Category: ITS Policy Policy No.: ITS-05-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 5 Effective Date: Feb. 7, 2024 Report No.: CPS-06-2024

Acceptable Use of Technology Policy

Purpose

To conduct business, Middlesex Centre provides access to technology in the form of hardware (such as laptops, workstations, and portable devices) and software (such as productivity tools). The purpose of this policy is to outline Middlesex Centre's expectations regarding the acceptable use of technology when using networks, email, internet, and all other technology and information systems.

Scope

This policy applies to Members of Council, all employees of Middlesex Centre including Paid-on-Call Firefighters and volunteers.

Definitions

"(ITS) Asset" means any physical electronic device owned by Middlesex Centre, which may contain or have access to sensitive information such as files and emails or has considerable value and is uniquely identifiable via a serial number or other means.

"Authorized Person(s)" means any employee, consultant or contractor of Middlesex Centre who has been approved by their respective department director under this policy.

"Bring Your Own Device (BYOD)" see "Personally Owned Mobile Device(s)" for further information.

"Confidential Information" is any and all information relating to the business and affairs of the Municipality and its assets which is not a matter of public record.

"Corporate Information" is any and all information in the control and custody of Middlesex Centre.

"Inappropriate Content" is content which (a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; (b) facilitates illegal activity; (c) depicts sexually explicit images; (d) promotes unlawful violence; (e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activity; or (f) causes damage or injury to any person or property.

"Information Systems" refers to computer hardware, software, data, security, user accounts, and the means in which they are interconnected.

"ITS" means Information Technology Services.

"Monitoring Tool" is an n application installed on a workstation, server, mobile device, or laptop which collects logs for the purposes of troubleshooting, data protection, or monitoring as defined under the Electronic Monitoring Policy.

"Personally Owned Mobile Device(s)" are any mobile devices which are owned and maintained by the Authorized Person and used for business purposes. These devices must adhere to the Mobile Device Security and Hardware Standards outlined in Cellphone and Mobile Device Policy.

Roles & Responsibilities

All members of Council and all employees of the Municipality of Middlesex Centre whether employed in a permanent, temporary or contract capacity, including full-time, part-time, casual, summer students, co-op students, and volunteers are responsible for the following this policy.

Department directors are responsible for ensuring that staff are aware of the policy and meet the standards set out in this policy.

Procedure

All staff of Middlesex Centre have access to Middlesex Centre's network and its services ("Information Systems") provided it is for business purposes. Occasional use of Information Systems for personal activities is allowed so long as it does not interfere with the security of the network, their productivity, or the productivity of other users of the network.

Middlesex Centre staff shall use technology in a manner that supports the organization, maintains the confidentiality of protected information, and ensures the integrity of all systems, servers, and networks of Middlesex Centre.

1. Privacy

Middlesex Centre respects the privacy of its employees. This privacy may not extend to an employee's use of technical resources provided by the Municipality, including internet and email. Middlesex County ITS will only actively review a user's email account or network history at the direction of the employee's department director and with approval from the Manager of Human Resources or Chief Administrative Officer as outlined in the Electronic Monitoring of Information Policy.

Middlesex County ITS staff may, through the course of approved regular support activities, come across information regarding staff activities defined under this policy (both real-time and

historical). In these circumstances, this data may only be used for the purposes of troubleshooting and supporting day-to-day activities of the organization.

2. Systems, Network, and Server Usage

a) Staff shall only access Middlesex Centre Corporate Information using technology which has been approved for this use by Corporate Services in collaboration with the Middlesex County ITS department.

b) An employee whose user account is used to access any Information Systems on the Middlesex Centre network is responsible for its acceptable use at all times.

c) Staff shall not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, the use of password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any Middlesex Centre ITS Asset.

d) Staff must consult with Middlesex County ITS prior to installing any software application, extension, or plugin on Middlesex Centre ITS Assets. Middlesex County ITS may, at its discretion, deny the request to install any application, extension, or plugin.

e) Staff shall not, in any way, attempt to gain access to Information Systems or any information that they have not been authorized to access.

f) Staff shall report any potential security risk or breach to Middlesex County ITS immediately upon learning of such a risk or breach.

3. Email and Internet Usage

Email and internet may be used to perform Middlesex Centre business-related activities.

a) Electronic communications shall not misrepresent the originator or Middlesex Centre.

b) Employees shall not use personal email accounts to send or receive Middlesex Centre confidential information.

c) Employees shall not use the email system (internal or external contacts) to engage in commercial, for-profit or personal mass mailing such as, but not limited to, fundraising, selling products, goods or services, or sending notification of upcoming events that are not business related.

d) Employees shall not download or store copyrighted material such as, but not limited to, songs, movies, books, or photos.

e) Staff should not intentionally access, create, store, or transmit material which the Municipality of Middlesex Centre may deem to be offensive, indecent, or obscene.

f) The internet may not be used to view inappropriate content, carry out malicious activities, break the law, or cause harm to others in any way.

g) Staff shall not use corporate email for personal use such as social media, banking, etc.

h) Staff shall not use TikTok on any municipally-owned device.

i) Staff must take care when using artificial intelligence (AI) software (e.g., ChatGPT, among others) to ensure confidential or sensitive information is not put into unsecure systems. Further, staff must review any outputs from AI software to ensure the accuracy and truthfulness.

4. Private and Confidential Communications

Middlesex Centre staff shall not send emails containing Confidential Information without taking the appropriate action to make it known that the email is private and confidential. To mark an email as private and confidential please follow the below steps:

a) At the top of the email in bold, capital letters put “PRIVATE AND CONFIDENTIAL”

b) At the bottom of the email body, add:

“Confidentiality Notice: The content of this communication, including the content of any accompanying attachments, is private and intended for the exclusive use of the intended recipient only. The content, including the content of any accompanying attachments may also contain information that is confidential, privileged and/or is exempt from disclosure pursuant to applicable law. If you are not the intended recipient, you are strictly prohibited from reading, using, disclosing, copying, or distributing this email or any of its content. If you have received this email in error, please notify the sender by reply email immediately (your_username@middlesex.ca) and permanently delete this email and its attachments along with any copies thereof. Thank you for your cooperation.”

5. Device Management

a) Staff shall not knowingly disable any software or system identified as a monitoring tool, mobile device management, or endpoint protection tool.

b) Corporate Services in collaboration with Middlesex County ITS may, at any time, ask staff to produce any device capable of accessing corporate information for review. The purpose of the review is to ensure the security of the device and Middlesex Centre’s network infrastructure.

c) Staff shall return any Middlesex Centre owned and provisioned device upon completion of employment with Middlesex Centre, unless prior arrangements have been made with the CAO and the Director of Corporate Services.

6. Documentation and Reporting

Staff shall immediately notify Corporate Services and Middlesex County ITS if an Asset is:

a) Moved to a new permanent location

b) Reassigned to a different staff member on a temporary or permanent basis

c) Damaged, compromised, lost, or stolen

7. Other Devices

All other Middlesex Centre ITS Assets, such as, but not limited to, computers, printers, phone system, audio/video and mobile devices shall be used in a respectful, professional manner to assist staff in carrying out Middlesex Centre business.

8. Compliance

Corporate Services and Middlesex County ITS enforce this policy and related standards. Anyone who has reason to suspect a deliberate and/or significant violation of this policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS and the Director of Corporate Services.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.