**Town of Deep River**

**POLICY / PROCEDURE MANUAL**

|  |
| --- |
| Corporate Policies and Procedures |
| **DEPARTMENT:** Administration | **POLICY #:**IT-01 |
| **POLICY:** Responsible and Proper Use of Information Resources |
| **DATE OF ORIGIN:**Dec. 15, 2021 | **REVIEW DATE:**   |  **REVISION DATE:** | **APPLICABLE TO:**All Employees | **PAGE #:**1 of 4 |

**POLICY**

Employees of The Town of Deep River are responsible for using information resources in an effective, secure, ethical, and legal manner. The Town establishes the following procedures to promote a stable, secure, and reliable computing environment. Department specific guidelines may supplement, but do not supersede, this policy.

**DEFINITIONS**

**Information Resources**

Information resources are defined as information in electronic or audiovisual format, or hardware or software that makes possible the storage and use of such information. This includes but is not limited to local and externally accessed databases, electronic mail (e-mail), text/instant messaging, CDs, DVDs, USB/SD/external drives, recorded magnetic or solid-state media, photographs, and digitized information. These resources may be individually controlled, shared, stand-alone, networked, temporary, or permanent.

**Service Provider**

A service provider is defined as an agency outside of the Town that provides information technology services to the Town or one of its departments on a sustained basis e.g., file service, internet access, database hosting, cloud computing, communications infrastructure, technology support, computational cycles, and statistical analysis.

**System Administrator**

System Administrator is defined as, and will apply to, an individual who is assigned the responsibility to be the first line support that assists users, troubleshoots problems, performs maintenance tasks and is the first point of contact for departmental workstation issues.

**PROCEDURE**

1. Use information resources in a manner consistent with the public service, training, and administrative objectives of the Town of Deep River, as well as the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to information services.
2. The Town of Deep River characterizes as unethical, unacceptable, and just cause for taking disciplinary action, any activity through which an individual:
3. violates the Town or third-party copyright or patent protection and authorizations, as well as license agreements and other contracts; therefore, respect copyrights and licensing of programs, data, and software e.g., do not make copies of licensed computer software to avoid paying additional license fees or to share with other users;
4. interferes with the intended use of the information resources; therefore, respect the information resources’ intended use e.g., use the username and password, funds, transactions, data, and processes assigned to you by Supervisors, the System Administrator, only for the purposes specified;
5. seeks to gain or gains unauthorized access to information and / or information resources;
6. without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of Town, as well as third party, computer-based information and/or information resources; and
7. without authorization, invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information retained by the Town of Deep River.
8. All Town users are required to utilize information resources with respect for the public trust placed in the Town of Deep River, i.e., perform tasks with competence and integrity, and demonstrate ethical and acceptable conduct.
9. All Town users, by their access to information resources, accept responsibility to protect the IT environment from abuse, disruption, and unauthorized access; therefore, safeguard all data, personal information, passwords and authorization codes, and confidential data, by taking full advantage of the file security mechanisms built into the computing systems.
10. When creating your password, consult with the System Administrator regarding password guidelines.

6. Respect the privacy of others, i.e.:

1. do not intentionally seek information on, obtain copies of, or modify files, records, or passwords belonging to other users or the Town;
2. do not attempt to represent others, unless explicitly authorized to do so by those users; and
3. do not divulge sensitive personal data to which you have access, without explicit authorization to do so.

7. Respect the rights of others by complying with all Town policies regarding harassment as they apply to users of information resources.

8. Comply with any requests made by System Administrators, and / or Supervisors pertaining to account and systems use, provided such requests do not violate any other policy or procedure.

9. Respect the integrity of the system or network i.e., do not intentionally develop or use programs, transactions, data, or processes that harass other users, infiltrate the system, or damage or alter the software or data components of a system. Alterations to any system, network software, or data component are made only under specific instructions from the system administrator.

 10. Respect the financial structure of the Town’s computing or networking systems e.g., do not intentionally develop or use unauthorized mechanisms to alter or avoid charges levied by the Town for computing, network, or data processing services.

 11. The system administrator is required to follow the same policies, procedures, and conditions of use as all other employees, except when intervention or special actions are required to forestall an immediate threat to the security of a system or its users. These actions may include:

1. suspending system access for users involved in a violation that is being investigated;
2. taking necessary action to preserve the state of files and other information relevant to an investigation; and
3. examining content of e-mail and other private files, where the content may jeopardize the security of systems, the safety of users, the ability of the Hospital to conduct necessary business, or any other appropriate use as directed.

 12. Respect the acceptable use standards of external networks with which the Town has

connections e.g., web-based networks, cloud computing services, or social media; the Hospital cannot and will not extend any protection to you should you violate the policies of an external network.

 13. Violations of the above guidelines may result in appropriate corrective action, or may

even constitute a criminal offence; information concerning violations should be reported to the respective Department Head for the system involved. If you are unsure whom to report to, contact the Chief Administrative Officer (CAO), who will redirect the information to the appropriate person(s).