Community Connections Support Services - Policies and Procedures

Section	**Technology Policy and Procedures**
Subject	**Technology Acceptable Use (tp020)**
Applies To	**Employees**
Revised Date	**May 2020**

Policy: All employees are to follow technology acceptable use procedures that are intended to enable employees to use technology to maximize productivity and effectiveness while also protecting the agency, its reputation, and its information assets.

Scope: This policy and accompanying procedures apply to all users of CCSS Information Technology (IT) Resources and all CCSS electronically stored information (ESI). The use of personally-owned equipment that involves the use of CCSS IT Resources and/or ESI is covered by this policy and accompanying procedures.

Definitions:

CCSS Electronically Stored Information (ESI) means electronic information that is created, stored, retrieved and communicated in digital form and which is accessible through CCSS IT Resources.

CCSS Information Technology Resources (IT) include, but are not limited to:

- networks, including wireless access services, wired networks, switching and routing, load balancers, firewalls, telecom equipment and cables, pbx and other network-related devices, equipment and services;
- servers;
- databases;
- business systems;
- learning management systems;
- websites;
- computers and computer systems, laptops, workstations, computer labs, thin clients, mobile devices, storage devices; and
- online collaborative tools including email, and social media sites (e.g. Twitter, Facebook and YouTube sites).

CCSS Technology is used here to refer to ESI and IT collectively.

Users means anyone who uses or attempts to use CCSS Technology and includes:

- employees,
- management,
- persons supported.

Procedures:

Acceptable Technology Use

Users of CCSS Technology must:

- Use resources supplied for purposes which are consistent with the business and mission of Community Connections Support Services and for authorized purposes only,
- Use the agency computing and information resources, including data, hardware, software and computer accounts, responsibly and appropriately.
- Protect your user identity, password and system from unauthorized use. All users are responsible for all activities on their user accounts or that originate from their devices.
- Respect the rights and property of others.
- Access only information that you own, that is publicly available, or to which you have been given authorized access.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
- Comply with all applicable federal, provincial, and local laws and CCSS policy.
- Comply with all contractual and license agreements
- Safeguard equipment and data entrusted to them
- Report incidents such as stolen laptops or passwords, or virus infections that are not automatically cleaned by resident anti-virus software. Any such activity must be reported immediately to the Service Coordinator or Directors.

Users of CCSS Technology must not:

- Use technology for any purpose which violates local, provincial or federal laws.
- Use the agency's systems or networks for personal gain; for example, by selling access to user identities or to agency's systems or networks, or by performing work for profit with agency IT resources in a manner not authorized by CCSS.
- Engage in unauthorized copying of information stored on the agency's IT assets.
- Use excessive computing resources, data storage or network bandwidth in activities such as the propagating of chain letters or broadcasting inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages or printing excessive amounts of paper.
- Access, send or store for retrieval patently harassing, objectionable or extremely offensive, intimidating, or abusive material. Such material includes but is not limited to racist material, hate literature, sexist slurs or sexually explicit material.

- Misrepresent your identity or affiliation while using CCSS IT resources.
- Use someone else's identity and password for access to IT resources, logging others into the network to access IT resources, or using the network to make unauthorized entry to other computational, information, or communications devices.
- Attempt to evade or crack passwords of systems on the network.
- Attempt to circumvent or subvert system or network security measures.
- Reproduce, download and/or distribute material protected by trademark, trade secret, or other intellectual property without appropriate authorization.
- Make or use illegal copies of copyrighted materials, software or movies, storing such copies on agency systems, or transmitting them over CCSS networks.
- Copy or modify files belonging to others or to the agency without authorization, including altering data, introducing or propagating viruses, Trojans or worms, or simply damaging files.
- Purposefully interfere with or disrupt another user's work or the proper functioning of IT resources.
- Intercept or alter network packets.
- Engage in any other activity that interferes with the work of other employees or the normal operation of the CCSS IT resources.

Agency-Issued Equipment

Agency-issued equipment is for CCSS employee use only. Depending on your role and location of your worksite, you will be assigned agency-issued equipment to use in performing your job. You are responsible both for the equipment issued to you and its use. Always exercise caution if leaving your equipment unattended. The agency retains ownership and reserves the right to add, remove, upgrade and replace hardware and software on those systems as deemed necessary. Employees must produce agency-issued equipment when requested.

When transporting agency-owned equipment, please be aware of your surroundings. Although the agency has taken steps to prevent data from being misappropriated or misused in the event of lost or stolen equipment, you should treat agency-issued equipment as if it were your own. CCSS does not back up data stored on mobile equipment. If you believe any of your agency-issued equipment has been lost or stolen, contact your Service Coordinator immediately.

Personal Use of Agency Technology

Employees assume responsibility for appropriate usage and are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use is defined as use that is not job related. In general, incidental and occasional personal use of the agency’s computing systems, including the Internet and email and printing of personal documents is permitted as long as the personal use does not interfere with the employee’s normal work duties, productivity, or work performance and does not adversely affect the efficient operation of the agency’s systems and networks result in significant financial loss. Individuals are expected to be careful, honest,

responsible, and civil in the use of computers and networks. Employees must respect the rights of others, respect the integrity of the systems and related resources, and use these resources in strict compliance with the law and agency policies.

Employees are ultimately responsible for any and all activity that originates from use of agency technology. CCSS takes no steps to maintain, retain, back up, or return personal data. As CCSS systems are subject to monitoring (see policy tp030 Technology Security), you should not store sensitive or confidential personal information on agency resources.

Use of Non-Agency Equipment

Generally, employees are expected to use agency-issued equipment for conducting agency business. This helps ensure the safety and security of the agency's network and information assets.

In cases where it is reasonable for an employee to use personal equipment to conduct business and access CCSS ESI , the employee may be given authorized and secured access to select agency systems and data. Procedures found in this policy and CCSS policy ol055 Confidentiality & Privacy apply to all CCSS ESI accessed through non-agency equipment.

References:

Bill & Melinda Gates Foundation. (2011). Technology Usage Policy. Retrieved May 7, 2020, from https://docs.gatesfoundation.org/documents/technology-usage-policy.pdf

Ontario Tech University. (2020). Technology Use Policy. Retrieved May 7, 2020, from https://usgc.ontariotechu.ca/policy/policy-library/policies/legal,-compliance-and-governance/information-technology-acceptable-use-policy.php

Ryerson University. (2018). Acceptable Use Information Technolgy Policy. Retrieved May 7, 2020, from https://www.ryerson.ca/policies/policy-list/acceptable-use-policy/

Trinity University. (2020). Responsible Information and Technology Use Policy. Retrieved May 7, 2020, from https://policies.trinity.edu/a8376318-ebd6-421f-be63-acf8c88376a1_a58a2cf3-1435-41fa-8a09-dfa6ad0758fd.html?v=50113

uOttawa. (2020). IT Resources Acceptable Use Policy. Retrieved May 7, 2020, from https://www.uottawa.ca/administration-and-governance/it-resources-acceptable-use-policy

For further information on this policy or permission to reprint, please contact:
Vivienne Prather
Director – Strategic Management
Community Connections Support Services
Unit 236
9-3151 Lakeshore Rd.
Kelowna, BC V1W 3S9
ph. (250) 491-2907 fx.1-866-728-2938
viv@commconn.ca
www.commconn.ca