

**DATE:** May 2, 2023

**TO:** Board of Trustees

**FROM:** Darrel Robertson, Superintendent of Schools

**SUBJECT:** Digital Literacy and Cybersecurity for Staff and Students  
(Response to Request for Information #014)

**ORIGINATOR:** Cliff Richard, Chief Infrastructure and Technology Officer

**RESOURCE STAFF:** Lea Beeken, Blythe Evans, Terry Korte, Aaron Muller, Ann Parker, Karen Plant, Bernice Pui, Will Rice, Mark Strembicke

**REFERENCE:** March 7, 2023 Board meeting (Trustee Sumar)  
[CN.AR – Creation, Use and Maintenance of Division Information](#)  
[CNB.BP – Information Security](#)  
[CNA.AR – Security of Personal and Division Information](#)  
[DK.BP – Division Technology](#)  
[DK.AR – Division Technology Standards](#)  
[DKA.AR – Division Technology Specifications](#)  
[DKB.AR – Appropriate Use of Division Technology](#)  
[GI.AR – Teaching and Learning Resources](#)  
[Alberta Education Teaching Quality Standard](#)

---

## **DEFINITIONS**

**Digital Citizenship:** Beyond conversations about personal responsibility, digital citizens are active participants in online communities who see possibilities instead of problems, and opportunities instead of risks as they curate a positive and effective digital footprint (International Society for Technology in Education (ISTE)).

**Digital Literacy:** The knowledge of and ability to use digital technologies to locate information; evaluate information; synthesize, create, and communicate information; and understand the human and technological complexities of a digital media landscape (ISTE).

**Cyber security:** The practice of protecting systems, networks, and programs from digital and physical attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

**Bring-your-own-device (BYOD):** Personal mobile devices that students bring to school and devices such as laptops, Chromebooks, tablets, and mobile phones.

**Third-party apps:** third-party apps are any digital tools that are not licensed or supported by Division administration. These digital tools can include websites, apps and platforms where students access

information, upload content, create accounts to access or save progress or use Division credentials to log in (e.g., *Flip, SeeSaw, EdPuzzle, Kahoot*, etc.).

**ISSUE**

At the March 7 Board meeting, Trustee Sumar submitted the following request for information:

- Given the increasing prevalence of cyber attacks and ransomware attacks,
- Given that six in ten Canadian children as young as ten years old have experienced or are experiencing cyberbullying ([source](#)),
- Given that problematic media device use has been linked to low academic outcomes, a reduction in concentration, and mood disturbances ([source](#)),
- Given the increasing reliance on the use of technology for educational purposes,
- Given that provincial, federal, and international governmental bodies have limited the use of social media applications like TikTok ([source](#)):

1. What is being done to develop the digital literacy of staff and students?
2. What cybersecurity training is being provided to staff? What cybersecurity education is being provided to students?
3. What are schools doing to ensure that students are using smartphones and other devices appropriately? This includes but is not limited to the use of social media and digital well-being.
4. What measures are being taken to protect student and staff data being stored on Google?
5. What is being done to ensure equitable access to education for students who do not have a cell phone in the classroom?
6. What input has the Division given to the provincial government about including digital literacy in the new curriculum?
7. What is being done to ensure the applications used in Division schools have been vetted for appropriateness, education value, and digital security? Who vets the resources used in Division schools, and on what criteria?
8. Does the Division provide educators with a database/resource list of safe-for-school applications? What opportunities is the Division engaging in to find efficiencies in vetting educational resources and/or creating a database? Is the administration aware of how the process for creating such a database compares across provinces?
9. What avenue(s) of communication will the Administration, clubs, sport teams, etc. use to connect with students that is consistent throughout the Division to ensure all students are included?
10. When choosing classroom activities or course work for students, what mechanisms are in place to ensure that all students have equitable access to modern electronic devices when they are needed? For example, if students are asked to use their cellphones in class, how are students without a phone accommodated?

**KEY POINTS**

1. The Division has a range of resources to support teachers in providing digital citizenship and digital literacy instruction to students. Principals determine the priority for this work using a site-based approach.
2. The applications used with students are selected at the school level through a site-based approach. Principals are responsible for the selection of teaching and learning resources at their school.
3. Division applications (e.g., Google Workspace for Education, Powerschool, etc.) are licensed and managed by central administration. Other resources (including online applications) are vetted by

- school staff for age appropriateness and educational value, then submitted to administration to determine the alignment of privacy, security, and technical compatibility with Division systems.
4. Technical and administrative controls are in place to ensure the privacy and security of Division applications and staff and student information.
  5. Training and awareness of staff is critical to protecting the Division's information assets.
  6. Equitable access to technology for students is supported by the [Technology Evergreening Strategy](#) – Attachment II.
  7. Cyber Security Services (CSS) uses an industry standard to drive the CSS strategic plan to respond to and mitigate the cyber risks associated with the use of technology by both students and staff.

