Administrative Procedure 140

ACCEPTABLE EDUCATION AND INFORMATION TECHNOLOGY USAGE

Background

The Division recognizes and supports that the use of computers, telecommunications, wireless devices, cloud and networked services provides staff, students and the community with unique and powerful ways to enhance teaching and learning.

Definition

For the purposes of this policy, the term "network" shall refer to the physical infrastructure as well as all other devices and services (hybrid cloud services, switches, routers, printers, servers, backup devices, wireless devices, IoT devices, BYOD etc.) connected to it.

Guidelines

Use of Information & Education Technology (ET/IT) and networks

1. Purposeful use of ET/IT technology and networks:
   - 1.1. All students will have access to and use technology to enhance learning across the curriculum.
   - 1.2 All teachers will have access to and use technology to enhance teaching, planning, assessing, reporting, and personal/professional development.
   - 1.3 All schools and central services departments will use appropriate technology to enhance planning, communicating, financial management, and the flow of information.
   - 1.4 Services will be available to assist schools and services departments in formulating and implementing plans for technology.
   - 1.5 All schools and central services departments will plan effectively for technology integration and technology change.

2. Division ET/IT technology must be used in ways that are consistent with the following principles:

   2.1 Inappropriate Use

   Inappropriate use would include any activity that could compromise one's position as a representative of the school and/or school division. Division technology is intended for educational purposes and for business purposes in the operation of schools and the Division. Personal use of electronic communication must not interfere or conflict with its use for work purposes. Division technology cannot be used for purposes that are illegal, unethical or immoral.

   2.2 Privacy and Personal Safety

   Activities involving Division technology will, as much as possible, protect the privacy of personal information of all users and the personal safety of students. All users will be educated about ways that they can protect their own personal information and personal safety. Section 34 of the FOIP act requires us to protect personal information that is in our custody or control by making reasonable security

arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. The use of key logging software and any similar software which compromises the privacy of an employee or student is expressly prohibited. Staff using laptops must take steps to secure the data contained on the laptop. NLPS ET/IT Services will either implement or suggest software that encrypts the data for the purpose of reasonable protection from risk of loss.

In addition, students are forbidden to use a staff or NLPS business related computer or device due to the nature of the sensitive personal, learning or business related data that could be stored on the device. Staff are to ensure that their computer systems and devices are secure at all times; are used only by themselves or other approved users, and that passwords are not shared at any time.

2.3 Security of Systems and Information

Individuals using Division technology or other personal owned devices shall not compromise the security and integrity of data, and information stored on Division or school computer systems and devices. Individuals shall not attempt to compromise the network with Division Technology or personal devices on the network.

2.4 Network Etiquette

- Be polite. Do not get abusive in your communications to others.
- Use appropriate language. Do not swear, use vulgarities, or other inappropriate language.
- Do not engage in activities prohibited under municipal, provincial or federal law.
- Do not reveal your or any other person's personal information (home address, phone number, passwords, photos).
- Do not reveal any passwords assigned to you.
- Electronic mail (email) is not private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities and will result in loss of user privileges.
- Use the network and the internet in such a way that you will not disrupt the use of the network by other users.
- If you see a security problem on the network, report it to a system administrator.

2.5 NLPS Cloud Services

Cloud services within NLPS are an extension of learning, productivity and communication tools outside of the classroom. The same policy, security of information, acceptable usage and etiquette standards that apply to internal NLPS network services also apply to NLPS Cloud Services.

2.6 Social Media

NLPS has a comprehensive social media procedure established, AP151. All of the procedure in the AP140 applies to the AP151. As well any procedure set forth in the AP151, applies to the AP140, as they both involve the use of technology and communication.

Procedures

1. Staff will blend thoughtful use of educational technology, electronic information and research skills throughout the curriculum from a pedagogical perspective while providing guidance and instruction to students in the appropriate use of such resources.
2. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway.

