Policy Series 1100

INFORMATION TECHNOLOGY

Policy Series 1100: Information Technology

Nisichawayasihk Education Authority's Information Technology Policy provides the operational detail required for the successful implementation of a safe and efficient computer network environment for Alice Moore Education Centre (AMEC), Otetiskiwin Kiskinwamahtowekamik School (OK School) and The Nisichawayasihk Neyo Ohtinwak Collegiate (NNOC). It has been developed based on understanding the educational and administrative needs of the schools and an evaluation of the existing technical configuration and requirements.

Effective security is a team effort involving participation and support from every Authority employee and associate who deals with information and/or information systems. Every computer user is responsible to know these guidelines, and to conduct their activities accordingly.

Policy 1101: Computer Use

The Authority has directed the Information Technology (IT) department to develop this policy to ensure fair and reasonable use of Authority computing facilities and services, and to establish a framework for consistency in professional practices and processes.

The term "facility" includes, but is not limited to: network devices, routers, switches and other supporting devices; computers, whether networked or stand-alone; networks, whether wired or wireless; software; systems; and gateways used to access external networks such as the Internet and the World Wide Web. IT "services" include: e-mail, file storage, portals and other web services, web page hosting and others.

Guidelines & Procedures

1. The Authority provides computing facilities and services to support the business of Alice Moore Education Centre (AMEC), Otetiskiwin Kiskinwamahtowekamik School (OK School) and The Nisichawayasihk Neyo Ohtinwak Collegiate (NNOC), including teaching, learning, research /artistic work and administration.
2. All staff and students are entitled to use Authority computing facilities and services for which they have authorization. A computer account will be used to access these facilities and services will. The Authority may withhold or withdraw this entitlement with cause.
3. Use of all Authority computing facilities and services is subject to this policy and whether the account holder is accessing facilities and services both within and outside the Authority's intranet domain.

A. Scope

This policy governs the appropriate use of all computing facilities and services owned and operated by the Authority, including those acquired through donation or through some contractual agreement (such as, lease contract) by the Authority. It covers all Authority-owned computing facilities and services regardless of where they are located or from where they are being accessed (within the Authority intranet domain or outside the Authority intranet domain).

B. Policy

The Authority provides staff and students with computing facilities and services, to be used in conjunction with their duties or educational activities. The Authority may also provide services to others with whom it does business, including but not limited to visitors, contractors and third-party service providers. Everyone who uses Authority computing facilities and services must comply with this policy. Access may be withheld or withdrawn with cause.

Access to the Authority's computing facilities and services is provided through an account issued to each individual. No one is authorized to use any Authority computing facility or service without such an account. Computer accounts and authorization are not transferable. The person to whom authorization is granted is responsible for all use of that account and is expected to take reasonable steps to secure the account.

Under certain circumstances shared account are permitted (school lab use and AMEC visitors), but individuals using a shared account carry the same responsibilities as they are using a unique account.

Authority computing facilities and services do not support any personal purposes. The Authority is not responsible for any personal loss caused by using Authority computing facilities and services but reserves the right to take all necessary further steps to sue and to charge the damage to Authority computing facilities and services caused by personal use.

Users are not allowed to use Authority computing facilities and services for personal purposes if the personal use may compromise the business of the Authority, may increase the Authority's costs, may expose the Authority to additional risk, may damage the Authority's reputation or may be part of an activity that the account holder does for personal profit.

Users should not by design or any chance bring media, including but not limited to USB drives, CD/DVD, and files sent through Internet, to jeopardize Authority computing facilities and services.

File downloading is restricted and is only allowed from certain trusted websites for educational purposes and Authority business needs.

Users should not by design or by any chance change configurations of Authority computing facilities and servers. Neither should they take any chances to bypass or override Authority IT security settings.

Unless authorized, the right of software installation is limited to Authority IT department personnel.

Access to information on the Internet is governed by Canadian and provincial laws relating to copyright, privacy, information confidentiality and community standards. Use of the Internet to transmit material that violates any applicable law, regulation or policy is prohibited.

