cause either a general loss of service or interference with the work of another will be subject to disciplinary action. Users are prohibited from using the Borough's Resources, including printers, for any non-Borough related commercial or political activity.

Incidental Personal Use: Occasional personal use of minimal time and duration, which results in no additional cost to the Borough. Examples include use of email to send personal messages to friends or family, checking the ferry schedule for personal travel, or scanning/copying a personal document. If personal use adversely affects or conflicts with Borough operations, the use is no longer incidental and the user is expected to cease those activities. All direct costs (for example, printer or copier paper and other supplies) attributed to personal incidental use must be assumed by the user.

- B. **Copyrights, licensing, and data handling requirements.** Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format without the express written permission of the owner or the proper licensor, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarize, or illegally using unlicensed products. Federal and state laws regarding access to public information apply to data files maintained on computer and electronic systems just as they do to other media.
- C. **Offensive material.** Users shall not deliberately print, archive, store, distribute, edit, record or otherwise display any sexually explicit image, file or document that may reasonably be considered offensive or disruptive to anyone on any Borough system. Offensive material would include, but is not limited to: sexual comments or images, racial slurs, or other comments that would reasonably offend someone on the basis of his or her age, sex, race, religion, national origin, or disability.
1. Users shall take immediate action to delete any inadvertently accessed prohibited material.
 2. The user shall immediately notify the System Administrator or Borough Clerk and request assistance with the deletion process.
- D. **System and Data Security.**
1. **Security systems.** The Borough has installed security systems to assure the safety and security of the Borough's networks. No user shall attempt to disable, defeat or circumvent any security feature. Any deliberate action to damage or disrupt the system, alter its normal performance or cause it to malfunction is prohibited.
 2. **Non-Borough hardware.** Connecting any non-Borough issued computing hardware to the network is strictly prohibited without prior approval. This includes, but is not limited to: personal laptops; devices hosting any form of virtual ware or operating system simulation, hosted personal mobile computing, or storage appliances. Third-party hardware used by contract staff for Borough business purposes may be granted access to the staff and/or the guest networks but must receive prior approval from the Borough Manager in consultation with the System Administrator.
 3. **Viruses, etc.** Knowingly introducing computer "viruses" or other disruptive/destructive programs into the Borough network is prohibited. All software, files, programs or data which are copied on to Borough computers, must be checked for viruses prior to use.
 4. **Unattended computers.** To prevent an unauthorized person from browsing through files, sending messages or entering unacceptable Internet sites, the following procedures should be followed:

- Short periods of time: Lock the computer when absent or away from desk for short periods of time. Press the Windows and L keys simultaneously to lock a computer.
 - Overnight or longer periods of time: Computers should be shut down unless remote desktop access has been authorized.
5. **Passwords.** The use of passwords is important for the security of the work environment.
 - a. Change all passwords regularly and at a minimum of every six months.
 - b. Passwords are required to be at least 8 characters long and contain both letters and numbers or symbols. Avoid passwords that are family members' names, the favorite pet's name or a dictionary word. These types of passwords can be easily guessed.
 - c. Network login passwords should not be shared with others unless required by a supervisor or IT support staff.
 6. **Access to data.** It is prohibited to restrict access to material or other communications by using passwords or other methods (outside of Windows login) that are inaccessible to an employee's supervisor or the Borough Manager.
 7. **Encryption of Data / Data Handling.** Certain types of information are subject to additional handling requirements. Your supervisor will provide specific rules for how to properly identify, store and transmit such data.

II. INTERNET USE

DISCUSSION

The Internet is to be used to further the Borough's mission, to provide effective service of the highest quality to the Borough's customers and staff, and to support other direct job-related purposes. The various modes of Internet/Intranet access are Borough resources and are provided as business tools to employees, elected officials, and other users who may use them for research, professional development, and borough work-related communications.

All Borough policies and procedures apply to users' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, Borough information dissemination, standards of conduct, misuse of Borough resources, anti-harassment, and information and data security.

The Copyright Act and the Electronic Communication Privacy Act of 1986, as well as certain Alaska Statutes, apply to various aspects of Borough internet usage.

The capacity of the Borough's Internet services is limited and is directly affected by the type of use. Improper use can lead to increased costs and negatively impact simultaneous users. In addition, there are serious implications surrounding the issues of ownership, privacy, and security regarding Internet usage. Consequently, the Internet Use Policy is established to ensure that Resources remain available for Borough business and to protect the Borough and its employees and elected officials from violating Federal law or State statute.

