Policy 311

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) USE

New Nouveau Brunswick

DEPARTMENT OF EDUCATION AND EARLY CHILDHOOD DEVELOPMENT

Effective: 16 July 1996
Revised: 7 September 2004, 31st January 2024

1. Purpose

This policy defines the minimum standards for appropriate use of information and communication technologies in the public school system.

2. Application

This policy applies to students or school personnel or any invited organization member or volunteer with electronic access to the school network.

3. Definitions

App refers to any application or software that can be installed on a personal device.

Assistive technology refers to digital devices (apparatus, equipment, software or tools) offered to certain students to increase, maintain or improve their functional abilities in daily life or as part of their learning activities.

Bring Your Own Device (BYOD) refers to the practice of students and school personnel using personal devices for learning activities involving apps and for accessing the internet through the school network.

BYOD Zone refers to the electronic wireless school network through which students, school personnel or any invited organization member or volunteer can use personal devices to access the internet.

Cloud service refers to internet-based services that provide functionality and/or storage capacity, accessible anywhere in the world.

Information and Communication Technologies (ICT) refers to forms of technology used for the creation of physical or electronic objects, documents or information and for processing, displaying, sharing and storing this product and communicating it to others. This includes: multiple technologies, such as printers (including 3D models), audiovisual recording devices, phones, computers, networks and any equipment using the

internet in any form, including connection to the network, among others. ICT also refers to digital devices that are used in learning activities, including robotics, assistive technologies and electronic learning toys (ex: Robokind).

Online service refers to any internet-based service that may be provided from servers that are local (on premises, such as Service New Brunswick services) or global (cloud services, such as Microsoft Office 365).
Parent, as defined in the *Education Act*.

Personal device refers to any electronic device that is owned by school personnel, students or parents that can be used to connect to the internet and that is not provided by the Department of Education and Early Childhood Development (the Department), school district or school.

Personal information, as defined in the *Right to Information and Protection of Privacy Act*, refers to recorded information about an identifiable individual, including but not limited to

a. the individual's name,
b. the individual's home address or electronic mail address or home phone or facsimile number,
c. information about the individual's age, gender, sexual orientation, marital status or family status,
d. information about the individual's ancestry, race, colour, nationality or national or ethnic origin,
e. information about the individual's religion or creed or religious belief, association or activity,
f. personal health information about the individual,
g. the individual's blood type, fingerprints or other hereditary characteristics,
h. information about the individual's political belief, association or activity,
i. information about the individual's education, employment or occupation or educational, employment or occupational history,
j. information about the individual's source of income or financial circumstances, activities or history,
k. information about the individual's criminal history, including regulatory offences,
l. the individual's own personal views or opinions, except if they are about another person,
m. the views or opinions expressed about the individual by another person, and
n. an identifying number, symbol or other particular assigned to the individual.

Privacy Impact Assessment (PIA) refers to an assessment of an initiative, such as a program, activity or information system, that identifies the actual or potential risk the initiative might have on the privacy of individuals, and sets out recommendations for managing, minimizing, or eliminating that risk.

School personnel, as defined in the *Education Act*.

Social media refers to apps and websites where the content is created and shared in a social manner and is capable of being communicated with a global audience.

Software refers to any app, online service, cloud service, program or platform that could be used by students and school personnel in the public school system.

Student refers to a pupil, as defined in the *Education Act*.

Threat Risk Assessment (TRA) refers to a process used to identify, assess, and remediate risk areas. The result of this process is to keep the network integrity strong and help reduce and prevent attacks.

User refers to any student or school personnel or any invited organization member or volunteer with electronic access to the school network.

4. Legal Considerations and Authority

EDUCATION ACT, SECTION 6

> The Minister…
> *(b.2) may establish, within the scope of this Act, provincial policies and guidelines related to public education, …*

Subsection 6 (a), Powers and duties of the Minister

Section 31.1, Mandatory reporting of non-professional conduct

Section 40.1, Provision of information to the Minister

Section 56.3, Conflict with *Right to Information and Protection of Privacy Act*

5. Goals/Principles

5.1.

