IT Security Policy

Procedure: IT Security			
Policy Number:	430.01	**CUSTODIAN:**	Special Projects
Approved Date:	11/17/2020		
Effective Date:	11/17/2020		
		REVIEW DATE:	11/2020
REFERENCES: WETCC Student and Employee Handbook Family Educational Rights and Privacy Act (FERPA), Telework policy			

Part 1. Policy Background and Purpose.

The computing resources at WETCC support the Anishinaabe educational, instructional, research, and administrative activities of the College and the use of these resources is a privilege that is extended to members of the WETCC community. As a user of these services and facilities, you have access to valuable College resources, to sensitive data and to internal and external networks. The purpose is for all users to understand the roles and responsibilities of the information systems of WETCC.

Part 2. Definitions.

Computer security incident is any adverse event where some aspect of computer security may be threatened, such as: misuse, damage, loss of data, loss of confidentiality, disruption of data or system integrity, or a disruption or denial of accessibility.

Electronic communication system includes e-mail, fax machines, telephones, and Internet use.

Information Technology ("IT" includes IT systems, IT infrastructure, and computer resources) includes, but is not limited to, computers, telephones, copy, and fax machines including related hardware and software and associated codes owned by WETCC.

Users means any individual who is a staff, student, or community member who is issued a login or password for a system within the WETCC IT infrastructure and/or any individual who used IT equipment of WETCC.

Telework is when an employee works from home or another location that is off campus.

Part 3. Responsibility.

The IT Coordinator has overall responsibility for the implementation of this policy and the accompanying IT Procedures.

The IT Coordinator is responsible to oversee the implementation and maintenance of WETCC's information systems, including security, up-to-date hardware and software, and compliance with this policy.

Users are responsible for the content of their personal use of the WETCC IT system and may be subject to liability resulting from that use.

All WETCC users are responsible to report any real or potential computer security incidents immediately to the IT Coordinator.

Part 4. Policy

Subpart A. Hardware and Software

Access to specific software packages of WETCC are restricted to employees who need the information to perform the duties of their job responsibilities.

Any hardware or software added to the WETCC IT infrastructure must be reviewed and approved by the IT Coordinator before being installed or used. Users are prohibited from downloading files from the Internet or installing software without the authorization of the IT Coordinator. The IT Coordinator will review the requirements, including licensing and ensure the software is suitable and compatible with WETCC IT infrastructure. WETCC prohibits all users from making, using, or transmitting illegal copies of copyrighted materials or pirated software on the WETCC IT system.

It is the policy of WETCC that any software used on IT equipment must be appropriately licensed; in addition, all licensing agreements must be adhered to by users, including copyright restrictions.

Subpart B. Security of System

WETCC has assigned the IT Coordinator the responsibility of protecting the IT infrastructure with appropriate firewalls and virus protection.

Users are not allowed to (or attempt to) decode passwords or access-controlled information; attempt to circumvent, subvert, or damage system security measures; or engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating computer viruses, disrupting services, or damaging, deleting, or destroying files.

Any breach (real or potential) with the IT system must be reported to the IT Coordinator immediately.

Subpart C. Acceptable and Unacceptable Use

Acceptable use of technology must be aligned with out Anishinaabe teachings, legal, ethical, reflect academic honesty and demonstrate restraint in the use of shared resources. Acceptable use must follow WETCC Code of Conduct, intellectual property rights, copyright policies, data system security mechanisms, individual rights to privacy (including FERPA) and free from acts of cyber bullying or unwarranted annoyance.

Acceptable Use

1. You may use only the computers, computer accounts, and computer files for which you have authorization.
2. You may not use another individual's account or attempt to capture or guess other users' passwords.
3. You are individually responsible for appropriate use of your computer, account and all resources assigned to you.
4. The college is bound by its contractual and license agreements respecting certain third-party resources; you are expected to comply with all such agreements when using such resources.
5. You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access.
6. You must not attempt to access restricted portions of the network, individual computers, or attempt to monitor network traffic without approval of the IT Coordinator.
7. You must not develop or use programs, software, or processes that disrupt other computer or network users, or that damage or degrade performance, software, or hardware components of a system.
8. You may use WETCC computers, laptops, printers, or other equipment to perform telework.

Unacceptable Use

1. Users may not use the campus computing or network services to transmit or display information which
    a) Violates or infringes on the rights of another person, including the right of privacy.
    b) Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
    c) Violates WETCC policy prohibiting sexual harassment.
    d) Restricts or inhibits other users from using the system or the efficiency of the computer systems.
    e) Uses the system for an illegal purpose.
2. Users may not illegally share or obtain copyrighted material
3. Users may not use computing and network services for uses that are inconsistent, incompatible, or in conflict with state or federal law or WETCC policy.
4. Users must respect the privacy of other users, including others digital property.
5. Users may not share their password with others or let others used their account.
6. Users must respect the intellectual property of others and adhere to College standards of academic honesty.
7. Users must not intentionally disrupt the campus computing system or obstruct the work of other users such as by interfering with the accounts of others, introducing or spreading viruses or other destructive programs on computers or

the network, sending chain letters or blanket e-mail messages, or knowingly consuming inordinately large amounts of system resources.

Subpart D: Access

Wireless Access
WETCC provides wireless network access on the WETCC campus for internet use only. Use of these Wi-Fi networks are covered by this computer use policy and acceptance of this is required for access.

Public Access
WETCC provides public access computing in designated areas only. Use of these public computers is subject to this computer use policy and all public users must comply with all requests and instructions from the IT Coordinator.

Subpart E. Rights and Responsibilities

Data transmitted via WETCC IT systems are not guaranteed to be private.

WETCC reserves the right to implement security measures, including but not limited to, the right to monitor any use of the IT system. It is the responsibility of the data owner to identify information security requirements needed on the IT system to protect the integrity of the data they are responsible for.

WETCC is not responsible for any personal or unauthorized use of its IT system or the security of personal data or devices on or using the IT system.

WETCC reserves the right to restrict or prohibit any use of its IT system by any user without notice.

Any user who knows of or reasonably believes that a breach of this policy has occurred must immediately report to their applicable Cabinet Member who will promptly notify the It Coordinator.

Violations of this policy are considered misconduct under applicable student and employee conduct standards. Users who violate this policy and/or the accompanying procedures may be subject to other penalties, including disciplinary action.

Suspected legal violations will be referred to the appropriate law enforcement agency.

The IT Coordinator is responsible to keep a log of all equipment that is assigned to an employee.

Subpart F: Academic Freedom

Nothing in this policy or the accompanying procedure shall be interpreted to expand, diminish, or alter academic freedom.

Subpart G: Lost or Stolen Devices

The loss of a WETCC IT system or device shall be reported to the applicable Cabinet Member and the Security Coordinator within one business day. Any item that has been classified as an asset by the Finance Department must also be reported to the CFO.

When an employee-owned device containing WETCC data is lost or stolen, it is important to take steps to protect the security and privacy of the data. Employees must promptly report a lost or stolen device to their Cabinet Member who will report the incident to the Security Officer. The employee will be asked to cooperate in an investigation and wiping the data from the system if necessary.

Subpart H: Damage to Equipment

Employees will be responsible to report any damages that are due to employee misuse that is above and beyond normal wear and tear.