MEMORANDUM

To: All Employees
From: John R. Corso, City & Borough Attorney
Via: Dave Palmer, City and Borough Manager
Subject: Telecommunications Policy
Date: December 9, 1998

Read this memorandum carefully: it establishes policies about your privacy rights and other important subjects.

Section 1. Introduction

The Capital City is a leading proponent and user of telecommunications and information technologies. These technologies, when properly used, support our governmental functions and enable closer and more timely communications within the CBJ and with the public. There is a continuing evolution of laws and conventions governing acceptable use of telecommunications tools. Careless use of these tools can have dramatic consequences, harming the CBJ, our citizens, and our employees. These policies are intended to minimize the likelihood of such harm by educating our employees and guiding their actions. Existence of these policies will also serve to protect the CBJ in litigation and other disputes. These policies are mandatory. Employees who violate them are subject to discipline up to and including termination from service. CBJ department and division heads should adopt and communicate these policies. Please direct any questions to the MIS Division or the Law Department. The CBJ intends generally to observe these policies but also reserves the right to change them at any time without prior notice. The CBJ will make reasonable efforts to provide such notice. These policies apply to “telecommunications tools”, a term which includes email, voice mail, and internet access. These policies do not apply to voice telephone, voice radio, facsimile machines, or public use of public internet terminals in libraries.

Section 2. Use and Misuse of Telecommunications Tools

2.0 Access. Access to CBJ telecommunications tools is provided in conjunction with official CBJ business and your job responsibilities. Your use of these tools is subject to this policy and to other CBJ policies and procedures. CBJ telecommunications tools also may be made available to individuals who are not CBJ employees, such as members of advisory committees, contractors, temporary service people, vendors, and members of the public. Use of these tools by such persons is subject to this policy and to applicable agreements. Telecommunications tools and all messages produced or carried by such tools are CBJ property, subject to reasonable inspection by CBJ supervisors.
2.1 Acceptable Use. In the course of your job, you may use these telecommunications tools to communicate internally with CBJ coworkers or externally with citizens, consultants, vendors, and other business acquaintances. The CBJ provides you with telecommunications tools to facilitate official telecommunications and to enhance your productivity. As with the telephone, there may be occasion to use these facilities for personal purposes. Personal use is permitted so long as it does not interfere with the performance of your job, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Such facilities are not to be used for personal financial gain, or to solicit others for activities unrelated to official business, or for the purpose of advocating voting for or against a candidate for federal, state or municipal office, or a federal, state or municipal ballot issue, with the following exception: the MIS Division may make available or otherwise authorize special-purpose bulletin boards and web pages enabling employees to market and sell personal property (other than for commercial purposes), and in connection with CBJ-approved social events, sporting events, and other sanctioned activities. When making use of these CBJ-provided facilities for personal use, always remember that you have a very limited expectation of privacy (see discussion below).

In addition to other restrictions and conditions discussed here, you may not use any telecommunications tool:

- To carry any defamatory, discriminatory, or obscene material;
- In connection with any infringement of another person’s intellectual property rights such as copyrights;
- In a manner that violates the terms of any applicable telecommunications license or any laws governing data collection, protection, privacy, confidentiality, and security;
- In connection with any attempt to penetrate computer or network security of any CBJ or other system, or to gain unauthorized access or attempted access to any other person’s computer, email or voicemail accounts or equipment; or
- In connection with the violation or attempted violation of any other law.

For purposes of this policy, “obscene” means sexually explicit images or text which depict sexual conduct in a patently offensive way, which, taken as a whole, appeal to prurient interest and which lack serious literary, artistic, political, or scientific value. “Sexual conduct” is defined in detail in the footnote below.

The CBJ understands that web “surfing” may be business-related and serve a legitimate business function, but the potential for abuse exists. The Internet provides access to a huge amount of information and resources that can greatly enhance our ability to deliver services efficiently to our customers. Today there is no single, comprehensive directory of resources available for the Internet and users sometimes must navigate through much unneeded information to reach useful material. The CBJ encourages exploration of the Internet for legitimate business-related or professional activities, but you should avoid “browsing the web” on CBJ time, creating personal “home pages”, or otherwise using CBJ facilities to access Internet sites for reasons unrelated to the CBJ’s business and your job responsibilities.