POLICY

A. **Acceptable Internet Use.**

1. Conformance with use of the Borough's Internet services, as outlined in this policy statement, is required. If the Internet Use Policy is violated, access to Internet services may be suspended. Disciplinary action, per Borough policy, may be appropriate in some cases. If laws are broken, criminal or civil action may be taken.
2. Each employee, elected/appointed official, or other user using the Borough's Internet access shall identify himself or herself honestly, accurately and completely when setting up accounts on outside computer systems. Participating in chats or newsgroups as a representative of the Borough should only be undertaken with approval from the employee's supervisor or Borough Manager.

3. While accessing the Internet, employees and elected/appointed officials represent the Borough. As with any other communication medium, users should conduct themselves appropriately.
4. **Downloading.** Department managers in conjunction with the System Administrator may authorize users with Internet access to download software that has direct business use. It must be properly licensed and registered and used only under the terms of its license. Any software or files downloaded via the Internet into the Borough's network become the property of the Borough.
5. **Cloud Storage.** Any use of cloud storage for Borough information must be authorized by the employee's supervisor or the Manager. In general, Cloud storage should only be used for information that is readily available and approved for distribution to the general public.

B. **Unacceptable Internet Use**

1. The Borough's Internet service and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, or other local jurisdiction in any material way. Use of the Borough's resources for illegal activity may be grounds for immediate dismissal, and the Borough will cooperate with any legitimate law enforcement inquiry.
2. No user may use the Borough's Internet access to knowingly disable or overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user.
3. Deliberate access to or distribution of material that can be construed as sexually explicit or otherwise offensive is expressly prohibited. If a user finds they connected incidentally to a site that contains this material, they must disconnect from that site immediately.
4. **Viruses, spy bots, and other malicious bugs.** No user may use the Internet to deliberately propagate any virus or other destructive program. All software, files, programs or data that are copied from the Internet to a Borough computer must be checked for viruses prior to use.

C. **Personal Internet Use.**

1. Users may utilize their Internet access for non-business research or browsing during mealtime or other breaks, or outside work hours, provided that all other usage requirements are adhered to.
2. Users with Internet access may not use Borough Internet facilities to download entertainment software or games, or to play games against opponents over the Internet. This includes personal portable devices such as MP3 players and smart-phones.
3. Use of Internet-delivered streaming media such as radio broadcasts, movie trailers, or music service for entertainment purposes is prohibited.
4. Using the Internet for personal shopping is prohibited (including online bidding and auction sites).

- D. **Monitoring.** No user should have any expectation of privacy as to his or her Internet usage. The Borough Manager, department managers, or other personnel designated by the Borough Manager may review Internet activity and analyze usage patterns, and they may utilize this data to assure that Borough Internet resource usage conforms to this policy and are devoted to maintaining the highest levels of productivity.

III. ELECTRONIC MAIL (EMAIL)

DISCUSSION

Specific Federal and State laws regarding access to public information apply to data files maintained on computer systems just as they do to other media. Therefore, electronic communications may be subject to public records requests and could become public information. Additionally, from a legal point of view,

email messages are discoverable in litigation to the same extent as any other record maintained by the Borough.

Other laws, including the Copyright Act and the Electronics Communications Privacy Act of 1986, as well as certain Alaska Statutes, can also apply to various aspects of email usage.

The capacity of the Borough's network to store information can be limited. In addition, there are serious implications surrounding the issue of ownership, privacy and security regarding email usage.

Consequently, the Electronic Mail Use Policy is established to ensure that Borough network resources remain available for Borough business and to protect the Borough and its employees and elected officials from violating Federal law or State statute.