   2.1 General school rules for behavior and communications apply on networks that are often public in nature.

   2.2 The network is provided for students for educational purposes, to conduct research and communicate with others.

   2.3 Access to network services will be provided to students who act in a considerate and responsible manner.
3. All users, staff, students and volunteers, will be responsible and accountable for their use of Division technology. Due to network maintenance and performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review.
4. Schools will request that students and their parents or guardians sign an appropriate use agreement (F140-1) that confirms their understanding of school and Division guidelines and procedures. The network is provided for students for educational purposes. Independent access to network services is provided to students who agree to act in a considerate and responsible manner. Access is a privilege and entails responsibility.
5. Schools will request that all staff and volunteers annually review the Employee and Volunteers Acceptable Use of Technology guidelines F140-2. The network is provided to staff and volunteers to enhance business, teaching, planning, accessing, reporting and personal/professional development.
6. The Superintendent expects staff to communicate with parents and guardians regarding independent student access to technology. Such communication shall include making available educational opportunities for parents and guardians to view, first hand, the technology being utilized. A discussion of expectations staff have for students when students work independently with electronic information resources will then ensue.
7. Cloud services allow the extension of some NLPS resources beyond the classroom. As a result of this, parents are encouraged to emphasize digital citizenship best practices, and other social media safe practices to ensure the safety of students while using personal internet and digital devices to access school and personal information resources.
8. Staff will provide developmentally appropriate guidance and instruction to students as they make use of technology and electronic information resources to conduct research and other studies related to the Division curriculum.

9. All students will be informed by staff of their responsibilities as users of the Division network prior to gaining access to that network, either as an individual user or as a member of a class or group. Methods of informing students may include combinations of assembly announcements, class lessons, and newsletters.
10. Staff may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that stored files will be private.
11. Extra care is required when using computer equipment that is equipped with built-in cameras. Users may not take pictures, publish, store or transmit pictures when doing so would constitute a violation of privacy in accordance with the Freedom of Information and Protection of Privacy Act.
12. While the Division feels that the network has great potential as an information source and communication tool and should be used in a variety of ways, the following are not to be permitted:

    - Accessing inappropriate websites (obscene or threatening material, written or pictorial, including but not restricted to material which contains or promotes pornography, racial supremacy or ethnic hatred or violation of human rights)
      ** The IT department recognizes that accidental access may occur, however, this is clearly evident by the user's actions in backing out of site and entry into correct site.
    - Sending or displaying messages or pictures that contain profanity, vulgarities, or any other inappropriate language, including sexual, racial, religious or ethnic slurs, or any abusive, threatening or otherwise offensive language.
    - Posting personal information including photos or videos without the owner's consent.
    - Obviously harassing, insulting or attacking others
    - Damaging computers, computer systems or computer networks
    - Vandalism of accounts or systems including hardware
    - Violating copyright laws
    - Using others' passwords or sharing passwords with anyone besides a staff member
    - Trespassing in others' folders, work or files
    - Intentionally wasting limited resources
    - Playing network intensive games, or using IRC (Internet Relay Chats)
    - Downloading or uploading unauthorized, excessively large files (greater than 2GB capacity)
    - Subscribing to inappropriate newsgroups
    - E-mail or newsgroup correspondence inappropriate to educational purposes
    - Any activity posing potential risks to oneself or to others
    - Harassing other users (e.g., with unwanted e-mail messages)
    - Illegal activity
    - Activities that would violate school handbook policies

- Failure to report known security problems
- Any other inappropriate use or misuse of the system
- Employing the network for commercial purposes
- Making purchases that charge back to the system.

13. Responsibilities for Staff members or volunteers who supervise students using technology:

    13.1 A staff member is required to be present and be able to provide adequate supervision when any student is using the internet.

    13.2 All student use of the internet must be authorized by an NLPS educator.

    13.3 As a part of all internet lessons and periodically during other technology lessons, acceptable use of technology should be reviewed.