The Department of Education and Early Childhood Development (Department) recognizes that the public school system is instrumental in creating a learning environment where students develop foundational knowledge and skills using technology to meet complex challenges in ways that are useful, factual, positive and beneficial for the students in the present and in the future. Digital competencies are recognized as essential skills required for success.

5.2.

The Department supports and encourages the age-appropriate use of technology in education and recognizes that technology is a useful learning tool as part of a well-rounded education, including the development of skills and knowledge that will help students succeed beyond the school.

5.3.

The Department recognizes that a safe and secure online learning environment for all users should be founded on a good set of information protection directives. This protection is necessary for legal reasons. It is also simply good practice to do so. All users have a role to play in promoting and encouraging this environment.

5.4.

The Department affirms that the use of technology and access to the internet in the public school system is essential to learning; however, this is contingent on appropriate use and adherence to the ethical guidelines relevant to its use.

5.5.

The Department recognizes that as society acclimatizes to more technologies and increased connectivity, the school system must foster the development of good ethics and cyber citizenship of students and school personnel regarding the use of technology.

6. Requirements/Standards

6.1. ADHERENCE TO ICT STANDARDS

6.1.1. Each year, all students, or their parents (if required), and school personnel must sign a form attesting to their commitment to respect the laws, regulations, policies and guidelines regarding the appropriate use of information and communication technologies (ICT) available at the school, including access to the internet, personal devices and assistive technologies assigned to certain students. These standards align with the requirements outlined in *Policy 703 - Positive Learning and Working Environment* - Appendix D *New Brunswick Student Code of Conduct*.

The school district must develop a common form for the schools to administer and distribute to students or their parents (if required) and school personnel for their signature.

6.1.2. The collection, use, retention, disclosure or disposal of any personal information by school personnel shall be in accordance with the provisions of the *Right to Information and Protection of Privacy Act*, the *Personal Health Information Privacy and Access Act*, and any other applicable law, regulation or policy.

6.1.3. Users of ICT services available in the school must use it appropriately. More information can be found in Appendix A – *Appropriate Use of Information and Communication Technologies (ICT)*.

6.1.4. School personnel responsible for the school software, websites and social media accounts must regularly monitor them for immediate deletion of any unsuitable or broken links, obsolete documents, or any material considered inappropriate or in violation of the policies of the Department, the district, or the school.

6.1.5. When social media accounts are created for a school, the username and password must be shared with the school's principal. The same must be shared with the superintendent in the case of a school district's account. In both cases, they must be stored securely, with at least two people knowing where it is located. If two-factor or multi-factor authentication is available, it will be used. This allows the principal or the superintendent to access their respective social media accounts at anytime.

6.1.6. All applicable rules on the use of personal devices as detailed in this policy or by the school district, including the code of conduct, apply regardless of the connection type or internet provider used, including personal data plans.

6.1.7. All student and school personnel behaviour, comments, messages or actions online, in public or in private, during school hours, school-sponsored events and whenever the school is responsible for a student, that harms the school environment for another student or school personnel, may lead to repercussions or disciplinary measures at the school. Standards on the negative conduct of school personnel and students can be found in Policy 701 – *Policy for the Protection of Pupils* and Policy 703 – *Positive Learning and Working Environment* respectively. (For example, a person who says something about another student or school personnel online, at a school-sponsored event or on the school bus, that could negatively impact at least one person attending or working at the school, could be subject to disciplinary measures taken by the school or school district.)

6.1.8. Policy 703 – Positive Learning and Working Environment Appendix D – Provincial Student Code of Conduct Guidelines applies to both in-person and electronic conduct (for example, on the internet).