POLICY

- A. **Acceptable Email Use.** The Borough email system is provided to facilitate conducting the business of the Borough. Conformance with acceptable use, as outlined in this policy statement, is required. If the Email policy is violated, disciplinary action per Borough policy may be appropriate.
- B. **Unacceptable Email Use.**
 1. Fundraising, political campaign or ballot proposition activities or public relations activities not specifically related to Borough government activities.
 2. Non-borough related commercial business or private employment.
 3. Using Borough email mailing lists for other than Borough business.
 4. Gambling.
 5. Transmission of confidential information to unauthorized person or organizations.
 6. Any use related to conduct that is prohibited by federal, state, or local law, rule or policy.
- C. **Security.**
 1. Standard Internet email is not a secure communication medium. This should be kept in mind when sending any message that is of a confidential manner. You should assume that people other than the recipient would be able to read your email message. Confidential information, including sensitive passwords and account numbers, should **never** be sent either in the body of an email message or in a non-secure attachment.
 2. Email messages received should not be altered without the sender's permission; nor should email be altered and forwarded to another user and/or unauthorized attachments be placed on another person's email message.
 3. For security and public records reasons, it is not permitted to install Borough email accounts on personal devices, such as computers, phones, and tablets. Access to email from non-Borough devices is restricted to webmail through an Internet browser at the following address: <https://mail.haines.ak.us/owa>. A borough employee or elected official believing they require mobile access should submit a request to the borough manager for a Borough device. The request should outline sufficient justification and budgetary resources.
- D. **Email Management.** Message retention fills up large amounts of storage space on the network server, and can also slow down performance. In addition, because email messages can contain confidential information, it is desirable to limit the number, distribution and availability of such messages. Therefore, the following shall apply:
 1. Email messages created or transmitted via the Borough email system may be considered public records and should be managed accordingly. (See Attachment A - *Types of Email Messages and when an Email is a Public Record*)
 2. Deletion by users: As a general rule, if a message does not require specific action or response on your part, you should delete it promptly after reading it. If the content of the message needs to be saved for longer than a week, it should be placed either within a special folder in your email program or printed out and saved in the appropriate file. Please review

your messages each week and delete those that are not needed or otherwise archive those you wish to save.

3. Notwithstanding the above, if the email message has any lasting administrative, legal or historical value, or if it is evidence in a pending or probable lawsuit, remove it from your general "in" or "sent items" folder and preserve it in an appropriate location on your system; either within a special folder in your email program or by exporting it to your local or network directory file system as a pdf or text file.
 4. If the content of an email message is related to actual or pending litigation or a government investigation, it shall not be destroyed. This restriction begins from the moment at which any user *gains knowledge that litigation or a government investigation is imminently foreseeable* (even though the lawsuit or investigation has not yet officially commenced) and continues until removed by the Borough Manager as advised by the Borough Attorney. The term "imminently foreseeable" is defined as the point in time at which a Borough user initially gains knowledge that any particular record or document may be or will be relevant to an actual or possible lawsuit or government investigation. Users who violate this policy are subject to disciplinary action and/or judicial penalties imposed by courts of law.
 5. Unwanted email or Spam. Employees, contractors and other users of the Haines Borough network must not deliberately open and/or forward malicious emails or emails sent from unknown sources. This would include the downloading of attachments sent with that type of email. Rather than letting curiosity take over, obvious junk mail and questionable emails should be deleted without opening or if uncertain, the user should contact the System Administrator or Borough Clerk. Users should not attempt to remove themselves from a spam mailing list by replying to the message. Any kind of response can verify to the sender that the user's email address is valid. Note: spam has increased to the point that it consumes over 80% of all email traffic on the Internet.
- E. **Email Structure.** Email should be as professional as any other official communication. (See Attachment B – *Email Etiquette*)
1. Subject Lines: Email should be clearly labeled via the subject line, being as descriptive as possible (i.e., "Quarterly Financial Report" not "Report", or "XYZ Committee Minutes" not "Minutes").
 2. Subject Matter: There should only be one subject matter per email, if possible.
 3. Carbon Copies: Carbon copies (cc) are public records and fully subject to disclosure.
 4. Blind Copies: Blind copying email (bc or bcc) is discouraged. Inadvertent blind copies cannot be deleted or unsent. A blind copy is a public record and fully subject to disclosure.
 5. Content: The content of every email message should be constructed with the same care as if it were a paper letter or memorandum. Messages should not involve or contain content that may be reasonably considered offensive or disruptive to any employee or elected official. Remarks of a derogatory nature are strictly prohibited.
 6. Signature: Users are required to properly identify their position with the Borough through the use of an email signature. Signatures should also include notification that all Borough correspondence is subject to public disclosure laws. Care should be taken to include this signature at least once in any email thread.
- F. **Personal Use.** Personal use of email is similar to the use of the office telephone for personal calls. Incidental personal use is allowed as long as it does not interfere with the business of, or reflect poorly on, the Borough. The contents of all such email messages must be in keeping with the standards of conduct appropriate to the workplace and to this policy and guidelines established herein. When using a Borough email account for personal use, it should be clear the communication does not represent the Haines Borough.

G. Monitoring.

1. The Borough owns all network facilities, computer systems and email accounts and has the express right to monitor and audit all computer files and network traffic on the network or individual hard drives.
2. All email (Borough and Internet) may be monitored, at any time, by the Borough Manager, the employee's department manager or other individual designated by the Borough Manager. Such monitoring may include printing and reading any email entering, leaving or stored in Borough computer systems. No user, therefore, should have any expectation of privacy with respect to email message sent, stored or received.