The use of computer facilities and services may be monitored. This may include, but is not limited to, gathering data for diagnosing service problems, capacity planning, service enhancement planning, and investigating violations of this policy, other policies, regulations or laws.

The Authority reserves the right to adjust configurations and customaries settings of its computing facilities and services to meet its needs and to improve IT security without further notice.

C. Privacy

A user's reasonable expectation of privacy is subject to the Authority's right to examine systems, directories, files or usage logs if there is reason to suspect violation of this policy, other Authority policies, or of other regulations and laws.

D. Responsibilities of Account Holders

The account holder is responsible to:

1. Comply with all laws, Authority policies, regulations and guidelines regarding use of Authority computing facilities and services.

2. Use Authority computing facilities and services in a responsible manner and ONLY for purposes for which use has been authorized. Resources are not to be wasted nor used in such a way as to deny or restrict access to others.
3. Abide by the security measures and restrictions in place.
4. Respect the policies of external networks and remote sites.

E. Responsibilities of Service Providers

The Director of Education, Principals, Department/Unit Heads and teachers are individually and severally considered the custodian of all computing facilities and services under their jurisdiction and must take reasonable steps to ensure those using the facilities and services are aware of applicable policies and abide by them.

Those responsible for maintaining any Authority computing facility are responsible for ensuring institutional standards for security, data backup, user authentication and access control are appropriately applied.

Policy 1102: Network Security

The Board believes the Authority's network is a shared resource critical to teaching, learning, research, Education Authority operations and service delivery. The Network is critical to Authority communications, which includes data, text, voice and video.

Guidelines

The purpose of this policy is:

1. To help ensure the reliable operation of the Authority Network so that staff, students, and other Authority members have access to the network resources they require.
2. To help reduce the Authority's liability and risk of litigation due to inappropriate or illegal use of the Authority Network. Such use includes but is not limited to distributing materials protected by copyright, illegal materials, confidential information and personal information.
3. To help protect the Authority's reputation from harm resulting from inappropriate or illegal use of the Network.
4. To define the responsibilities with respect to IT security of Network users

A. Principles

The Network is a critical Authority resource.

1. Everyone who uses the Network has a role in maintaining a secure network and computing environment, including students, teachers, staff and authorized guests.
2. Network users have a reasonable expectation that their communications are private. This privacy is subject to the Authority's legal obligation for disclosure and its business requirement to ensure a reliable Network service and to protect its users.

B. Scope

This policy applies to the Network at all Authority locations (AMEC, OK school and NNOC). The Network encompasses wired and wireless network connections in classrooms, offices, libraries, student computing facilities, laboratories, teacherage areas and other Authority locations. It includes connections to

external networks such as provincial, Canadian, and international and educational networks as well as the Internet.

This policy applies to all members of the Authority's community and authorized guests of the Authority:

1. Who connect network-capable devices to the Network (wired or wireless) within the Authority's intranet domain;
2. Who access resources or services located on the Network from outside of the Authority's intranet domain (their home or anywhere else on the Internet).

A **network-capable device** is any device that can connect to the Network with either a wired or wireless connection. Network-capable devices include, but are not limited to, routers, switches, desktop computers, laptop computers, tablet computers, printers, copiers, servers, personal digital assistants, cameras, security system equipment, robots, teaching equipment and VoIP phones.

This policy governs the IT security practices for any and all network-capable devices that use the Authority's Network regardless of whether the devices are personally owned or owned or leased by the Authority.

The policy has been developed in the context of, and is designed to complement existing Authority policies and guidelines, particularly the Computer Use Policy and policies governing the use of Authority property and services, privacy, security and copyright.

C. Policy

Students and staff are only authorized to connect network-capable devices of an approved type to the Network. The Director of Education and IT Department may extend this authorization to guests on a temporary basis if they judge that doing so supports the Authority's mission, but in so doing the guests assume responsibility for their behaviour.