6.2. APPROVED SOFTWARE AND PROTECTION OF PERSONAL INFORMATION

6.2.1. The protection of personal information is vital. Only software approved by the Department may be used when the personal information of students and school personnel is to be used or stored in the software. An approved software will be analyzed for a variety of issues, such as security and the ability to use it within the network structure. Any school personnel, school, district or third party working in the school system wanting to use a software not approved by the Department must contact the Department's IT Strategy and Business Solutions Branch through this email to request permission.

The Department maintains a current list of all approved and prohibited software for use in the schools and school districts. This list promotes the sharing of information and best practices between schools and school districts.

6.2.2. Only cloud services approved by GNB may be used. (EECD Solution Repository.)

6.2.3. The registration of a website domain name must be approved by the Department's IT Strategy and Business Solutions Branch, which will provide available options. Registration of a website domain name without approval increases costs and the risk of harming the reputation of the school, the school district and school system, among other things, while preventing the ability to shut down the website in case of a breach of security or other unforeseen issue. (More information is available at the following link: Domain name (sharepoint.com)

6.2.4. Following the *Right to Information and Protection of Privacy Act* and applicable sections in the *Education Act* (see section 4 of this Policy), personal information that is considered necessary may be shared between the Department and the school districts and schools for the purposes of delivering public education.

6.3. PRIVACY IMPACT ASSESSMENT (PIA) AND THREAT RISK ASSESSMENT (TRA)

6.3.1. When a request for approval of a new software is received, the Department will determine whether a PIA and TRA should be conducted, as required. PIAs and TRAs allow the Department to ensure software conforms with legal, policy, and organizational requirements and with best practices in the protection of privacy. They also address stakeholders' primary concerns regarding the protection of the confidentiality of information that is collected, used, shared, and they incorporate the protection of privacy from the outset. For more information concerning this process, contact the Departmental Information Security Officer (DISO).

Of note: When the Department approves a system, it only approves the risks related to the system's safety. The district is the one that approves its use on its territory, and it must consider the reputational risks of its use.

6.4. POSTING AND SHARING OF PERSONAL INFORMATION AND PHOTOS/VIDEOS

6.4.1. The privacy and safety of students and school personnel is paramount. To not compromise their rights, students and school personnel shall not publish, on the internet or elsewhere, any video or audio recording, photo or other personal information of another person, taken at school or during a school sponsored event, without their consent (or parental consent where applicable), on any software program or app, whether personal or not, or any software program or app belonging to a school or a school district. Doing so may lead to disciplinary measures.

6.4.2. On a yearly basis, the school must obtain the written consent of students and parents (if applicable) before publicly sharing or publishing personal information (electronically or not). Parental consent must be obtained for all students under the age of 16.

6.4.3. Personal information may be disclosed without consent in cases where there is a legal authority to do so. For example, consent is not required when personal information needs to be shared confidentially in order to offer educational services to a student, for use in approved software, when it is necessary to prevent harm to a person, when it is needed for a legitimate search, when it is needed in a case where an individual's health or safety is deemed to be at risk or as part of a regularly offered service and it is reasonable to believe that students and their parents are already aware.

School personnel are to consult the school district personnel responsible for privacy in their respective school district when they have questions regarding the disclosure of personal information.

6.4.4. The risk of the online use of an individual's name, photo or any other identifying information must be carefully assessed. Even with consent, this poses a considerable risk. (The risk to the safety of users increases each time personal information is shared publicly. Even with consent, consideration should be given to whether posting the information is worth the risk.)

6.5. APPS FOR PERSONAL DEVICES

6.5.1. Any apps that school personnel ask students to use on their personal devices for educational purposes, must be;

a. approved by the school district before it is approved by the Department;
b. age appropriate and used respecting any age restriction listed in the terms and conditions of the app; and
c. available at no charge to students (whether free or purchased by the school, school district or Department).

6.5.2. For educational uses linked to learning, only free apps or those with a Government of New Brunswick corporate licence may be used by students in class. The disbursement of costs to activate certain functions in applications, such as in-app purchases, is not allowed.