**BACKGROUND**

Principals are responsible for the selection of teaching and learning resources used in their school following the *GI.AR – Teaching and Learning Resources Administrative Regulation* criteria. In addition, principals and individual staff members determine the priorities for school staff and personal professional learning each year, taking into consideration the priorities and goals in the Division Strategic Plan; current provincial, Division and catchment initiatives; as well as staff requirements.

Teachers, as outlined in the *Alberta Education Teaching Quality Standard (TQS): Demonstrating a Professional Body of Knowledge*, plan and design learning activities that address the learning outcomes outlined in their assigned programs of study while also striving to “incorporate a range of instructional strategies, including the appropriate use(s) of digital technology, according to the context, content, desired outcomes and the learning needs of students.” They incorporate digital technology and resources when and where appropriate, with a goal of building student capacity for communicating and collaborating with others and evaluating information from different sources (among other competencies).

Technology and Information Management (TIM) is responsible for the provision of technology across the Division for instructional and business purposes. TIM supports teaching and learning by providing an equitable base level of access to devices, applications, infrastructure and networks that facilitate the secure and effective integration of technology. The TIM team includes Enterprise Technology Support, Network Operations, Programming Services, Student Information, Information Management and FOIP (Freedom of Information and Privacy), Cyber Security, Information Security, School Supports and Training, Help Desk, and the Information Technology Store (ITS or IT Store).

TIM staff regularly solicit feedback regarding digital literacy, digital citizenship, and cyber security from school and central stakeholders through a variety of mechanisms. The TIM principal advisory committee meets quarterly to provide feedback on these and other topics. The Safer Schools Collaborative Cyber Team (SSCCT) of central leaders will be established in May 2023 to address emerging issues in schools, document best practices, and provide input on training to school staff. In addition, a network of educational technology (EdTech) leads from each school meet monthly to discuss emergent issues and provide input on new initiatives from the perspective of the classroom teacher.

TIM collaborates with Division Support Services, Communications and Division Security when incidents such as cyberbullying occur. The teams work collaboratively to support the school when incidents occur, including assisting with any associated investigations related to student conduct.

Within TIM, the School Supports and Training unit includes the Technology Integration and Planning Support (TIPS) team which has led the Division's collaborative work around digital citizenship, the use of

third-party apps, teacher professional learning regarding Division systems, and cross-departmental projects. Network Operations staff manage the Division network, central computer systems, filters and firewalls, and the access to and administration of major Division systems including Google Workspace for Education. A team of TIM staff meet weekly to discuss the configuration of settings and investigate new features in Google Workspace for Education.

In the 2021–2022 school year, TIM established a Cyber Security Services (CSS) unit. The purpose of CSS is to implement the pillars of cyber security including hardening the Division’s cyber security posture, increasing information stakeholder awareness, and shifting security posture from reactive to proactive. This includes assessing the state of current controls and developing and sustaining a strategic plan based on risk. Milestones reached in the first year included:

- Operational endpoint protection
- Implementation of multi-factor authentication (MFA) for remote access
- Pilot and evaluation of extended endpoint protection
- Standards framework developed, and three standards approved
- Incident response plan implemented
- Cyber Aware and Secure staff training program implemented

In the 2022–2023 school year, Cyber Security Services will reach the following major milestones:

- All staff have two-step verification enforced for Google Workspace
- Ransomware incident response plan developed and tested
- 24/7 cyber security response to high incident alerts
- Integrating Google Workspace security with Microsoft Defender
- Cyber investigations protocol developed

## **CURRENT SITUATION**

Responses to Trustee Sumar’s questions:

### **1. What is being done to develop the digital literacy of staff and students?**

Central administration works closely with school-based staff to provide professional development opportunities, resources, and a policy framework focused on student digital literacy. School principals provide direction to staff and set priorities for the time and resources to be dedicated to these topics. Some of the supports provided to staff include:

- a. Professional development:
  - i. Separate EdTech Lead networks of school-based staff exist for both high school and K–9. Every school has a designated EdTech Lead; this creates a distributed leadership model to develop the capacity to support the effective integration of educational technologies into teaching and learning. Each month the EdTech Lead teachers are invited to a collaborative meeting facilitated by the TIPS team. The agendas are co-created by participants in order to address the most relevant topics. Digital Citizenship is a repeated topic of focus at both levels. Resources are shared and offerings for in-school support are communicated.
  - ii. EDU 597 series: TIPS consultants work in partnership with the University of Alberta to offer a year long professional learning series from October to May, with an opportunity for staff to obtain three credits in Open Studies at the university with the completion of an academic paper. The topic of Digital Citizenship is woven throughout the series.