    13.4 All students must have a signed NLPS Acceptable Use Agreement form on file at their school before they can access any technology.

    13.5 Due to limits of bandwidth, security and privacy issues, activities must be limited to those activities that directly support the instructional process and are a part of approved lesson plans.

    13.6 Staff who observe a student violating the NLPS Acceptable Use Agreement form must report the student to the school administration.

    13.7 Students and Volunteers using personally owned devices, and or BYOD, on school property utilizing NLPS network services or their own personal network service, are expected to abide by the AP140.

    13.8 Staff have the same responsibility to be present and provide adequate supervision for personally owned devices and or BYOD.

14. The Division expects violations of the above and other inappropriate technology uses will result in sanctions.

    14.1 Inappropriate use shall result in denial of device, network and service privileges (temporary or permanent).

    14.2 Additional disciplinary action may be determined at the school level in line with existing practice regarding inappropriate language or behaviour.

    14.3 Inappropriate use of network and service privileges may result in exclusion from a computer course option.

    14.4 When applicable, law enforcement agencies may be requested to become involved. Criminal prosecution as detailed in the computer crimes provisions of the Criminal Code of Canada.

Reference: Section 60, 61, School Act

Definitions:

IoT Devices: The “Internet of Things” devices, which could include but is not limited to wireless or wired media boxes, streaming media devices (google Chromecast, Apple Airplay etc.), building automation devices (SCADA), automated environment assistants (Google Home, Apple HomePod), automated task devices (internet connected fridges, coffee makers etc.)

G-Suite: Formerly Google Apps for Education (GAFE). A Google Cloud hosted set of Applications and Services such as a Word processor, spreadsheet, presentation maker etc. for use by students and staff to enhance education and business productivity.

BYOD: Bring your own Device.

Northern Lights PUBLIC SCHOOLS	STUDENT ACCEPTABLE USE OF TECHNOLOGY GUIDELINES AND AGREEMENT	**F140-1**

INTRODUCTION AND GENERAL INFORMATION FOR PARENTS AND STUDENTS

Northern Lights Public Schools provides students with access to computers, devices, educational technology, cloud services, network services and the Internet to support and enhance learning and teaching.

Electronic communication is a tool for life-long learning, and responsible use will allow students to expand their knowledge by accessing and using information resources, and by analyzing, collaborating and publishing information.

All users must assume responsibility for understanding the Student Acceptable Use of Technology Guidelines as a condition of use. Use of division resources in a manner inconsistent with these guidelines may result in loss of access as well as other disciplinary or legal action.

ACCEPTABLE USE AND BASIC PREMISES

At all times, students are to demonstrate the highest level of respect for all division technology resources. Students shall use these resources in a safe, responsible, efficient, ethical and legal manner in accordance with all school and division rules, regulations and guidelines.

Students shall promptly disclose to their teacher or system administrator any exposure to inappropriate material or anything that makes them feel uncomfortable.

Students shall immediately notify their teacher or system administrator if they have identified a possible security problem.

Students shall use the system ONLY for educational or curriculum related activities. Additional freedoms and limitations may be imposed by the school or by the division administration.

WHEN USING TECHNOLOGY, CLOUD OR NETWORK SEVICES, ALL STUDENTS SHALL CONDUCT THEMSELVES IN A MANNER WHICH MAINTAINS THE SAFETY, POSITIVE REPUTATION AND DIGNITY OF THE DIVISION AND ITS SCHOOLS.

UNACCEPTABLE USE

Students should be aware that their personal files may be accessible under the provisions of the Freedom of Information and Protection of Privacy Act. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating acceptable use guidelines or the law. An individual search will be conducted if there is reasonable belief that a user has violated the law or the division's acceptable use guidelines. The division has the ability to see specific users accessing specific sites through the use of our monitoring software.