IV. SOCIAL MEDIA AND INTERNET PRESENCE

DISCUSSION

It is the intent of the Borough to represent itself appropriately, consistently and positively on the Internet. Collaborative technologies are fundamentally changing how information is provided, received and how the Borough may engage its citizens and reach out to visitors. This policy applies to any existing or proposed social media web sites and online community accounts that may be created by Borough departments. It also provides guidelines and standards for individuals regarding the use of social media for communication with citizens, colleagues and the world at large. No user may bring the Haines Borough Administration into disrepute on any website.

"Social Media Sites" refers to websites that facilitate user participation, networking and collaboration through the submission of user generated content.

While the Borough encourages its employees and elected officials to enjoy and make good use of their off-duty time, certain activities on the part of users may become a concern if they have the effect of impairing the work of other users; harassing, demeaning, or creating a hostile working environment for any employee; disrupting the smooth and orderly flow of work within the office; or harming the goodwill and reputation of the Borough among its customers or in the community at large. In the area of social media (print, broadcast, digital, and online services such as Facebook, LinkedIn, MySpace, Plaxo, and Twitter, among others), employees and elected officials may personally use such media in any way they choose as long as such use does not produce the adverse consequences noted above, both on and off duty.

POLICY

- A. **Required Work-Related Use, as applicable.** This includes content on Borough web sites and use of social media that may be sanctioned as part of user's job function (e.g. when an employee, as part of their job responsibilities, posts on behalf of the Borough on a Borough Facebook account).
 1. Any social media sites used by a Borough department to provide information must first be authorized by the Borough Manager and established in the name of the Haines Borough.
 2. Any information posted to a Borough social media site must be authorized by the employee's supervisor or Borough Manager in accordance with this policy and the purpose of the site as initially authorized by the Borough.
 3. Only authorized users may post information on Borough social media sites.
 4. Any authorized poster must monitor the social media site to ensure compliance with this policy and all other applicable state policies.
 5. Any authorized poster and the supervisor of that Borough social media site must remove any scandalous, libelous, defamatory, pornographic, etc. material that is posted.
 6. A process will be developed and instituted to save and retain all postings, outgoing and incoming, as all posted material is a public record.

7. All material and links published on the Borough's Internet websites or Intranet should be appropriate to the work environment. Such material can be posted only by those given the authority to do so by the Borough Manager or designee.
- B. **Personal use at work.** Due to the risk of Borough information being shared inadvertently (through the use of tracking by social media sites), personal use of social media while at work using Borough technology resources is prohibited. This includes personal use of social media while at work by an employee or elected official (e.g. logging onto Facebook and providing personal updates to a Facebook page or Twitter account during work hours using their own or the Borough's information technology resources, when such activity is outside of the employee's official job function).
- C. **Personal use outside of work.** This includes use of social media by an employee or elected official in his or her personal capacity outside of work.
 1. Users are prohibited from posting official agency information on personal media sites.
 2. Personal use should not be attributable to the Borough or the employee's/official's Borough job function.

V. MOBILE DEVICES

DISCUSSION

By using a mobile device provided by the Haines Borough, an employee or elected official implicitly agrees to the requirements and terms set forth by this policy. Abuse of this policy could result in loss of Borough device privileges and other disciplinary actions. Certain positions have been determined to benefit from assignment of a Borough mobile device and have been assigned one or more. For the procedure to request a device, see III. Electronic Mail (Email), C. Security, item 3.

POLICY

A. Usage.

1. **Limits.** It is the Borough's responsibility to communicate the allotment of minutes, data and messaging available to users within a specific timeframe when applicable. This information will be provided when the device is provisioned and prior to any change in plan allotment. It is the user's responsibility to track usage of these features and report to their supervisor or the Manager if limits are likely to be exceeded. The employee's supervisor and the Borough's technical staff will review plan options to ensure the user has adequate allotment while providing the best value option for the Borough. It is the responsibility of the user to ensure that allotted minutes, data and messaging are kept within the plan allotment unless there is prior approval from their supervisor and the cause is related to Borough business that could not be conducted through other means.
2. **International Use.** Current phone plans do not include international service. To avoid costly data charges, cellular data should be turned off prior to travel outside the US. Similarly, calls and messaging should be kept to a minimum. If the user will be outside the US for an extended period or if their duties require additional services, they should be added to the plan prior to departure. The user's department is responsible for all work-related international charges and the user is responsible for all personal charges.
3. Users should be aware that Borough supplied mobile phones are an extension of the Borough's network. As such, the Borough's Computer, Internet and Email use policies apply to users of Borough issued mobile phones.
4. The mobile phone user acknowledges their responsibility to follow all State, Local and Federal laws and Borough policies in effect regarding use. While traveling, it is the user's responsibility to know and adhere to the laws in effect in the areas of travel. Fines and charges related to the illegal use of Borough supplied equipment will be the responsibility of the user.