2.2 Representing the CBJ in Your Postings. The information you publish electronically (sometimes called a “posting”) reflects on the CBJ in general. Despite any disclaimers that you make (e.g., that your views are your own and may not reflect those of your employer) readers elsewhere will make the

1 “Sexual conduct” mean actual or simulated: (1) sexual penetration; (2) the lewd touching by one person of another person's genitals, anus, or breast; (4) masturbation; (5) bestiality; (6) the lewd exhibition of genitals; or (7) sexual masochism or sadism.
association between your posting and the CBJ. You should know that true anonymity is very difficult to obtain when using these tools. While Internet relay chat (“IRC”), newsgroup visits, and net “surfing” sometimes appear to be done anonymously (e.g., by employing pseudonyms), accessing such services or servers through CBJ network facilities normally leaves an “audit trail” indicating at least the identity of the CBJ internet server, and may leave a trail pointing directly to you. Inappropriate use of CBJ facilities may damage the CBJ’s reputation and could give rise to agency and individual liabilities. Accordingly, you should make every effort to be professional in all usage of CBJ telecommunications tools.

2.3 Unacceptable Content. Although the CBJ does not regularly monitor voicemail or electronic messages it reserves the right to do so at any time for any official purpose. Please be aware that even personal email and voicemail messages may be viewed publicly or by CBJ management without further notice. Under no circumstances may any posting, voicemail or email originating at the CBJ be in violation of the letter or the spirit of the CBJ’s Equal Employment Opportunity or Sexual Harassment policies.

Examples of unacceptable content include:

- Obscene messages, images, cartoons, or jokes (for the definition of “obscene”, see section 2.1);
- Unwelcome propositions, requests for dates, or love letters;
- Slander or libel;
- Ethnic, religious, or racial slurs;
- Any other message that could reasonably be construed as harassment or disparagement of others based on their sex, physical or mental disability, marital status, changes in marital status, pregnancy, parenthood, race, religion, color, or national origin.

Everyone should be aware that “sexual harassment” includes unwelcome sexual advances, unwelcome requests for sexual favors, or other unwelcome conduct (including comments) of a sexual nature. The standard for sexual harassment is whether the recipient could reasonably consider the message to be offensive – the sender’s intentions are irrelevant. In addition to prohibitions on sending or uploading offensive materials, CBJ telecommunications tools also shall not be used to access or download obscene materials.

2.4 Electronic Forgery. Electronic forgery is defined as misrepresenting your identity in any way while using telecommunications tools. This includes using another’s email account without permission, or by modifying another’s messages without permission. For example, messages written by others should be forwarded “as-is” and with no changes, except to the extent that you clearly indicate where you have edited the original message (for example, by using brackets or by using other characters such as * * * to flag edited text).

Electronic forgery is not allowed for any purpose. For email messages, you may not take any action to misrepresent the identity of the person responsible for the message. You may send email messages using another person’s account, but only with prior express approval from the account owner, and only when the text of the message indicates that you are the author.

2.5 Intellectual Property. The Internet offers a universe of information, useful in conducting and furthering business operations. You must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and inventions. Do not copy, use, or transfer others’ materials without appropriate authorization. Be aware that downloaded software and other copyrighted material may be subject to licensing obligations or
restrictions. Even “freeware” or “shareware” may contain restrictions that prohibit or limit the usage or commercialization of such items. If you have any questions in this regard, contact the City Attorney.

2.6 Transmitting Confidential Information. Confidential information (whether owned by the CBJ, its vendors, or other persons) is not to be disclosed to unauthorized persons without prior authorization. The question of “authorization” will be a function of the type and ownership of the confidential information. (For example, different authority may be required for disclosure of CBJ-owned information than for vendor-owned information). Also, “authorization” for disclosure may be limited to certain specific individuals within the agency on a need-to-know basis. Generally, the common-sense prohibition of casual disclosures means that confidential information should not be contained in email sent to outsiders or posted to newsgroups, and should not be placed on CBJ telecommunications tools that are available to third-parties, such as unsecure notebook computers that are accessible to non-CBJ personnel. You should post such information on web pages only when you are certain that the web page is not accessible from locations outside the CBJ firewall. Also, you should not set your CBJ email account to forward automatically your email to any non-CBJ account such as your America Online account.

2.7 Encryption. CBJ security standards and policies also govern the use of encryption tools. Only authorized encryption tools (software and hardware) may be used in connection with any CBJ telecommunications tools. Except with the prior written consent of the MIS director, all such tools must implement key-recovery or key-escrow techniques to permit the CBJ to access and recover all encrypted information (e.g., in the case of the absence of the employee who performed the encryption).