The following uses of any division electronic resources are unacceptable and may result in suspension, removal from network and cloud services, disciplinary or legal action. Unacceptable use is defined to include, but not limited to, the following:

- Violation of school or division rules, policy, guidelines and agreements.

- Transmission or access of any material in violation of any local, provincial, or federal law. This includes, but is not limited to: copyrighted materials, threatening or obscene material, personal information protected under FOIP or material protected by copyright or trade secret.

- The use of profanity, obscenity or other language that may be offensive to another user.

- Any form of vandalism, including but not limited to, damaging computers, computer systems or networks, and/or disrupting the operation of the network.

- Copying and/or downloading commercial software or other material (e.g. music) in violation of federal copyright laws.

- Unauthorized downloading or uploading of large amounts of data.

- Plagiarism (taking from others' ideas, writings, graphics or other creations and presenting them as if they were original).

- Use of the network for financial gain, commercial activity or illegal activity

- Use of the network for political activity.

- Use of the network to access pornographic or obscene material.

- Creating and/or placing a computer virus on the network.

- Providing your network ID and password to anyone other than the system administrator. You are responsible for maintaining your own password and account security.

- Accessing another person's account or any other computer system or resource on the network that goes beyond your authorized access. Students will not go looking for security problems as this may be construed as an attempt to gain illegal access.

Northern Lights Public Schools

Student Acceptable Use Agreement
(Grades 3-12)

School _____ Student ID# _____

Student Name _____ Grade _____

STUDENT SECTION (* To be signed yearly)

I have read the acceptable use guidelines. I agree to follow the rules contained in these guidelines. I understand that if I violate the rules, my account can be terminated and I may face other disciplinary measures.

*** Student Signature**: _____ **Date**: _____

PARENT OR GUARDIAN SECTION (Grades K-12) * to be signed yearly

I have read the acceptable use guidelines and have discussed them with my child.

I understand that access to computers, smart devices and network services is for educational purposes. I will instruct my child regarding acceptable use, including that which is set forth in the acceptable use guidelines. I will emphasize to my child the importance of following the rules for personal safety.

I acknowledge that my child (and the parents by extension) will be responsible for any financial costs involved should my child be responsible for damage to any network services, computer, smart device or related equipment that belongs to Northern Lights Public Schools.

I hereby release Northern Lights Public Schools and its personnel from any and all claims and damages arising from my child's use of, or inability to use, the Northern Lights Public Schools network services, cloud services, computers, smart devices and systems.

I give permission to allow Internet access for my child and certify that the information contained in this form is correct.

***Parent/Guardian Signature _____ Date_____**

***Parent/Guardian Name _____ Phone _____**

Northern Lights PUBLIC SCHOOLS	EMPLOYEE and VOLUNTEERS ACCEPTABLE USE OF TECHNOLOGY AGREEMENT	**F140-2** *To be distributed to all Employees and Volunteers*

INTRODUCTION AND GENERAL INFORMATION FOR EMPLOYEES AND VOLUNTEERS

Northern Lights Public Schools provides employees and volunteers with access to computers, devices, educational technology, cloud services, network services and the Internet to support and enhance learning and teaching.

Northern Lights Public Schools relies on networked computers and the data contained within these systems to achieve its missions and to support business practices. The Acceptable Use Policy is to protect these resources in accordance with provincial law and Northern Lights Public Schools rules. All individuals granted access to Northern Lights Public Schools technical resources must follow the acceptable use outlined in AP140 and summarized below.

All users must assume responsibility for understanding the Employee and Volunteer Acceptable Use of Technology Guidelines as a condition of use. All computers and technology used throughout Northern Lights Public Schools are to be used in a responsible, efficient, ethical and legal manner. Failure to adhere to this procedure and the guidelines established below shall result in the revocation of access privileges and/or disciplinary actions involving division, local, provincial or federal agencies.

