Chelsea Housing Authority
Information Technology Policy

This document formalizes the policy for employees and contractors ("users") of the Chelsea Housing Authority ("CHA") on the use of information technology ("IT") resources, including computers, printers and other related hardware, software programs, data, e-mail, local and wide area networks, and the Internet. Use of IT resources by any employee or contractor shall constitute acceptance of the terms of this policy.

1. User Responsibilities

It is the responsibility of any person using IT resources to read and follow this policy. In addition, users are expected to exercise reasonable judgment in complying with this policy and in the use of IT resources. Any person with questions regarding the application or meaning of this policy may seek clarification from supervisor or any senior staff manager. Failure to observe this policy may subject individuals to disciplinary action, up to and including termination of employment, subject to the provisions of any applicable collective bargaining agreement.

2. Acceptable Usage

The Chelsea Housing Authority firmly believes that IT resources allow users to function more efficiently and effectively by helping them to deliver better services with greater efficiency and lower costs. As such, employees and contractors are encouraged to use IT resources to the fullest extent in pursuit of the Authority's goals and objectives. Each user is responsible for ensuring that her or his usage is for an appropriate purpose and is conducted professionally and courteously.

Users are permitted to use IT resources for any work-related activity with the exception of those activities specifically prohibited in the following section. Outside of normally scheduled work hours, users are permitted to use IT resources for personal activity with the exception of those activities specifically prohibited in the following section.

The CHA is not responsible for any adverse consequences resulting from the use of IT resources for personal activity. Users waive any claims with respect to the CHA arising from their use of IT resources for personal activity.

If users wish to share access to their files or e-mail with other users, they should contact the “Terminal” for assistance in configuring their accounts to appropriately and securely share IT resources.

3. Unacceptable Usage

Users are prohibited from using any IT resources to interfere with the CHA's ability to conduct its business in an efficient, productive, and professional manner.

It is unacceptable for an employee or contractor to use IT resources:

1. In furtherance of any illegal act, including the violation of any applicable criminal or civil laws or regulations, whether state or federal;
2. For any personal political activity in support of particular candidates or causes;
3. To individually or collectively operate any profit or non-profit enterprise;
4. To send messages that contain racial slurs or other comment that maligns a person because of gender, age, sexual orientation, religious or political beliefs, national origin, disability or other status protected by federal, state or local law;
5. To access or share sexually inappropriate, obscene or other pornographic materials;
6. To knowingly to infringe any intellectual property rights;
7. To gain, or attempt to gain, access to any computer or program without authorization from the “Terminal”. Users may not use another user's passwords or accounts for any purpose without authorization, including accessing files or programs, creating or retrieving e-mail messages, or accessing Internet sites;
8. For any use that causes interference with, or disruption of, network users and resources, including the intentional propagation of computer viruses or other harmful programs;
9. To intercept or knowingly retain communications addressed to other persons;
10. To knowingly misrepresent either the CHA or a person's role at the CHA;
11. To distribute chain letters;
12. To access online gambling sites; or
13. To defame any person.
14. To access chat rooms or any other social media outlet

Users may not install software downloaded from the Internet or otherwise, including screen savers, onto a PC unless the “Terminal” has authorized the installation. The “Terminal” will conduct periodic audits of the CHA's computers without notice to detect unauthorized usage.

4. Data Confidentiality

In the course of performing their jobs, CHA employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors intentionally to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors knowingly disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs and the dissemination is authorized under state or federal law.

5. Copyright Protection

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users may not install any software downloaded from the Internet or obtained from any questionable source without contacting the “Terminal” so that the software, including "freeware" or "shareware" used for evaluation purposes, can be examined to ensure it is properly licensed. Users should exercise care and judgment when copying or distributing information that could reasonably be expected to be copyrighted.

6. Network Security

Most desktop computers are connected to a wide area network that links computers throughout the Authority. As such, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their Network or CCS passwords with anyone else, and should promptly notify the “Terminal” if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a terminal password-protected screensaver in operation. Finally, no user is allowed to access the Internet or other external networks via modem unless they have been specifically approved for access by their departmental manager and have been granted access by the “Terminal”.

7. Computer Viruses

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Users may not install any software downloaded from the Internet or obtained from any questionable source without contacting the “Terminal” so that the software can be examined for viruses. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. Suspicious e-mail messages, even those from a familiar source, should be immediately reported to the “Terminal”.

8. E-mail

When using e-mail, there are several points users should consider.

First, as with all IT resources, e-mail messages are the property of the CHA.

Second, because users' e-mail addresses (firstintial-lastname@chelseaha.com) identify the CHA as the organization sending the message, users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that their e-mails are written in a professional and courteous tone.

Third, "All Staff" messages should be used only for sharing information that is business-related and of critical importance to the entire organization. Users should obtain their manager's approval before sending an "All Staff" message.

Finally, although many regard e-mail as being like a telephone in offering a quick informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

9. Privacy and Confidentiality

Use of the CHA's IT resources is not private. IT resources are the property of the Chelsea Housing Authority and are to be used in conformance with this policy, subject to applicable law.

All communications, including text and images generated from or to the CHA's IT resources may be "records" for purposes of the Records Conservation law, G.L. c. 30, § 42, and may constitute "public records" for purposes of the Public Records law, G.L. c. 66, § 10, or under the Freedom of Information Act. They may be subject to disclosure to law enforcement or other third parties without the prior consent of the sender or the recipient.

All e-mail messages and Internet sites visited by CHA employees are automatically stored on the CHA's computer back-up systems. Users should be aware that even when a message is deleted, it may exist on a backup tape.

Employees and contractors who use the CHA's IT resources are acknowledging that the CHA may use software tools to track, review and monitor employee utilization of the Internet and the e-mail system and to measure electronic or service quality and may access and review users' computer data and e-mail for legitimate business purposes such as ensuring compliance with the CHA's policies regarding racial or sexual harassment and to carry out CHA business when the employee is not available. Use of the CHA's IT resources for any purpose constitutes consent to these conditions.