- iii. EdTech Summits: Several times a year on Division PD days, TIPS consultants in conjunction with EdTech leads present concurrent online learning sessions on a variety of topics. Digital Citizenship presentations have been frequently offered over the past several years.
  - iv. Summer Workshops: Based on a variety of research-based frameworks, platforms and digital tools, participants were engaged in learning sessions to make meaningful connections between classroom practice and technology. Collaborative time was given to create plans to develop digital citizenship skills for staff and students.
  - v. Pre-DLM sessions for school leaders: These sessions focus on the five-competency model of digital citizenship created by the *International Society for Technology in Education (ISTE)* that supports students to be inclusive, informed, balanced, alert and engaged. Critical research is shared to further understand the multi-faceted approach needed to develop digital citizenship skills in an appropriate manner. Sessions were hosted by TIPS consultants in collaboration with other central departments. Participants were engaged in the following ways:
    - creating a school plan for digital citizenship,
    - gaining understanding of central technology systems that are in place for student safety,
    - dialoguing with colleagues,
    - making curricular connections and reviewing resources available for teachers, students and parents.
  - vi. School requested sessions for Digital Citizenship: Each TIPS consultant corresponds directly with schools and catchments to provide timely and relevant professional development as it relates to school goals and initiatives. The TIPS Team follows the guidelines from the ISTE *Digital Citizenship in Action* course. This course explores the human side of technology and the analysis of what it means to be a citizen of digital spaces, and considers the implications of these ideas for our students and staff. The knowledge and skills developed set the foundation for initiatives to bring digital citizenship into Division classrooms in meaningful ways.
- b. Resources:
- i. Tutorial Videos: TIPS consultants regularly update the *Edmonton Public Schools – Technology Help* YouTube channel with support videos, recorded sessions and weekly *After School Tech Tips*.
  - ii. Searchable database: TIPS consultants maintain a searchable database of resources on [TIPS.epsb.ca](https://tips.epsb.ca) and Connect.
  - iii. Lesson plans: TIPS consultants prepared ready-to-use lesson plans, pre-recorded lessons, presentation slides and best practices resources for use with K–12 students on the topic of password safety.
  - iv. Digital Citizenship page on the TIPS website: TIPS.epsb.ca continues to be updated to reflect the new ISTE standards and provide resources to bring this work to life in K–12 schools. The layout of the page provides resources for considering all of the steps in creating a year-long digital citizenship plan that involves all stakeholders: teachers, students and families. Direct connections are made to the *Alberta Teaching Quality Standard*, the *Alberta Education Information and Communication Technology Curriculum*, as well as the *Alberta Education Competencies*, which guide the work of teachers in our Division and the province.

- v. Monthly EdTech updates: Information is shared every month with topics including: technology updates, leadership development, shared best practices and feedback for the TIM department. Suggestions specific to digital citizenship and inspiration for in-depth technology engagements are highlighted.
- c. Policy direction:
- i. EPSB *Responsible Use of Technology Agreement* (RUTA) template. Each school has their own RUTA or “*Acceptable Use of Technology Agreement*” which is typically shared with parents at the start of the school year via SchoolZone. The EPS RUTA template was reviewed by TIPS consultants in conjunction with other central consultants and school leaders to reflect the Division’s current framework for digital citizenship development. This is a student-centric document with three versions so the content and language can be age appropriate for each group. School leaders can edit the template as needed to communicate the direction of development for their school community. The purpose of the RUTA is to outline the positive actions students can take to develop the skills of a digital citizen. The action statements for students are based on the ISTE student standards and their five-competency model for digital citizenship.
  - ii. TIPS consultants worked collaboratively with leaders from Division Support Services to add a *Responsible and Ethical Use of Technology* section on page 10 of the *Student Rights and Responsibilities* template, in alignment with Board Policy *HG.AR – Student Behaviour and Conduct*. The student responsibilities are categorized under the following headings as they align with the *Responsible Use of Technology Agreement*: demonstrate respect and integrity, be safe and secure, and respect and protect property. See the [Student Rights and Responsibilities Template](#) – Attachment V.
- 2. What cybersecurity training is being provided to staff? What cybersecurity education is being provided to students?**
- a. Staff:
- i. Monthly *Cyber Aware and Secure* videos are sent to all Division staff, and various metrics are collected. See [Cyber Aware and Secure Campaign](#) – Attachment VI.
  - ii. Phishing exercises to increase staff capacity to identify phishing are assigned to staff every two months.
  - iii. Cyber Security Services is rolling out two-step verification to all Division staff, with accompanying training and communications to make staff aware of the value of two-step verification. The initiative currently has an acceptance rate of over 92 per cent among staff with over half the schools and central units enrolled. The rollout to all staff will be complete by May 30, 2023.
  - iv. Implementation of the *Safer Schools Collaborative Cyber Team* (SSCCT) – Spring 2023: The SSCCT’s purpose is to support positive and appropriate online student behaviour by providing school administration and teachers with proactive strategies and responsive resources for emerging and ongoing concerns in the online world. This team will consist of staff from Division Support Services (DSS), TIM (CSS, TIPS, Network Operations), Communications, Curriculum and Learning Services (Mental Health consultants) and Division Security. This initiative aligns with Priority 3 of the Division Strategic Plan. Technology and Information Management (TIM) will coordinate the SSCCT, which will provide a coordinated approach to:

