Grand River Conservation Authority

Report number: GM-09-22-72

Date: September 23, 2022

To: Members of the Grand River Conservation Authority

Subject: Human Resources Policy Update - 1.4 Acceptable Use of Information and Information Technology Resources

Recommendation:

THAT Human Resources Policy - 1.4 Acceptable Use of Information and Information Technology Resources be amended, approved, and implemented effective September 23, 2022.

Summary:

On April 11, 2022, Bill 88, Working for Workers Act, 2022 received Royal Assent. One of the requirements of this Act requires employers with 25 or more employees to have a written policy in place regarding electronic monitoring of employees. The policy must be in place by October 11, 2022.

The Ontario Ministry of Labour, Training, and Skills Development provided guidance on achieving compliance with the new requirements. Based on these guidelines, staff determined that some minor modifications to the current GRCA Human Resources Policy 1.4 'Acceptable Use of Information and Information Technology' are required for the GRCA to be in compliance with Bill 88.

Report:

On April 11, 2022, Bill 88, *Working for Workers Act, 2022*, received Royal Assent and is now law. Bill 88 included amendments to the *Employment Standards Act, 2000* that requires employers with 25 or more employees on January 1 of each year to have a written policy in place regarding electronic monitoring of employees by March 1 of the same year. A transitional provision gives employers with 25 or more employees on January 1, 2022 until **October 11, 2022** (six months after Bill 88 received Royal Assent) to comply with this new requirement.

On July 13, 2022, the Ontario Ministry of Labour, Training and Skills Development (Ministry) updated its online guide to the *Employment Standards Act, 2000* to include a chapter on the written policy on electronic monitoring of employees. Based on the guidelines, staff determined that some minor modifications to the current GRCA Human Resources (HR) Policy 1.4 'Acceptable Use of Information and Information Technology' are required for the GRCA to be in compliance with Bill 88.

To comply with Bill 88, an employer's policy statement must include:

a) Basic statement that employer electronically monitors employees
b) Description of **HOW** employer electronically monitors employees
c) **Description of circumstances** in which monitoring occurs
d) **Purpose** for which information is obtained through electronic monitoring

Policies must capture monitoring of employees' personal devices and any electronic monitoring which takes place in the context of a remote work arrangement (i.e. cell phones, personal laptops).

Staff recommend approval of the revised wording for HR Policy 1.4, with the recommended changes noted in the following sections:

- Section 1.4.1 General
- Section 1.4.11 Monitoring

Attachment A contains HR Policy 1.4 with the recommended changes highlighted.

Financial Implications:

None.

Other Department Considerations:

Not Applicable

Prepared by:

Sonja Radoja
Manager of Corporate Services

Approved by:

Karen Armstrong
Deputy CAO/Secretary Treasurer

APPENDIX A – GRCA Human Resources Policy

1.4 Acceptable Use of Information and Information Technology Resources

1.4.1 General
GRCA uses a variety of computing and communications systems in carrying out its business. All communication and information transmitted by, received from or stored in these systems is the property of GRCA and, as such, is intended to be used for job-related purposes only.

In the course of carrying out business, the electronic monitoring of employees may occur.

All Employees must read, understand and conform to this policy before receiving access to the various systems in use at GRCA. Any questions should be directed to the Employee's Supervisor or the Manager of Information Systems and Technology (IS&T).

1.4.2 Access
GRCA will provide computer accounts to GRCA Employees as required. External people, such as volunteers or contractors, may also be provided accounts as appropriate, and this will be determined on a case-by-case basis and all aspects of this Policy will apply to those users. The Employee managing the temporary or contract staff assumes responsibility for the identification of access requirements and use of the account. Accounts will be revoked on request of the user or Manager or when the Employee terminates employment at GRCA.

1.4.3 Passwords
Initial passwords are assigned by the IS&T Department and Employees must change the provided passwords as soon as possible. GRCA reserves the right to override any Employee-selected passwords and/or codes. Employees are required to provide the GRCA with any such codes or passwords to facilitate access as needed. Periodically, Employees may be required to change their passwords. At no time should an Employee allow a temporary, contractor or another Employee use of their user name or password. In the case where an Employee does provide another person access to Human Resources Policies – May 2022 Page 9 their account, they will be responsible for the actions of the individual using their account. Passwords should not be stored in computer data files, on the network, or be displayed openly at any workstation.