5. To protect private information on the device (data, contact information, emails, etc.) an access password must be set by the user when the device is provisioned. If the device is lost or stolen, a remote command to erase it will be initiated. This includes all data on the device, so important items should be stored in more permanent locations. If the device is found, the erase command can be removed if the device has not yet connected via cellular or wireless networks. As this device also allows an user to conduct Borough business discussions outside of the office, it is the user's responsibility to conduct private or sensitive Borough related business conversations where they are not likely to be overheard or recorded.
6. Pictures, Video, Audio and Data captured by or stored on issued devices is considered property of the Borough and should only be distributed, shared or posted in a manner in which the user is authorized and in ways that are consistent with Borough policies and mission. Borough mobile device data is subject to policies concerning classification, handling and encryption requirements and may be obtained to fulfill public records requests. Users are responsible for the proper handling of device data.
7. Borough devices are issued for work-related activities. While it is understood that occasional personal calls of short duration may be necessary when no other immediate means of communication is available, personal calls, incoming and outgoing, must be kept to a minimum and must be incidental to business use. Users should use good judgment when making personal calls and should recognize that detailed phone call billing statements and records are subject to public records requests.
8. Connecting a Borough issued device to public and unknown Wi-Fi networks can expose the device to threats, and only trusted networks should be utilized.
9. **Emails.** All emails originating from the device must be through a Borough email account.
10. **Text messages.** Text message is considered a public record. Text messaging should be limited due to the difficulty of storing the messages off of the phone.

B. Personal email and personal accounts

Accessing personal email and personal accounts on social media networks is prohibited on Borough distributed devices. Social media use is only permitted for Borough accounts and only for users who are authorized social media representatives for the Borough.

C. Safety

It is potentially hazardous to talk on a cellular telephone while operating a motor vehicle. To minimize the risk of accidents, users should not use cellular telephones while operating Borough vehicles. Every effort should be made to pull to the side of the road to a safe location prior to answering or initiating cell phone calls.

D. Smartphone Apps

The Borough will maintain a list of approved apps (specifying Free or Paid versions) and provide a mechanism to request approval of additional apps. If an user's supervisor or the Manager decides a certain app is required to fulfil the duties of a position, a request to purchase the app can be submitted. Any free app on the approved list can be installed by the user.

Some apps may have features that could cause the Borough to incur additional charges, such as data use, text messaging or in-app purchases that are charged to the account holder.

E. Additional Equipment

With the assignment of a portable device the Borough will provide a wall charger and a case/holder. Additional equipment such as a car charger, or a hands free system may also be supplied as deemed appropriate by the employee's supervisor or the Manager.

Personal hands free Bluetooth devices and headphones can be used with Borough supplied devices.

F. Device Management

Various software is used to manage and secure mobile devices provided by the Borough. This may include software that tracks device location and can lock or erase data if warranted. Any attempt to circumvent or disable device management features or software is a violation of this policy.

It is the user's responsibility to notify Borough technical staff if they have reason to believe security of their Borough device has been breached. The Borough technical staff may also detect that an employee's device has been compromised and request that the device be powered down and turned in immediately.

G. Loss, Theft and Damage

In case of loss or theft of a device, a user must contact a supervisor or the Borough's main contact for the mobile account at the soonest reasonable time, and law enforcement if it is warranted by the situation. Each user is accountable for assigned devices and will be charged for lost equipment including chargers and other accessories.

Additionally, a user's supervisor or the Manager should be notified in the event that a device is damaged or the battery will no longer charge.

H. Monitoring. All uses of these devices are subject to Borough-sanctioned monitoring.



David Sosa
Borough Manager

1 June 2015

Signature Date

Policy Acknowledgement Form

I have read, and am aware of, the requirements, obligations and responsibilities outlined in the Haines Borough *Information Technology Policy* (version 04-2015). I have been given a copy and advised to retain for reference.