6.6. BYOD ZONE

6.6.1. Usernames provided by the school must be used when connecting to the BYOD zone (the school network). This strengthens the network's security as it allows activity to be traced back to an individual, if necessary. Passwords will not be shared with others and will be kept confidential.

6.7. USE OF PERSONAL DEVICES

6.7.1. Schools and school districts must not require, or request that students or parents purchase or use specific brands or models of personal devices. However, personal devices used must meet the recommended device specifications, which can be found in Appendix B – *BYOD Program and Personal Devices*.

6.7.2. For multiple reasons, a student may be eligible to borrow a device on a temporary basis. Eligibility criteria for borrowing a device and the processes for assigning and returning the device can be found in Appendix D – *Deploying Temporary Devices*.

6.7.3. When kindergarten to grade 8 students are told they may use a personal device for an in-class activity, the school must make an effort to ensure students without access to a personal device for the activity are given access to a device, allowing them to participate and complete the assigned task. If applicable, students may also share devices among themselves.

6.7.4. Schools must develop guidelines concerning the appropriate use of personal devices. In cases of undesirable use, school personnel may confiscate a student's personal device. However, students' personal devices can be essential tools. In cases where the student uses their personal device for accessibility, for critical communication purposes, (such as a translation device) or for medical reasons, school personnel will need to discuss alternate methods of dealing with undesirable device usage.

6.7.5. Device confiscation, as detailed in subsection 6.7.4, is not considered a search and seizure as defined in Policy 712 – *Search and Seizure*; therefore, confiscated devices (in these cases) cannot be searched. If the search of a personal device is required, the search must comply with Policy 712.

6.7.6. Any user who connects a personal device to the BYOD zone must ensure the device is kept up to date and any available patches (such as iOS updates) are installed to reduce security risks to their devices and to the school network.

6.8. LAPTOP ASSISTANCE PROGRAM

6.8.1. With the BYOD learning strategy for students in high school (grades 9 to 12), and for personalized learning, students may use devices they are already familiar with. The Department offers a subsidy program that provides the opportunity to purchase a device that meets the recommended device specifications. More information on this program, including the recommended device specifications, can be found in Appendix C – *Purchasing a Laptop*.

6.9. COMMUNICATIONS (INCLUDING EMAILS) BETWEEN SCHOOL PERSONNEL, PARENTS, AND STUDENTS

6.9.1. Students and school personnel must use a communication method approved by the Department when communicating with each other. This includes using the school personnel official email address (such as @nbed.nb.ca), online services (Microsoft 365) and apps (Microsoft Teams), and it enables the tracking of communication between users, if necessary. As an example, a coach of a school sports team may use Teams to communicate with the members of the team.

An exception may be made if the school personnel coaching a team (i.e. volunteer) does not have access to a Department approved communication method. In such cases, and with approval of the school principal, a group chat may be started. This group chat will include all students on the team, along with one school personnel selected by the school principal. In these cases, the technology used is irrelevant, however it must be approved by the Department, using the process as described in section 6.2 of this policy.

6.9.2. No written communication between school personnel and parents shall take place on public websites or social media platforms (such as Facebook), nor by phone text when it is regarding a student. These discussions must be held privately, via a method of communication assigned by the employer. This includes using official email addresses (such as @nbed.nb.ca), online services (Microsoft 365) and apps (Microsoft Teams). This will ensure personal information is protected.

6.10. USE OF SOCIAL MEDIA/WEBSITES BY A SCHOOL OR SCHOOL DISTRICT

6.10.1. Only approved social media platforms may be used for official school use. Contact the Department for a complete list of approved platforms. A school district may choose to restrict how many, and which approved social media platforms it uses.

6.10.2. To have a social media platform approved, the school district must first discuss its potential use internally, and with its IT Governance committee if it has one. If recommended by the committee, the school district should then contact the Department's IT Strategy and Business Solutions Branch to make the request. Each request will be evaluated for approval or not.