The Authority's intranet domain is a highly professional business environment. Students, visitors and staff should not connect any personal network-capable

devices to the Authority's Network without authorization. Authorization and access to the Network may be withheld or withdrawn with cause.

Only approved devices and device configurations may be connected to the Network. Information about, and configuration requirements for approved devices will be maintained and provided by the Authority's IT Department. Equipment that does not comply with these requirements may not be connected to the network. Exceptions to these requirements may be authorized to meet the academic needs of OK School and NNOC.

Activities that interfere with the reliable operation of the Network are prohibited. These include, but are not limited to: operating network-capable devices that attack or compromise other network-capable devices, users of the Network and the Network itself; operating wireless access points, cordless phones and other devices using the unlicensed radio communications spectrum; and impersonating or interfering with Network equipment or Network services. Devices that interfere with the Network may be disconnected and/or removed and the user's access to the network may be suspended.

Scanning and mapping the Network, as well as monitoring Network traffic, are prohibited unless authorized by the IT Department. Units are authorized to scan and monitor only the equipment they are responsible for maintaining, subject to this activity not interfering with the Network or others' use of the Network.

The IT Department may scan devices connected to the Network for security issues and vulnerabilities. Network traffic may be monitored to help ensure a reliable Network service and to protect Network users. Devices suspected to be in violation of this policy may be disconnected from the Network.

D. Responsibilities

Guests of the Authority, who are authorized to connect network-capable devices to the Network, are also responsible for ensuring that those devices meet the Authority's Security Requirements.

Members of the Authority's community who authorize guests to connect to the Network are responsible for making them aware of this policy and their obligations under this policy.

Users of the Authority's Network must:

1. Use Authority computing facilities and services in a responsible manner and only for the purpose for which use has been authorized. Resources are not to be used in such a way as to deny or restrict access to others
2. Report any suspicious activities, behaviour and incidents which violate Authority policies and which may jeopardize the Authority's Network
3. Comply with all Authority policies, regulations and guidelines regarding use of Authority computing facilities and services, including the Computer Use Policy
4. Respect the policies of external networks and remote sites.

Comply with all laws.

The IT Department is responsible for designing, implementing and managing the Network and maintaining efficient and effective operation. This includes:

1. Monitoring the Network (wired and wireless) to help ensure reliable performance as well as to detect unauthorized activity, intrusion attempts or other security risks
2. Scanning the Network and network-connected devices to detect vulnerabilities and compromised equipment
3. Disconnecting devices that are not compliant with this policy or do not meet the Authority's IT Security Requirements
4. Blocking some forms of Network traffic to reduce the damage caused by viruses and other Internet-based attacks
5. Managing the allocation of the Network resource when users' needs for Network service conflict or when the capacity of the Network is insufficient to meet the needs of all users.

The Director of Education may authorize exceptions to the *Approved Devices and Configurations Requirements* to meet specific needs of Authority business.

Policy 1103: Email

The Board believes the purpose of an email policy is:

1. To define acceptable use of Authority email
2. To outline user responsibilities
3. To establish guidelines for effective practices and processes.

Guidelines

1. The Authority's email system is an important part of The Authority's information technology services infrastructure and a mission-critical service..
2. E-mail is a medium for the exchange of information within the Authority's community and other parties associated with the Authority. Service will be provided and maintained centrally.
3. All teachers, administrative staff and other authorized staff are entitled to email services accessed through a centrally provided computer account. The Authority may withhold or withdraw these services with cause.
4. The Authority uses email as an official communications tool.
5. The Authority email address is the official electronic mailing address for all staff. The account holder is responsible for reading and attending to email sent to this address. The Authority will not collect, store or maintain information on other accounts.

A. Scope

This policy has been developed in the context of, and is designed to complement existing Authority policies and regulations, particularly those governing computer use; data management, access and use; privacy; copyright; and intellectual property.

B. Policy

The Authority will normally provide email services to all teachers and administrative staff, to be used in conjunction with their duties or activities. The Authority does not provide email services to students, educational assistants (EA), hallway monitors, and cleaning staff. Service to any account holder may be withheld or withdrawn with cause.