Section 3. Limits of Privacy

3.0 Retention and Security of Messages. Email and voicemail messages and computer-stored items all are CBJ property and business records. They are also public documents. They must be administered as required by the Alaska Archives Act, the Alaska Open Records Act, and CBJ document retention policies. In addition, messages may become evidence in a lawsuit and thus subject to the rules of court regarding discovery.

It is the policy of the CBJ that email messages are temporary informal documents that should be routinely destroyed after 90 days unless you make a deliberate decision to preserve them. As specified by the authorities listed above, and by this policy directive, you are required to administer your email messages as follows:

- Immediately upon sending or receiving a message, you should make a determination whether the copy of that message on your computer has any lasting administrative, legal, or historical value, or if it is evidence in a pending or probable lawsuit.

- If the message has no lasting value and does not constitute evidence, you may destroy it immediately or you may do nothing: just leave it in the “inbox” or whatever your email program calls the general reception area for incoming messages. The inbox should be set to destroy all messages older than 90 days. Before a message is destroyed, you may change your mind about the value of a message, or its status as evidence. If so, remove it from the inbox and preserve it as described below.

- If the 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 “out” 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.
Email messages are official documents until they are destroyed, and may have legal and operational effect identical to that of traditional, hardcopy documents. Accordingly, all email messages preserved in a special folder, or held in your inbox but not yet destroyed, should be treated as though they may later be viewed by others (while confidential information may be contained in such messages, these messages should be created with the same care you would use in creating hardcopy documents). Messages preserved outside your inbox folder are subject to inspection and copying by the public under the Open Records Act. They are also subject to discovery by the parties in a lawsuit under the rules of court.

Messages in your inbox folder but not yet destroyed are regarded as temporary documents and are not subject to inspection or copying by the public under the Open Records Act. However, they are still subject to discovery by the parties in a lawsuit. Do not attempt to evade these requirements by moving or destroying documents in response to legitimate requests under the Open Records Act or because a lawsuit has been or probably will be filed. Any such attempt is illegal, will probably be detected, and will subject the CBJ and you to severe penalties.

Remember that no electronic communications facility is completely secure. This means that information stored or carried over CBJ telecommunications tools may be the subject of accidental or intentional interception, misdelivery, attack, or authorized CBJ review.

When stored on computers, email messages and other files typically are subject to routine backup procedures. This means that copies of these files may be retained for long periods of time (in accordance with backup recycling and document retention procedures). Also, keep in mind that many site-wide backup systems do not guarantee privacy of backup copies (e.g., system administrators may have access).

3.1 A Limited Expectation of Privacy. The CBJ respects the personal privacy of its employees. However, because telecommunications tools are provided for CBJ’s official purposes, employee rights of privacy in this context are quite limited. Employees and others subject to this policy should have no expectation that any information transmitted over CBJ facilities or stored on CBJ-owned computers is or will remain private. These systems are owned and controlled by the CBJ and are accessible at all times by the CBJ for maintenance, upgrades, or other business or legal purposes. Employees who use CBJ telecommunications tools should be aware that our security tools create an audit log detailing every request for access in either direction by each user. Also, in the course of their duties, system operators and managers may monitor employee use of the Internet or review the contents of stored or transmitted data. Passwords for email and other systems are issued to employees for the purpose of excluding unauthorized personnel, and not in order to provide privacy from official review. When employees change their passwords, they should provide copies of the updated passwords to their supervisors.

The CBJ permits personal use of all these telecommunications tools on the express understanding that it reserves the right for official purposes to review employee use of, and to inspect all material created by or stored on, these telecommunications tools. Use of these tools constitutes each employee’s permission for the CBJ to monitor telecommunications and to access files that are made on or with these telecommunications tools.

3.2 Agency Access to Computers, Voicemail, and Email Systems. CBJ Supervisors will not routinely examine employees’ communications or files. However, such examination generally may be expected to occur in the following circumstances, and other situations where warranted:

- Ensuring that CBJ systems are not being used to transmit discriminatory or offensive messages, or in connection with the infringement or violation of any other person’s rights,
- Determining the presence of illegal material or unlicensed software,
Counteracting theft,
 Ensuring that telecommunications tools are not being used for inappropriate purposes,
 Responding to legal proceedings that call for producing electronically stored evidence, or
 Locating, accessing, and retrieving information in an employee’s absence.

3.3 Unsolicited Email. Unsolicited commercial email, also known as “spam”, is a waste of CBJ resources. Do not respond to spam, even to request removal from a mailing list: it only invites more unwanted messages. Any email from an unknown source can present the danger of viruses contained in attachments to the message. For these reasons, you should proceed cautiously before opening email attachments from an unknown source.