1.4.4 Physical Security
Access to server rooms and communications closets will be limited to Employees who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive(s) should be secured in a locked room or office during non-business hours. Equipment which is to be removed from GRCA property must be approved in advance by the IS&T Department and an inventory of this equipment maintained by IS&T. Any equipment that is to be removed from the premises must be documented in accordance with Human Resources Policy No. 7.2 Moveable Assets. If the Employee leaves the employment of GRCA, he or she must return the equipment to GRCA prior to the last day of employment. To ensure protection of data, disposal of any surplus Information Technology equipment must be carried out by the IS& T Department.

1.4.5 Network and Systems Security
The IS&T Department implements and maintains tools and procedures to provide adequate protection from intrusion into GRCA's computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Employees should not store personal, business or other credit card/account information, or passwords within word processing or other data documents.

All Employees are responsible for protecting the network against malware and/or virus attack by ensuring that tools installed on their devices, such as firewalls and anti-virus applications, are

not disabled. Staff should lock their devices or log off of the network when they will be away from their workstation for an extended period.

1.4.6 Employee-owned Electronic Devices
Employees may be authorized to access certain GRCA services such as email, calendars, contacts, etc. from Employee-owned electronic devices such as computers, tablets, smartphones, etc. Such access must be authorized by the Manager of the IS&T Department and the business use of such devices will be subject to the Monitoring section of this Policy. The Employee will be responsible to ensure compliance to the Passwords, Message Content, and Network and Systems Security sections of this Policy at all times when accessing GRCA services or conducting GRCA business on personally-owned devices. GRCA reserves the right to withdraw this privilege at any time without notice.

1.4.7 Software
Only legally licensed software will be installed on GRCA's computers, smartphones and other endnode devices. Users are expected to read, understand and conform to the license requirements of any software product(s) they use or install. Employees are expected to use the standard software provided by the IS&T Department, or identify applications they need in the course of their work. Employees are not permitted to install software, applications, demos or upgrades without the approval of the IS&T Department. Employees must use the standard email and messaging systems provided by GRCA for official email communications. Human Resources Policies – May 2022 Page 10

1.4.8 Data
Information and data created or obtained in the course of employment with GRCA is the exclusive property of GRCA. Release of data owned or licensed by GRCA to others shall be in accordance with GRCA's data licensing policies, which can be obtained from the IS&T Department.

Collection, use and disclosure of Personal Information must be in compliance with the Municipal Freedom of Information and Protection of Privacy Act (see also Human Resources Policy 1.1.10).

1.4.9 Protection of Data and Backup Procedures
All network files are backed up on a regular basis, and backup copies are stored off-site. Data stored on other devices, including local PC's, is not routinely backed up, and as a result, important data and applications should not be stored locally on these devices.

Employees are responsible for ensuring that GRCA information, data and communication remain within the control of GRCA at all times. The storage of GRCA information on personal or non-GRCA controlled environments, including devices maintained by a third party with whom GRCA does not have a contractual agreement, is prohibited unless such storage has been approved by the Manager of the IS&T Department.

1.4.10 Email Retention
All emails sent and received through GRCA's email system will be automatically archived by a centralized secure email archiving application. Archived emails will be retained in accordance with regulatory requirements.

1.4.11 Monitoring
GRCA provides the server, storage and network infrastructure, email system, personal computing devices (including PC's, smartphones and tablets) and other devices for employees' use on GRCA business. GRCA reserves the right to monitor the use of its Information and Information Technology Resources at any time, with or without notice, to ensure that such use is appropriate and in accordance with this Policy.

The GRCA also maintains video surveillance equipment at various GRCA locations and GPS devices in vehicles. The GRCA may monitor the information on this equipment in accordance with GRCA's Video Surveillance Policy and Procedure and Fleet Management System Policy.

GRCA understands that occasional personal use of Information and Information Technology Resources by employees may take place. Employees should note that such use, which includes but is not limited to personal emails, documents and other files is subject to all other sections of this Policy and will not be deemed personal or private.

While GRCA does not routinely monitor individual usage of its Information and Information Technology Resources, the normal operation and maintenance of these resources require backup of data and communication, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. Personal monitoring of a particular employee's usage by the IS&T Department will only take place if required by law or if there is a reasonable belief that the Information and Information Technology Resources are being used inappropriately. Such personal monitoring and/or disclosure must be approved in advance by the Chief Administrative Officer or the Human Resources Department.

1.4.12 Legal Proceedings

Electronic files, including emails, text messages, photos, etc sent or received by Employees may be used in legal proceedings or subject to disclosure under applicable legislation. Employees should be aware that email messages are considered official written correspondence and are potentially the subject of discovery, subpoena, Freedom of Information requests, etc.