The email address is the property of the Authority. Email accounts will be

withdrawn for staff no longer working for the Authority. The Authority is not responsible for the loss of all information stored in that email account.

The content of email messages sent using any Authority account and/or stored on any Authority server is subject to the Computer Use policy.

All account holders have a responsibility to ensure they conduct email exchanges with professionalism and courtesy, and manage their email responsibly.

Use of invalid or forged "From" addresses or any other attempt to misrepresent the identity of the sender will be considered a violation of this policy.

Inappropriate or offensive emails, emails containing viruses, spam, or malicious codes, or emails that are threatening, discriminatory, harassing or obscene, must not be sent or forwarded, except as requested in making a complaint of inappropriate or offensive emails.

Staff may use Authority email services for personal purposes, with the understanding that all messages stored on Authority servers are considered to be Authority records. The Authority reserves the right to copy, delete and forward any information stored on Authority servers.

Acceptable personal email use will not compromise the business of the Authority, will not increase the Authority's costs, will not expose the Authority to additional risk, will not damage the Authority's reputation and will not be part of an activity the account holder does for personal profit.

C. Privacy

A user's reasonable expectation of privacy is subject to the Authority's right to access e-mail records, including those that have been deleted by the account holder but which may not yet have been deleted centrally, where there is determined to be a clear business need. This need may relate to the need for business access in the absence of an employee, a request under the Local Authority Freedom of Information and Protection of Privacy Act, or to recover evidence while investigating allegations of misconduct and managing actual or

potential criminal or civil litigation in which the Authority is or may become a party.

Wherever practical, employees will be notified promptly when their e-mail records have been accessed.

D. Responsibilities of Account Holders

The account holder is responsibile to ensure email received at his/her official address is attended to in a timely manner. The account holder may forward the email to be read at another account but the Authority assumes no responsibility for delivery to an off-domain account.

Since the email bears identification marks of the Authority, account holders are expected to treat emails in the same manner they would use Authority letterhead, and to ensure that all communication is carried on in a professional, respectful and courteous manner.

Policy 1104: Data Management

This purpose of Data Management is to provide a common basis of understanding of data as a business-critical Authority resource, and responsibilities of using the Authority data resource by all students of OK School and NNOC and all members of the Authority.

Guidelines

The Authority's data resource covers all information stored on servers, computers and other electronic and non-electronic information including any forms of records, reports, files, documents and profiles. It is one of the Authority's most valuable assets. The Authority's data-management policies, procedures and practices are designed to safeguard three vital aspects of data: integrity, security, and accessibility.

1. Data *integrity* includes qualities of accuracy, consistency, and timeliness. Data integrity begins with the person or office creating the data, and is the continuing responsibility of all who subsequently access and use it.
2. Data *security* encompasses all means to ensure data is protected from corruption and leakage. Data must be safeguarded at all levels against damage, loss, and breaches of security with all who use it sharing this responsibility.
3. *Accessibility* to Authority data is granted internally when a legitimate business or educational need for the data is demonstrated, and externally when release of such data would not violate the Authority's stewardship obligations, privacy legislation, or legal contracts.

A. Scope

This policy has been developed in the context of, and is designed to complement existing Authority policies and regulations, particularly those governing computer use.

B. Policy

Data users must carry out all tasks related to the creation, storage, maintenance, cataloguing, use, dissemination and disposal of Authority data responsibly, in a timely manner and with the utmost care.

Data users must not knowingly falsify data, delete data that should not be deleted or reproduce data that should not be reproduced.

Data users must respect the privacy of individuals whose records they may access. No subsequent disclosure of personal information contained in files or databases may be made. Disclosure is understood to include (but is not limited to) verbal references or inferences, correspondence, memoranda and sharing of electronic files.