I agree to abide by this policy and understand that apparent breaches will be investigated by the Borough Manager and, if confirmed, may result in disciplinary action, up to and including dismissal. Any violation of local, state, or Federal laws may carry the additional consequence of prosecution under the law - where judicial action may result in one or more of the following: specific fines, imprisonment, litigation costs, or payment of damages.

I am aware that a copy of this signed acknowledgement will be placed in my personnel file.

Name: _____

Position: _____

Department: _____

Signature: _____

Date: _____

Attachment A

Types of Email Messages and when an Email is a Public Record

Types of Email Messages

Email messages come in many forms. Some messages are clearly Borough business-related while others are of a personal nature and still others come as unsolicited advertisements (Spam). Other messages are meant to inform and no reply is needed (temporary or transitory messages) and finally there are messages that are meant to solicit a reply. Below are examples of the various types of email messages:

- 1) **Personal email** can be defined as a personal exchange not covered by the Borough records retention schedule. This type of email should be extremely limited in use and deleted after it is read.

Example:

To: Chris From: Marge Subject: Lunch I'll take you to lunch for your birthday. Let's meet at noon. Marge
--

Other examples of personal emails include:

- Lunch plans
- Jokes
- Chain letters
- Messages to family and friends
- Attached files such as photographs

Note: Minimize your use of the Borough's email system for personal purposes. Remember, email messages are subject to discovery under public records laws.

- 2) **Spam** is an unsolicited email message usually containing some form of advertisement.

Example:

To: Mary From: Market Access Subject: Discount Pills Get great deals on prescription drugs!
--

Other examples of spam include:

- Free Money
- Great deals on products and services

Note: Spam is very hard to control. In addition to the spam filters on the Borough's systems, you can help to control spam by not opening a message that appears to be spam or from an unknown source. By opening spam you verify that your address is real, subjecting you to more spam messages. Spam messages need to be deleted immediately.

- 3) **Temporary or transitory e-mail messages** are any exchange of communication that is fulfilled almost immediately upon request. Keep these messages until the task is complete or their value has passed. If you are uncertain, assistance is available at the Borough Clerk's Office.

Example:

To: Mike From: Fred Mike, send me that report we talked about when you get a chance. Thanks. Fred

Other examples of email with temporary/transitory value:

- Charity campaigns
- Listserv messages
- Company-wide communications
- Meeting reminders
- Deadline reminders
- Routing slips
- Fax confirmation
- Reading materials
- Reference materials
- FYI email information that does not elicit a response

Note: Unnecessary retention of temporary emails can drive up storage costs and damage the Borough in litigation. Remember that your email is never private.

- 4) **Email messages soliciting a response** is any exchange of communication that requires the recipient to respond or to perform an action on the message received. These messages may include attachments that the recipient will also need to respond to. The retention of these emails and any accompanying attachments will depend upon the content of the message.

Example:

To: Joe
From: Sam

Attached are my fourth quarter figures. Please add yours in the appropriate columns and return it to me ASAP!

Other examples of emails soliciting responses are:

- Contract negotiations
- Administrative or fiscal communications
- Policy drafts
- Reports
- Requests for information

Note: Email messages that require a response are almost always public records in relation to access and retention. Remember that the email system is not a secure medium and information of a confidential or sensitive nature should **never** be sent via email.

Identifying Email Messages Subjected to Records Retention

Many email messages fall under the definition of public record found in HBC 2.64.030 and Alaska Statutes. Email that constitutes a public record needs to be identified, managed, protected and retained for as long as needed to meet the administrative, legal, financial, and historical needs of the Borough, and the retention and disposition should be according to the most current *Haines Borough Record Retention Schedule*. It's important to note that since email is a method or a tool for communicating, a blanket retention for "Email Records" does not exist. Therefore each message needs to be evaluated for content to determine which retention to apply. The Records Retention Schedule and assistance is available at the Borough Clerk's Office.

1) **Employees may delete the following:**

- Email records after they have been filed in a record keeping system; and
- Records of transitory or little value that do not document agency activity

Examples of messages that typically do not constitute a public record are:

- Personal messages or announcements
- Copies or extracts of documents distributed for convenience or reference
- Announcements of social events
- Messages received via a listserv
- Spam

(See Email types 1-3 on the first page of this attachment)

2) **Employees must retain messages that are considered public records** and according to the most current *Haines Borough Record Retention Schedule*.