USER RESPONSIBILITIES (all employees and volunteers)

As the user of technology resources provided by the Northern Lights Public Schools, each employee must read, understand, and accept all of the following rules and guidelines as stated in this section:

1. I understand that all computer use must be for educational purposes, whether on school property or at another location. The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines concerning the ethical and legal use of the network resources; therefore:

- I will use NLPS technology resources and telecommunications for purposes in support of education and research that is consistent with the educational objectives of the Board;
- I will not use NLPS computers, devices or network services to conduct personal business or for the exclusive benefit of individuals or organizations that are not part of Northern Lights Public Schools;
- I will not use NLPS technology to view, create, modify or disseminate obscene, objectionable, violent, pornographic, or illegal material;
- I will not use NLPS technology for commercial or for-profit purposes that include, but are not limited to, home businesses, gambling, advertising, political lobbying or soliciting;
- I will not use NLPS technology to send unsolicited, offensive, abusive, obscene, harassing, or other illegal communications.

2. I understand that employees have access to confidential information and files and that I am responsible for protecting the confidentiality of this data; therefore:
   - I will log off the computer, device, network and cloud services when not using it;
   - I will not allow students, parents, or unauthorized people access to my accounts;
   - I will not reveal any personal information about a student or employee contained on information systems contained within NLPS;
   - I will not attempt to learn other employees' passwords;
   - I will not copy, change, read, or use files that belong to users without their permission.
   - I will save all critical Division data in the DocuShare system (for those with DocuShare authorization) and for all other staff on network servers to ensure backup of data.
   - I will manage all records (electronic and paper) in accordance with the Northern Lights Public Schools Records AP171 Records Management Policy.

3. All employees are provided with a Northern Lights Public Schools G-Suite email account which is accessible by using the NLPS G-Suite web interface and app. I understand that the following electronic mail (email) activities are not allowed:
   - Using email for purposes of political lobbying or campaigning,
   - Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account,
   - Reading another users' email unless authorized to do so by the owner of the email account,
   - Sending or forwarding "chain" letters,
   - Sending unsolicited messages to large groups except as required to conduct Division business,
   - Sending excessively large messages or attachments unless in performance of official Division business,
   - Sending or forwarding email that is likely to contain computer viruses.

4. I understand copyright laws protect a variety of materials (print, non-print and ideas) including those found on the Internet; therefore:
   - I will not install any unauthorized software, including personal software on NLPS equipment. Unauthorized software is defined as software outside the legal licensing agreement created by the author or the program;
   - I will not make copies of any software found on NLPS equipment, systems or on the Internet to keep, lend, give, or sell outside of the legal license agreement;
   - I will not use shareware beyond the trial period specified by the program unless I purchase it;
   - I will not download any copyrighted materials from the Internet without the permission of the copyright holder. This includes but is not limited to music, digital files and video files.

5. I understand the importance of maintaining the technology that I use for my job; therefore:
   - I will not attempt to bypass or disable any security and/or anti-virus software installed on my computer, device or on the network;
   - I will inform the NLPS ET/IT department about any problems with technology and follow the work order process implemented to fix the problem;
   - I will not attach any devices, including notebooks and electronic devices, to the network without the prior approval of the NLPS Technology department;

6. Special care must be taken to protect information stored on notebooks, smart devices, phones or any other portable computing devices, and in protecting such devices from theft. All portable computing devices must encrypt all NLPS data to ensure confidentiality in the event that the device is lost or stolen, therefore;

- I will contact the NLPS Education and Information Technology Department to provide me with the NLPS standard for encryption of my portable computing device as per the NLPS device encryption procedures.

I have read the rules and regulations above. I also understand that any computer or device, as the property of the Northern Lights Public Schools, is subject to random auditing for the purpose of determining the presence of unauthorized software, by either NLPS staff or authorized software organizations.

Employee Signature _____ Date _____

Employee Name (please print) _____

*** This signature page must be on file at the Personnel Office for the employee to maintain technology access.*