- Debriefing and identifying recommendations arising from past and ongoing cyber-incidents.
  - Identifying potential issues on the horizon (i.e., from other jurisdictions, trends).
  - Monitoring and reporting on cyber issues in schools such as social media issues.
  - Identifying professional learning and training opportunities required for school administrators and teachers.
  - Developing processes and roles for schools to follow in the case of a situation of concern.
  - Identifying resources and learning opportunities required for parents and students.
  - Advising TIM staff on account security options for student applications (e.g., SchoolZone, Google Workspace, etc.).
- v. Ransomware response (simulation) exercises with key central staff in Finance, Technology and Communications took place in February 2023, with future simulations planned for other central departments in spring and fall 2023.
  - vi. Onboarding Cyber Security Training has been added to the current HR process.
  - vii. *Safer Schools Together* training (train the trainer model) with attendance from Information Management staff and Division Support Services – included Online Behaviour Trends and Updates (a monthly update). The cyber investigations team has ongoing training about investigating digital threats: Digital Threat Assessment training levels Standard and Advanced, to support school administration.
  - viii. Catchment professional learning session – *Advanced Digital Threats for School Administrators*.
  - ix. Resources and support for school administrators through the cyber investigation process.
- b. Students:
- i. This is a site-based approach, supported in part by the resources identified above. Digital citizenship and cyber security education is identified in the Alberta Program of Studies. Administration has identified these curricular outcomes and their alignment to the current curriculum.
  - ii. Age-appropriate resources including presentations, videos and lesson plans have been provided to staff for use with students.
  - iii. Cyber security education resources (including tutorials and lesson plans) for teachers (see response 1(b)(iv) above).
  - iv. Wallpapers for Division Chromebooks. Internal Communications created logos and designs related to five digital citizenship tips that align with the five-competency model from ISTE for wallpapers that are displayed throughout the year on all Chromebook start pages.
3. **What are schools doing to ensure that students are using smartphones and other devices appropriately? This includes but is not limited to the use of social media and digital well-being.** Principals make site-based decisions regarding the rules about the use of smartphones and other devices, as well as whether applications such as Google Chat or social media applications (e.g., TikTok, Instagram, Reddit, etc.) will be permitted, and at which grade levels. TIM provides advice, guidelines and templates for school staff, and provides a mechanism for principals to request changes to the network-level filtering at their site. Three examples of different site-based approaches to the use of personal devices are described below:

- a. Jody Lundell, principal of Dr. Margaret-Ann Armour School (K–9) says, *“Ensuring students are using technology safely, responsibly and ethically is an ongoing challenge faced by schools. We are well aware that students are spending many hours using technology, during school and outside the school day, and this has a significant impact on their physical and mental health as well as their focus and attention.”* To address these issues, the school encourages physical activity and alternative learning activities that do not involve technology, limits the use of technology, and has implemented a ‘no phone/airpod’ policy during school hours along with disabling Google Chat for students. Lunch hour use of phones or airpods is only permitted for Grades 7–9. Staff also educate students about the impact of technology on their physical and mental health, academics and friendships/relationships, and encourages students to report unsafe behaviour and cyberbullying to a parent or adult using an anonymous reporting process. They educate parents by sharing information through newsletters, parents evenings, letters, etc.
- b. Tara Copeman, principal of Bannerman School (K–6) writes, *“In low SES [socio-economic status] schools, reliable access to technology AT SCHOOL is a critical tool to support students to develop a number of academic skills, with digital citizenship being just one of them. Just as we would explicitly teach students how to use manipulatives as a tool to help them learn essential concepts such as fractions, we must explicitly teach students the purpose of the technology we use, how it helps us learn, when it does not help us learn, and how to use it responsibly. I do not have within my control to ensure equity of access to technology for all my students at home; however, I can ensure the school provides instruction and access to technology to all students that they can then leverage outside the school.”*

The school has one-to-one access to technology, both iPads and Chromebooks, starting at Kindergarten. Principal Copeman describes the cultural norms they have established to support the responsible use of technology:

- i. We use technology for learning. Teachers must explicitly teach and model the behaviours and habits we want to see with technology use.
  - ii. We take care of our technology so that when we need it, it is always ready for us.
  - iii. We use technology respectfully and responsibly, just as we would any other school tool (like scissors, pencils or gym equipment!).
  - iv. We learn how to use technology effectively as a multi-purpose learning tool – typing, speech to text, text-to speech, manipulating print size, accessing audio files/books, word-finding apps, how to research, using shared documents for collaborating, Pear Deck for engagement, etc.
  - v. We know everyone needs different things at different times, so we respect that some people will use more technology and some people will use less.
- c. Rick Oldring, Assistant Principal at Victoria School (K–12) says: *“We recognize that the ubiquitousness of the online world is adding to the work we do in schools to keep students feeling safe. It is very difficult for us to manage the issues that occur online as they happen very quickly, spread faster than we can stay on top of, and occur outside our jurisdiction; physically in regards to time and place and digitally in regards to access through data plans.”* He outlines the following guidelines for smartphones and personal devices at Victoria:
    - i. We use technology for learning. Teachers must explicitly teach and model the behaviours and habits we want to see with technology use.
    - ii. We take care of our technology so that when we need it, it is always ready for us.
    - iii. We use technology respectfully and responsibly, just as we would any other school tool (like scissors, pencils or gym equipment!).
    - iv. We learn how to use technology effectively as a multi-purpose learning tool – typing, speech to text, text-to speech, manipulating print size, accessing audio files/books, word-finding apps, how to research, using shared documents for collaborating, Pear Deck for engagement, etc.
    - v. We know everyone needs different things at different times, so we respect that some people will use more technology and some people will use less.



- i. Cell phones are only permitted in Grade 1–9 classrooms at the discretion of the teacher. Teachers with the confidence to manage cell phones see it as an opportunity to model appropriate use.
- ii. Teachers who use cell phones as teaching tools with students use the norm of “Screen Up/Screen Down” to manage their use during class. Students may have their cell phones taken away from them for a class if their phone screen is “up” when it should be “down”.
- iii. We regularly ask for screenshots as one means of validating the claims of bullying or inappropriate online behaviour. Students will often come to us with screenshots.
- iv. We have a section on the *Responsible and Ethical Use of Technology* in our Students Rights and Responsibilities document. We review this section with the students at orientation in September and at the semester change in February. If the students behave inappropriately on their own devices with their own data, we focus on the unacceptable behaviour section in the Students Rights and Responsibilities Document, which transcend the device used.

Templates:

- a. Students and their families are made aware of *Responsible and Ethical Use of Technology* (RUTA) expectations contained within each schools' Student Rights and Responsibilities document and prompted to acknowledge this annually through a form in SchoolZone. School leaders can reference the RUTA and add customised messages about school specific practices for use of technology (see response 1(c)(i) above).
- b. Principals can reference the Division's [Bring Your Own Device Guidelines](#) which include strategies and sample expectations when developing their school protocols for personal device use.

**4. What measures are being taken to protect student and staff data being stored on Google?**

- a. Administration has reviewed Google Workspace for Education's privacy policies and security measures and is satisfied that it protects the privacy of users (staff and students). The [Google Workspace for Education and Privacy in Edmonton Public Schools](#) (Attachment I) provides an overview of data ownership, privacy and security of EPSB data stored with Google. This document is shared with staff and students on internal sites as well as with parents and guardians via the [Collection and use of personal information by Edmonton Public Schools](#) – Attachment III and on SchoolZone.
- b. A Privacy Impact Assessment (PIA) was conducted and submitted to the Office of the Information and Privacy Commissioner (OIPC) for review when EPSB began using Google Workspace for Education. The Commissioner accepted the PIA and stated, "*In my opinion EPS has made reasonable efforts to protect personal information as required under section 38 of the FOIP Act.*" The Division continues to review and assess updates and changes to Google Workspace for Education as it evolves.
- c. EPSB is satisfied that Google Workspace for Education (which differs from public Google or Gmail accounts) meets the requirements under Alberta's *Freedom of Information and Protection of Privacy Act (FOIP Act)* to ensure security and privacy. Specifically:
  - i. All of a user's data is owned by the user and EPSB and Google makes no claim on the content. Google does not scan or index Google Workspace for Education accounts for advertising or other purposes.

- ii. Google Workspace is governed by a detailed Google Workspace for Education privacy policy and an Education Trust policy which ensures Google will not inappropriately share or use personal information placed in EPSB systems.
- iii. The Google Workspace for Education Terms of Service contractually ensures that students and staff are the owners of their data.
- iv. EPSB data on Google is stored in Google data centers. All data stored with Google is encrypted in transit and at rest, and is protected by six layers of security.
- v. Google complies with applicable U.S. privacy law and the Google Workspace for Education Terms of Service specifically details their obligations and compliance with U.S. *FERPA (Family Educational Rights and Privacy Act)* regulations. For the Alberta context, the Terms of Service have been reviewed to ensure that they meet our requirements under the *Alberta FOIP Act*.
- vi. Google includes tools to ensure that confidential or sensitive information that is emailed outside of the Division can easily and securely be encrypted. [Division Encryption Guidelines](#) – Attachment IV.