Examples of messages sent by email that typically are public records include:

- Policies and directives
- Correspondence or memos related to official business
- Work schedules and assignments
- Agendas and minutes of meetings
- Drafts of documents that are circulated for comment or approval but only until the document is final. At that point, the drafts may be deleted.
- Any document that initiates, authorizes, or completes a business transaction
- Final documents or recommendations

(See Email type 4 at the top of this page)

3) **Disclosure Statement.** Emails between non-Borough email addresses and Borough email addresses relating to Borough matters are public records subject to records retention and public records disclosure laws. The following, or a similar disclosure statement, should be automatically (if feasible) inserted into all email originating from employees and public officials of the Borough:

Please be aware that email sent to or received from Borough staff or public officials is a public record and may be subject to public disclosure upon request.

Introduction

The use of email has become an indispensable tool for communicating as well as sharing and distributing information. As a communication tool, it is important to represent the Borough in a professional manner, respond to email clearly and efficiently, and protect the Borough from liability and unnecessary risk.

Purpose

The *Information Technology Resources Policy* establishes the expectations the Borough has for users when they are using the Borough email system. This attachment provides email etiquette advice and rules to help users become aware of their responsibilities when using the email system.

Why do we need email etiquette?

- **Professionalism** - by using proper email language the Borough will convey a professional image.
- **Efficiency** - email messages that get to the point are much more effective than poorly worded email messages.
- **Protection from liability** - user awareness of email risks may protect the Borough from costly lawsuits.

What are the etiquette rules?

There are many etiquette guides and many different etiquette rules. Listed below are the email etiquette rules that should be applied to use of the Borough's email system.

- **Email cannot replace personal contact**
There is a tendency to be less careful or formal when communicating using email and that can sometimes provoke anger or frustration. Direct, person-to-person contact is best for handling sensitive, difficult, complex, or emotional issues.
- **Email is public**
Assume the messages you send and receive are permanent and public. Don't say anything in an email message that you would not want to be made public or forwarded to others.
- **Do not use email to discuss confidential information**
Sending an email message is like sending a postcard. If you don't want your message to be displayed on a bulletin board, don't send it. Moreover, never make any libelous, sexist or racially discriminating comments in an email message. Nothing is private on the Internet. When you commit something to text, or worse, to pictures or videos and send it out, you've created something that lasts forever and can easily be sent on again and again and again.
- **Use proper spelling, grammar and punctuation**
This is not only important because improper spelling, grammar and punctuation give a bad impression of you and the Borough, it is also important for conveying the message properly. Email messages with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. If your program has a spell checking option, use it!
- **Read the email message before you send it**
A lot of people don't bother to read an email message before they send it out, as can be seen from the many spelling and grammatical mistakes contained in many of them. Apart from this, reading your email message through the eyes of the recipient will help you send a more effective message and avoid misunderstandings and inappropriate comments.

- **Use proper structure and layout**

Since reading from a screen is more difficult than reading from paper, the structure and layout is very important for email messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.

- **Avoid long sentences**

Try to keep your sentences to a maximum of 15-20 words. Email is meant to be a quick medium and requires a different kind of writing than letters. Also, take care not to send email messages that are too long. If a person receives an email message that looks like a long essay, chances are that they will not even attempt to read it.

- **Be concise and to the point**

Do not make an email message longer than it needs to be. Remember that reading an email message is harder than reading printed communications.

- **Do not write in all CAPITALS**

IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be highly annoying and might trigger an unwanted response in the form of a “flame” mail (an extremely critical or abusive email message or posting in public forum, often as retaliation).

- **Flaming**

Avoid public “flame mail” – messages sent in anger. Wait and think about what you want to say before responding. Messages sent in anger only “fuel the flames” and are usually regretted later. Take a few hours or even a day to reply. If time is of the essence, call or visit them in person instead. Often times, a face-to-face meeting can clear up a misunderstanding or defuse what could have been an ugly email confrontation. In terms of e-mail etiquette, take a moment to re-read and think about your e-mail before you send it out.

- **Don't send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks**

By sending or even just forwarding one libelous or offensive remark in an email message, you and the Borough can face legal charges resulting in multi-million dollar penalties.

- **Answer swiftly**

Citizens, elected officials, and staff use an email message because they wish to receive a quick response. Therefore, each email message should be replied to within at least 24 hours and, preferably, within the same working day. If the email message is complicated, send a response that you have received their message and that you will get back to them.

- **Do not attach unnecessary files**

Wherever possible, only send attachments when they are productive and, when necessary, compress the attachment. Large attachments can bring down an email system.