6.10.3. Any information to be posted on social media platforms and websites must follow the rules as described in section 6.4.

6.11. USE OF MATERIALS AND COPYRIGHT

6.11.1. All students and school personnel must ensure the appropriate use of materials created by others and must not breach copyright regulations. The Council of Ministers of Education, Canada (CMEC), has developed resources that explain how to use materials and what can and cannot be copied.

a. Fair Dealing Guidelines (https://www.fairdealingdecisiontool.ca/fdg/default.aspx) provides an overview of how materials may or may not be permitted for use.
b. Fair Dealing Decision Tool (http://www.fairdealingdecisiontool.ca/DecisionTool/). This is a tool that asks users to answer a few questions and provides them with a response explaining whether they can use the materials without obtaining prior consent from the author.
c. Copyright Matters! (Copyright Matters 5th Edition FINAL EN.pdf (cmec.ca)). The copyright guidebook for school personnel helps answer key questions on copyright and fair dealing.

6.11.2. Any other questions concerning the use of materials and copyright may be sent to the Department's Policy and Planning Division.

6.12. PASSWORDS

6.12.1. School personnel shall not keep printed or written copies of students' passwords for the accounts provided by the school, school district or Department. If a student's password is forgotten, the school personnel must find it in the correct location in the system. This increases the security of student accounts.

6.12.2. If a student's password is not working, the school personnel must submit an official password change request for the student.

7. Guidelines/Recommendations

7.1.

An ICT committee should be established in each school for effective communication and governance regarding the technologies used in schools. This committee's responsibilities could include receiving and facilitating requests for new technologies, being a point of contact for technology requests from the school and advising and recommending training for school personnel on the use of technology.

7.2.

To ensure school personnel and students are aware of any new developments, schools and school districts should offer regular training courses on the appropriate storage and use of personal data, for both school personnel and students. Such training is essential to promote the responsible use of ICT and ensure the security and privacy of school personnel and students.

7.3.

It is strongly recommended that school districts ensure that their school personnel receive up-to-date annual cybersecurity and privacy training. This training is essential to raise personnel awareness of online threats, and to protect the personal data of students and school personnel from the high risks associated with security breaches.

7.4.

Students and school personnel are advised not to use their NBED e-mail address for personal uses such as accessing a system or application or making online purchases. The purpose of this directive is to reduce security risks for the school network. By respecting this directive, users who never use their NBED address for personal purposes will be able to recognize fraudulent messages, such as those from fake e-commerce sites.

8. District Education Council (DEC) Policy Making

A District Education Council may develop policies and procedures that are consistent with, or more comprehensive than, this provincial policy. Their policy must be posted on the school district website and shared with all members of the school environment at the beginning of every school year.

9. References

Education Act
Right to Information and Protection of Privacy Act
Personal Health Information Privacy and Access Act

Policy 311 – *Information and Communication Technologies (ICT) Use*

- Appendix A – *Appropriate Use of Information and Communication Technologies (ICT)*
- Appendix B – *BYOD Program and Personal Devices*
- Appendix C – *Purchasing a Laptop*
- Appendix D – *Deploying Temporary Devices*

Policy 701 – *Policy for the Protection of Pupils*
Policy 703 – *Positive Learning and Working Environment*
Policy 712 – *Search and Seizure*

List of approved software

Departmental Information Security Officer (DISO)

Council of Ministers of Education, Canada (CMEC)

- Fair Dealing Guidelines (http://www.fairdealingdecisiontool.ca/fdg/default.aspx)
- Fair Dealing Decision Tool (http://www.fairdealingdecisiontool.ca/DecisionTool/)
- Copyright Matters! (cmec.ca)

10. Contacts for Additional Information

Department of Education and Early Childhood Development
Policy and Legislative Affairs
(506) 453-3090
edcommunication@gnb.ca

Department of Education and Early Childhood Development
IT Strategy and Business Solutions Branch
(506) 453-3678

Original signed by

Minister