**5. What is being done to ensure equitable access to education for students who do not have a cell phone in the classroom?**

- a. All schools in the Division are allocated student devices through the Technology Evergreening Strategy (TES) which is managed by TIM. This strategy provides baseline student-to-Chromebook ratios (2.5:1 for K–9 schools and 3.5:1 for high schools) to ensure that students have equitable access to technology. Students are generally not expected to have access to a smart phone in the classroom.
- b. Providing student devices beyond these TES ratios is a school-based decision. Some schools fund additional devices through their school budgets, and some have a more formally established BYOD program. Thomas Rogers, Assistant Principal at S. Bruce Smith (SBS) School (7–9) discusses how they choose to provide students with equitable access to devices:
  - i. As part of the yearly school supplies, students provide a device that meets the criteria that we outline in our SBS BYOD Policy to ensure it will be a good fit for educational use.
  - ii. For families who cannot or choose not to provide their own device, Chromebooks are loaned out by a process similar to a textbook loan.
  - iii. Outside of the challenge of access to school devices for provincial exams (which we have addressed by borrowing from within our catchment), we have not received a single parent concern with this approach in leveraging equitable technology for students.
- c. School principals also request Chromebooks for vulnerable students through the 'Chromebooks for Kids' program of the Edmonton Public Schools Foundation. In its first year almost 600 chromebooks were placed in the hands of students across the city.

**6. What input has the Division given to the provincial government about including digital literacy in the new curriculum?**

Alberta Education provided opportunities for all members of the public to provide feedback to the draft curriculum through individual submissions directly to the province. Many Division staff participated in this feedback opportunity. Group feedback sessions that Division staff participated in were considered confidential. The Division does not have information as to what specific feedback was provided.

Feedback Administration considers appropriate to share if directly engaged includes:

- a. Age appropriate stand alone topics as a thread in the provincial curriculum to assist divisions with setting aside time in class to focus on digital literacy/citizenship issues.
- b. Provincial resources developed to support school divisions might include:
  - i. Anonymous reporting tool – Through B.C.'s ERASE program, as an example, students are able to anonymously report serious cyber-issues using an online form. The agency then forwards the report to the identified school administration.
  - ii. Professional learning for teachers and administrators.
  - iii. Documentation of digital threat trends.
  - iv. An approved list of applications recommended for use in school divisions.
  - v. Privacy compliance support for school divisions (updated resources in response to school division issues). Examples from other jurisdictions:
    - [Accountable Privacy Management in B.C.'s Public Sector](#)
    - [Privacy Management Program Guidance for B.C. Public Bodies](#)
    - [B.C PIAs](#) including Blogger, FaceBook, Twitter, etc.
    - [A Guide to Privacy in Ontario Schools](#)

**7. What is being done to ensure the applications used in Division schools have been vetted for appropriateness, education value and digital security? Who vets the resources used in Division schools, and on what criteria?**

Administrative Regulation *GI.AR – Teaching and Learning Resources* provides guidance relative to responsibility for the selection of any teaching and learning resources, and provides criteria for the selection of those resources. The principal is ultimately responsible for the approval of resources at the school level using the criteria provided in the regulation, which includes appropriateness for grade level and educational value.

In turn teachers, as outlined in the *Alberta Education Teaching Quality Standard (TQS)*, select resources including digital technology to support a range of instructional strategies, and ensure their appropriateness for the learning needs of their students. If this resource is a new application they can work with their principal to submit the resource for a privacy and security screening using the *Third-Party App* process described in the response to Question 8 below.

TIM coordinates these Privacy Impact Assessments (PIAs) which include consideration of data privacy and security for educational apps and websites. Division-licensed applications (available to all schools) have had PIAs completed by the business owner (i.e., school or DU) and reviewed by the Division FOIP Coordinator.

- a. Depending on the scope and sensitivity of the initiative, PIAs may be submitted to the OIPC for review and acceptance. Division-licensed applications include:
  - i. Google Workspace for Education
  - ii. Read and Write for Google Chrome
  - iii. Pear Deck
  - iv. Adobe Spark and Creative Cloud
  - v. WeVideo for Education
  - vi. Sora eBooks and eAudiobooks