- **Do not overuse the high priority option**

We all know the story of the boy who cried wolf. If you overuse the high priority option, it will lose its function when you really need it. Moreover, even if an email message has high priority, your message will come across as slightly aggressive if you flag it as ‘high priority’.

- **Avoid using URGENT and IMPORTANT**

Even more so than the high-priority option, you must at all times try to avoid these types of words in an email message or subject line. Only use this if it is a really urgent or important message.

- **Don't leave out the message thread**

When replying to an email message, include the original message in your reply--in other words click ‘Reply’, instead of ‘New Mail’.

- **Do not overuse 'Reply To All'**
 Only use 'Reply to All' if you really need your message to be seen by each person who received the original message. Choose your recipients wisely. Do not default to "Reply to All." Avoid copying lots of other people "just in case" they might be interested. We're all too busy for that as we struggle to maintain some semblance of work-life balance.
- **Take care with abbreviations and emoticons**
 In Borough email messages, you may not want to use abbreviations such as BTW (by the way) and LOL (laugh out loud). The recipient might not be aware of the meanings of the abbreviations and these are generally not appropriate in business email messages.
- **Be careful with formatting**
 Remember that when you use formatting in your email messages, the sender might not be able to view formatting or might see different fonts than you had intended. When using colors, use a color that is easy to read on the background.
- **Take care with rich text and HTML messages**
 Be aware that when you send an email message in rich text or HTML format, the sender might only be able to receive plain text emails. If this is the case, the recipient will receive your message as a .txt attachment.
- **Do not forward chain letters**
- **Do not ask to recall a message**
 The chances are that your message has already been delivered and read. It is better to send a follow-up email message to say that you have made a mistake. This will look much more honest than trying to recall a message.
- **Do not copy a message or attachment without permission**
 Do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.
- **Use a meaningful subject line**
 Try to use a subject line that is meaningful to the recipient as well as yourself. This should also mean changing the subject line if the subject of the reply (or replies) changes from what the initial subject was. Often the subject line is the only clue the recipient has about the contents when filing and searching for messages. "Requested document" or "Check this out!" don't cut it as subject lines when people are receiving hundreds of messages per day. Use five to eight well chosen words so your reader knows immediately what you're writing about. A subject line such as "Wednesday Meeting" is not nearly as helpful as "Agenda for Wednesday Staff Meeting." If you don't write a descriptive subject line, you run the risk of not having your e-mail read. And if you leave the subject line blank, you don't even deserve a reply.
- **Use active instead of passive voice**
 Try to use the active voice wherever possible. For example, "Our department will contact you today" sounds better than "You will be contacted by our department today." The first sounds more personal and assures the recipient that you are actively working to meet their needs.
- **Don't reply to spam**
 By replying to spam or by unsubscribing, you are confirming that your email address is 'live'. Confirming this will only generate more spam. Therefore, just hit the delete button or use email software to remove spam automatically.
- **Use the "cc:" field sparingly**
 Try not to use the "cc:" field unless the recipient knows why they are receiving a copy of the message. Generally, you do not include the person in the "cc:" field unless you have a particular reason for wanting this person to see your response. Again, make sure that this person will know why they are receiving a copy.

- **As a general rule, do NOT respond to a message you were only copied on**

You were likely cc'd because the sender just wanted you to be informed...just an FYI. If the sender intended you to jump into the conversation, you would have been one of the main recipients in the "to" field. It is impolite and presumptuous to act as though you are part of that particular conversation. However, if you believe you must jump in to clarify a misstatement or to add some important feedback or information, reply *only* to the sender and explain your reason for responding.

- **Signatures**

Use a signature, and make sure it identifies who you are and includes alternative means of contacting you (phone and fax). The Systems Administrator can show you how. A disclosure statement similar to the following should be included:

Please be aware that email sent to or received from Borough staff or public officials is a public record and may be subject to public disclosure upon request.

- **Courtesy**

Email is all about communicating with other people and, as such, remembering basic courtesies is never a bad idea. If you're asking for something, don't forget to say "please" and if someone does something for you, make sure you say "thank you." ☺

- **Email Among Public Officials**

Email exchanges between public officials can create an unintended quorum by "serial communication" and violate the Alaska Open Meetings Act. Public officials should avoid email exchanges that ultimately involve or create a quorum. To avoid creating a quorum, reply only to the sender, or to the borough clerk. If public officials wish to send an informational email to a majority of the governmental body, it should be sent to the borough clerk who will distribute it and make it clear it is informational only and no response is desired. This applies to both elected and appointed officials.