Data must be stored in such a way as to ensure the data is secure and access is limited to authorized users. Secure storage of Authority data is a joint responsibility of network administrators, administrative staff and the data users who must ensure that passwords and other security mechanisms are used.

C. Responsibilities of Data User

The user is responsible to confirm the accuracy and safety of data before uploading to Authority servers or spreading within the Authority network.

The user is responsible to back up and secure personal data associated with their accounts including email, passwords and files stored in computers.

Data users should report any suspicious activities which may jeopardize the integrity, security and accessibility of the Authority's critical data assets.

D. Responsibilities of the Authority's IT Department

The IT Department will back up data stored on Authority servers and library databases in a timely manner and will test the ability to restore data from backup on a timely basis.

The IT department's duty is to ensure the accessibility of data to authorized personnel. However, the IT department is not responsible for the loss of information stored in individual user accounts.

Policy 1105: Awareness of the Policy

The existence of this policy will be communicated to all computer account holders at the Authority. New account holders will be informed at the time access to facilities is given.

Policy 1106: Non-Compliance

The Board believes Authority employees are individually liable for any and all damages incurred resulting from violating the Authority's IT policy, copyright, and licensing agreements.

Guidelines

If there is reason to suspect that laws or Authority policies have been, or are being violated, or that continued access poses a threat to a facility, other account holders, normal operations, or the reputation of the Authority, access privileges of any individual may be withdrawn or restricted.

Following due process, the Authority may take one or more of the following actions against anyone whose activities violate the law or this policy:

1. Restrictions or loss of access to any or all of the computing facilities and services at the Authority.
2. Legal action that could result in criminal or civil proceedings.
3. In the case of students, disciplinary action under the Council regulations for Student Academic Dishonesty and/or Non-Academic Student Discipline and Appeals.
4. In the case of employees, disciplinary action up to and including dismissal.

Policy 1107: Personal Electronic Devices

The Board believes that because of potential for disruption to teaching and school activities, clear regulations need to be in place regarding unauthorized use of all Personal Electronic Devices on school grounds.

Guidelines

Personal Electronic Devices include, but are not limited to laptops, netbooks, tablets, cell phones, personal digital assistants, MP3 players and IPods, digital cameras and electronic game devices.

As with all personal property, the school is not liable for damage to or loss of such devices and the onus is on students to adhere to this policy to ensure the responsible use and safekeeping of their property.

A. Policies

All students in possession of Personal Electronic Devices on school grounds must adhere to the following policies:

1. Students may not connect any unauthorized Personal Electronic Devices to the school's internal network.
2. Students may not capture unsolicited audio, video or photographs on school property.
3. Students may not post without express permission any audio, video, or photographs captured on school property that involve any students, teachers or other staff to personal or public sites such as YouTube, Flickr, Tumblr, Picasa, Facebook, Twitter, blogs, etc..
4. Accessing personal or public social media sites such as Facebook, Twitter, blogs, etc. and participating in any aspect of email, texting or electronic note passing is not permitted on school property.
5. Cell phones must be turned off and not used for receiving or communicating while on school property. This rule applies to both students and staff.
6. Ringtones, alerts, and other audible notifications for communication devices must be muted at all times while on school property.

B. Penalties

Failure to comply with these polices will result in the following penalties:

1. **First Offense** – The first offense will result in the offending device(s) being confiscated and taken to the office. The student will be able to reclaim the device at the end of the school day.
2. **Second Offense** – The second offense will result in the offending device(s) being confiscated and taken to the office. The device(s) shall remain in the school's possession in accordance with Authority policy. The student's parent/guardian must schedule an appointment to speak to an administrator to review the Personal Electronic Device Policy. The offending devices(s) may be returned to the parent at that time.
3. **Third and Final Offense** – The third and final offense will result in the student no longer being permitted to have such devices on school grounds at any time. All personal electronic devices (such as MP3 players, cell phones and Nintendos) will be immediately confiscated and held in the office in accordance with school policy until an agreement is reached with the parent/guardian to pick up the devices in person. Further disciplinary action for the student may result at the school's discretion.