TOWN of ROCKLAND

Approved

Computer/Internet Use Policy

TABLE OF CONTENTS

TOWN of ROCKLAND

Approved

Computer/Internet Use Policy

1. Introduction

The Town of Rockland provides staff with computer equipment and the ability to communicate and receive information using electronic mail and the Internet. The Town utilizes this technology to improve staff efficiency and communication, and to serve the public more effectively. These computer resources are the property of the Town of Rockland and should be used for appropriate business purposes only. Town employees have an obligation to use electronic mail and their access to the Internet in a responsible and informed way, conforming to network etiquette, customs, and courtesies.

Questions regarding acceptable use can be referred the Town Administrator's Office. This policy may be updated from time to time and amended at the discretion of the Town Administrator and/or the Board of Selectmen. Department Heads may supplement this policy to accommodate their specific departmental circumstances.

2. Prohibited Activities

The following activities are strictly prohibited:

- Any illegal activity, including, but not limited to, the transmission of copyrighted or trade secret material, obscene or threatening materials, or the participation in any type of criminal activity.
- Transmission of materials used for commercial promotion, product endorsement or political lobbying.
- Attempts to violate the Town of Rockland computer system or the computer system of any other municipality, institution, organization, company or individual.
- Software piracy, or the downloading and transferring of software for which the user does not have proper licensing.

TOWN of ROCKLAND

Approved

Computer/Internet Use Policy

---

3.   Use of Computers

3.1   Authorized Use

Computers are provided for specific employees who utilize them to perform their job functions. Department Heads are responsible for determining which personnel are authorized to use each computer under the Department Head's purview. Any unauthorized use of computer equipment is prohibited.

3.2   Software

The copying or installing of software programs without prior approval of the Department Head or the Town Administrator is prohibited.

3.3   Virus Checking

Data files such as word processing documents; spreadsheets and database files, which originate from computers other than those located in a Town office must be checked for viruses before use. Users needing procedures for checking viruses should contact the Town Administrator or the Department Head. The Town Administrator may impose additional restrictions or regulations on the importing of files from computers outside the Town's network.

3.4   Storage

Documents and data files stored on the town's computers are the property of the Town and may be accessed by authorized personnel for the purposes of, but not limited to, system maintenance, back-up, recovery, virus checking and adherence to this policy.

4. Use of User Account and Passwords

4.1 Confidentiality

User accounts are unique and assigned to authorized individuals for Town business. The sharing or unauthorized use of a user account is strictly prohibited and a violation of this policy.

Passwords should be kept confidential at all times. Employees should endeavor to create passwords that are unique and not easily discoverable. The most secure passwords have a minimum of 6 characters and contain both letters and numbers.

4.2 Changing Passwords

Users should periodically change their passwords. Users needing instructions for changing their password should contact their Department Head or the Town Administrator's office.

5. Use of Electronic Mail (Email)

5.1 Town Business

Email is an effective way to communicate with town employees and other job related contacts. Email is to be used for town business only. Email and any related on-line services, are the property of the Town of Rockland. Abuse of this privilege could result in the loss of electronic mail for the individual.

5.2   Content

Electronic mail should never be used for any illegal activity, including but not limited to, the transmission of copyrighted or trade secret material, the transmission of obscene, defamatory, or threatening material, or the propagation of any type of criminal activity. Electronic mail should also never be used to create offensive or disruptive messages or images. Among those things which are considered offensive are any messages or images which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

5.3   Public Record

Email messages are considered public record and therefore are discoverable. Users are considered the custodians of their messages and should maintain messages according to relevant public record law.

5.4   Confidentiality

Email (particularly Internet email) should be viewed as an unsecured mode of transportation. Confidential information should **NEVER** be sent via electronic mail. Employees should never assume that email messages or Internet postings are personal or confidential. All messages sent or received by electronic mail can be tracked by the Town's computer system. Employees are not authorized to retrieve or read messages that are not sent to them unless the intended recipient gives express permission.

═══

5.5 Unsolicited Email

Unsolicited email received from the Internet should not be opened. The user should delete the message immediately. Never open an attachment, especially if you do not know the source. Opening unknown attachments could initiate a virus.

6. Use of Internet Browsing Software

6.1 Privileges

Internet browsing capabilities are extended to those personnel requiring access to information on the World Wide Web.

6.2 Job Functions

Browsing should be limited to Internet sites directly related to the user's job function.

6.3 Downloading

Under no circumstances should software programs be downloaded from the Internet and / or installed without the prior permission of the Department Head or the Town Administrator. See section 3.2.

TOWN of ROCKLAND

Approved

Computer/Internet Use Policy

_____

6.4   Downloading of Documents

Careful consideration should be made before downloading any data files (e.g., word-processing, spreadsheets, files, etc.) from an Internet site. The reliability of the source of the document should be considered. Since harmful programs can be transmitted via documents, all documents and files must be checked for virus's prior to use. See section 3.3.

7.   Referral to the Town Administrator/Department Head

7.1   Unusual Occurrences

All matters relating to unusual occurrences must be reported immediately to the Department Head or the Town Administrator. When something unusual occurs, record information such as steps taken and warnings from the computer to aid in diagnosing the situation.

8.   Sanctions

Any employee who violates this policy or uses the Town's computer system for inappropriate purposes shall be subject to disciplinary action, up to and including discharge. Violations will also be reviewed as to whether criminal charges may be warranted.

TOWN of ROCKLAND

Approved

Computer/Internet Use Policy

═══

9. Acknowledgement - Receipt of Policy

The use of the Town's computer system constitutes employee consent to monitoring of systems and is conditioned upon strict adherence to this policy. Any employee who violates this policy or uses the Town's computer system for improper purposes shall be subject to discipline, up to and including discharge.

The Town Administrator is responsible for ensuring that any employee given computer and/or Internet services has read and signed a copy of this policy. A signed copy should be given to the employee and a second copy will be place in the employee's personnel file.

I certify that I was given a copy of this policy and provided the opportunity to ask questions about its content.

_____
Employee Name

_____   _____
Employee Signature   Date

_____
Department Head Name

_____   _____
Department Head Signature   Date