- vii. Lumio (by SMART)
  - viii. Minecraft education edition
  - ix. myBlueprint
- b. In addition, the Division coordinates school license purchases for SmarterMarks, Reading A-Z, RazKids, and Mathletics to take advantage of volume educational pricing. These applications have all had full PIAs completed.
- c. TIM also maintains a list of Available Google Apps, Add-Ons and Extensions for Students. When a resource is suggested to be added to the approved list, the Google Play App, Google Add-on or Google Chrome Extension is reviewed for security and privacy risks. If it passes, and there are no other current Division tools available to students to achieve the desired outcome of the request, the Google Administrator will enable the ability for students to use the tool.
- d. A governance model, *Using third-party Apps in Edmonton Public Schools*, to support school decision making regarding applications has been developed by the Information Management (FOIP) team and supported by the TIPS team. The Division's process for vetting third-party apps for privacy and security is as follows:
- i. The Division FOIP Coordinator is responsible for ensuring that there is an appropriate process to ensure the safety and security of student data.
  - ii. Teachers should use Division platforms when possible. If the Division does not have an app that has been reviewed, then consideration can be given to non-Division platforms.
  - iii. Teachers should discuss and receive approval from their principals regarding what platforms that they want to use and why.
  - iv. Once the teacher has received approval from their principal, they need to determine if the app has been reviewed by the FOIP Office.
  - v. If the platform has been reviewed by the FOIP Office there will be a PIA summary document with accompanying notification for parents.
  - vi. If a summary PIA has not been completed, the teacher can request a review by the FOIP Office or conduct a review of the privacy policies and terms of use to ensure the safety of student data following the governance model.
- e. Information Management is actively improving the review of third-party apps to make the process and subsequent privacy findings more accessible, efficient and effective. For example, a teacher who wants to use Kahoot in the classroom will be able to search for it on Connect and see whether it has been reviewed by TIM. If so, an overview will be provided, along with considerations for its use with students. Since this is not a program of the Division, parents would need to be notified using the Kahoot parent notification letter (provided), posted to SchoolZone.
- 8. Does the Division provide educators with a database/resource list of safe-for-school applications? What opportunities is the Division engaging in to find efficiencies in vetting educational resources and/or creating a database? Is the administration aware of how the process for creating such a database compares across provinces?**

Administration provides teachers with a list of approved applications, Google add-ons, and browser extensions. There are currently over 35 reviewed third-party apps. The process includes:

- a. If a teacher believes a third-party application is a pedagogical or curricular fit, they work with the permission of their principal to submit it to TIM via an online form. TIM staff review these third-party apps for privacy risks and generate a PIA summary for principals and a notification letter for parents. There is a marked increase post-pandemic of digital education tools that teachers have been exposed to, resulting in a high volume of platforms that need to be formally reviewed.
  - b. At this time, each school jurisdiction in Alberta has their own process. In 2022, Alberta Technology Leaders in Education (ATLE) approached Information Management indicating that they were interested in taking on coordinating a provincial approach to third-party app management. The Information Management (FOIP Office) has been an integral part of this ATLE working committee, providing advice and resources to help move this initiative forward. Administration has been working with ATLE to create processes and resources for all school divisions to help manage third-party applications and build these resources. Administration continues to work with ATLE towards creating a province-wide solution and repository of reviewed apps that would be accessible to all jurisdictions across the province.
  - c. The B.C. government has a registry of general assessments that has been completed and approved for use across the B.C. government. Each ministry then is required to complete a checklist to ensure that the requirements are met for each area. For example, users would have access to the *Blogger general assessment* and then would complete the *Blogger checklist* for their specific use and authority.
- 9. What avenue(s) of communication will Administration, clubs, sport teams, etc. use to connect with students that is consistent throughout the Division to ensure all students are included?**
- a. SchoolZone is the primary communication platform for the Division; parents and students are provided an account upon registration.
  - b. The Division supports the use of Google Classroom, Google Mail and Google Chat as standard platforms as they are part of the core suite of products in Google Workspace for Education and are freely available on most Division and personal devices used by students. It should be noted that it is a site-based decision to allow Google Chat. By default, Google Chat is disabled in K-6 schools.
  - c. School clubs and teams can and do use other tools (e.g., group text messages, TeamSnap, etc.) that they find effective to use with their audiences. The use of these third-party applications are subject to the same privacy and security standards as third-party applications used in the classroom.
- 10. When choosing classroom activities or course work for students, what mechanisms are in place to ensure that all students have equitable access to modern electronic devices when they are needed? For example, if students are asked to use their cellphones in class, how are students without a phone accommodated?**
- a. All schools in the Division are allocated student devices through the Technology Evergreening Strategy (TES) which is managed by TIM. This strategy provides baseline student-to-Chromebook ratios (2.5:1 for K-9 schools and 3.5:1 for high schools) to ensure

- that students have equitable access to technology. Students are generally not expected to have access to a smart phone in the classroom.
- b. Providing student devices beyond these TES ratios is a school-based decision. Some schools fund additional devices through their school budgets, and some have a more formally established BYOD program.
  - c. School principals also request Chromebooks for vulnerable students through the 'Chromebooks for Kids' program of the Edmonton Public Schools Foundation. In its first year almost 600 chromebooks were placed in the hands of students across the city.