1.4.13 Message Content

The email system is not to be used to solicit or promote commercial ventures, religious or political causes or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages. Human Resources Policy No. 1 Code of Conduct shall be considered the prevailing authority in the event of possible misconduct. In addition, the email system may not be used to send or receive copyrighted materials, trade secrets, proprietary information, or similar materials without prior authorization.

Employees are not authorized to retrieve or read any email messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so under the Monitoring section of this Policy.

1.4.14 Internet Use

The Internet is to be used for business purposes only. Employees with Internet access are expressly prohibited from accessing, viewing, uploading/downloading, or printing material that is in violation of the laws of Ontario, Canada and/or Human Resources Policy No.1 Code of Conduct. In addition, the internet may not be used to send or receive copyrighted materials, trade secrets, proprietary information, or similar materials without prior authorization. Employees should be mindful that there is no assurance that e-mail texts and attachments sent within GRCA and on the Internet will not be seen, accessed or intercepted by unauthorized parties. Any Public Wifi Access points that have been established for use by GRCA's visitors may be subject to limited access or a click-through acceptable use agreement, as determined by the IS&T Department, to ensure appropriate use consistent with this Policy.

1.4.15 Social/New Media

The GRCA makes use of various forms of social/ new media to promote programs, communicate topics of interest, educate and engage with the public (e.g. flood warnings, fire bans, promotion of GRCA programs, park events, etc.).

It is the responsibility of the Strategic Communications Department or their delegate(s) to manage the GRCA's official presence on social/new media networks and channels and to act as the official representative(s) of the GRCA for the purpose of posting content, answering questions, participating in discussions, etc. The GRCA acknowledges that other staff may be interested in following and/or contributing to GRCA's official social media activities.

From time to time, posts on the GRCA's social media accounts or about the GRCA can become contentious or difficult. The Strategic Communications department monitors its social media channels on an ongoing basis. Employees should refrain from participating in these types of online discussions, as they require a corporate and strategic approach. For further information, please refer to the GRCA's Social Media Framework.

Employees may wish to make their own posts about the GRCA, its activities and/or their program on their personal social media channels, and are encouraged to contact the Strategic Communications Department and/or their supervisor for guidance.

Staff members participating in social media for personal purposes, must not represent themselves as an official spokesperson of the GRCA. To ensure their personal posts or comments are not perceived as official GRCA communiques, staff should:

- not use a GRCA email address or user identification for personal social media activities;
- not use the GRCA's logo or other protected images on personal posts on social networks, blogs, etc
- not disclose any information entrusted to the GRCA that is confidential or protected by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); •not violate any copyrights, trademarks, or intellectual property rights that involve the GRCA and its partners; and
- not attempt to convey the GRCA's policies, practices or position on an issue when participating in personal social media activities.

When making posts or comments on any social media channel, whether public or private, staff shall conduct themselves professionally at all times. Be advised that inappropriate comments, videos, photographs, links, etc. on social media should be avoided.

In keeping with Human Resource policies on workplace harassment, violence and discrimination, defamatory or discriminatory content will not be tolerated and is meant to protect the health and safety of employees.

Staff shall abide by these guidelines whether they mention the GRCA by name or not. Even if the GRCA is not mentioned specifically, a link could be made to the GRCA, which could negatively affect the organization's reputation and may be considered a breach of this policy.

This policy is intended to ensure that the image, brand and reputation of the GRCA are not negatively impacted.

Staff should also be aware that members of the public may use mobile phones and other devices to take photographs or make recordings. Staff should always represent the GRCA positively and professionally. Staff who are photographed or recorded acting inappropriately or unprofessionally may be considered to have breached this policy.

Staff are encouraged to refer to the GRCA's Social Media Framework to further their understanding of the GRCA's use of social media as a corporate communications tool. If an employee is uncertain about this policy or has questions about the Framework, they should speak with their Supervisor/Manager/Director.

1.4.16 Recording Conversations in the Workplace

Staff are prohibited from recording conversations (video and/or audio) of other staff members while at work (notwithstanding the GRCA's Video Surveillance Policy and Procedure). Exceptions for recording conversations with knowledge and consent include:

- Public meetings and workshops
- Education and training materials
- Communications and media materials

Authorization from HR can be requested in advance for any exceptional circumstances.

1.4.17 Failure to Comply

Failure to comply with the Acceptable Use of Information and Information Technology Resources Policy may result in disciplinary action up to and including termination of employment. Any Employee who does not understand any part of this Policy is responsible for obtaining clarification from his/her Supervisor or the Manager of the IS&T Department. If an employee feels that a particular use of your computer, email, or Internet access should be permissible, but does not seem to be covered by this policy, they should consult with their Supervisor/Manager/Director.