**ATTACHMENTS and APPENDICES**

ATTACHMENT I	<a href="#">Google Workspace for Education and Privacy in Edmonton Public Schools</a>
ATTACHMENT II	<a href="#">Technology Evergreening Strategy</a>
ATTACHMENT III	<a href="#">Collection and use of personal information by Edmonton Public Schools</a>
ATTACHMENT IV	<a href="#">Division Encryption Guidelines</a>
ATTACHMENT V	<a href="#">Student Rights and Responsibilities Template</a>
ATTACHMENT VI	<a href="#">Cyber Aware and Secure Campaign</a>

TK:al

# Google Workspace for Education: Privacy & Security in Edmonton Public Schools



EPSB staff & students: Do a security and privacy check-up on your account - [HERE](#) (sign-in required)

## **Google Workspace for Education (formerly known as Google Apps or G Suite for Education) -**

Edmonton Public Schools provides access to and manages Google Workspace accounts for staff and students in the Division. These secure, online applications allow staff and students to communicate and collaborate using Google-powered email, calendars, document sharing, and websites. These applications are different from public Google applications (such as Gmail) in that they are managed by the Division, do not include any advertising, and have more strict filtering and content controls. Any content (emails, documents, presentations or other files) created in or added to Google Workspace EDU is stored on servers located outside of Canada and is subject to foreign (US) laws.



Edmonton Public Schools (EPS) values the personal information that it is responsible for, and takes all reasonable means to keep that information secure. The security of Edmonton Public Schools users' data stored on Google servers is the responsibility of Edmonton Public Schools - not Google.

**EPS has extensively reviewed [Google Workspace for Education's privacy policies and security measures](#) and is satisfied that it protects the privacy of users (staff and students) as they use these tools.**

All of our privacy documentation including our Privacy Impact Assessment submitted to the Office of the Privacy Commissioner of Alberta (January 2010) are available [here](#). This PIA was completed for our initial foray into student use of Google Workspace. A current review and new privacy impact assessment is underway.

Other organisations or school Divisions planning to use Google Workspace for Education should conduct their own privacy impact assessment, consider the risks, and make decisions based on their own business and educational needs, and on the advice of their own counsel.

## Contents

Ownership and types of data on Google Workspace for Education	2
No advertising to students, teachers, or any staff.	3
Access to personal information	3
Age restrictions in Google Workspace for Education	4
Confidential information and how Google handles it	4
Google's Privacy Principles	6
Privacy of student data on Chromebooks (from Google):	6
Awareness of terms of use and privacy information for users accessing Google Workspace through student and staff portals	6
Our data, US laws, and storage on US servers	6

## Ownership and types of data on Google Workspace for Education

EPS data (staff and student email, files or documents added to or created in Drive, Google Sites (such as this) are saved on Google servers. Some of this data may be saved in the US and thus would be subject to US law. Certain staff and student records, including staff pay information, aggregated student grades, demographic, and other data (i.e. PowerSchool data) are stored on servers in the Centre for Education behind our EPS firewall. In 2010 EPS completed a detailed Privacy Impact Assessment (accepted by Alberta's Privacy Commissioner) and EPS is satisfied that [Google Workspace for Education](#) (which differs from public Google or Gmail accounts) meets our requirements for security and privacy. Specifically:

- **All of a user's data is owned by the user and Edmonton Public Schools and Google makes no claim on the content. Google does not scan or index Google Workspace EDU for advertising or other purposes.**
- Google Workspace is governed by the detailed Google Workspace EDU [Privacy Policy](#), and the [EDU Trust policy](#), which ensures they (Google) will not inappropriately share or use personal information placed in our systems.
- The Google Workspace for Education Terms of Service contractually ensures that students, faculty, and staff are the owners of their data.
- Because faculty, staff & students own the data they put into Google Workspace applications, we believe it should be easy for your users to move their data in and out of our systems.



- The controls, processes and policies that protect user data in our systems have obtained a SAS 70 Type II attestation and will continue to seek similar attestation.
- Google complies with applicable US privacy law, and the Google Workspace EDU Terms of Service can specifically detail their obligations and compliance with FERPA (Family Educational Rights and Privacy Act) regulations.
- Although these laws have no legal standing in Alberta or Canada, EPS believes that they do demonstrate Google's commitment to the protection of personal information of our users.

At EPS we are using Google Workspace for Education for staff and student email, documents, presentations, websites, etc. (i.e. data). The data we are collecting and which will be stored on Google's servers also includes student login information (First Name, Last Name, User name), and their network login password. Passwords are encrypted and cannot be read by neither EPS staff nor Google.

- [Google Workspace for Education: Introduction to Privacy & Security \(Video\)](#)
- [James Snow, Security Strategist at Google - Security of data at Google](#)

EPS is confident that [Google Workspace for Education privacy and security policies](#) regarding the protection of personal information in accordance with our Division policies. However, under U.S. law our Division cannot guarantee against the possible secret disclosure of information to a foreign authority (e.g. NSA) as a consequence of foreign laws. Similar laws exist in Canada. EPS is aware of the risk associated with a possible "secret disclosure" and believes that the value and services provided outweigh the potential risks. Google continually updates and improves their tools and online security.

## No advertising to students, teachers, or any staff.

For Google Workspace for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with a Google Workspace for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an Google Workspace for Education account. Which means your school's content is not processed by Google's advertising systems.

This declaration covers the Core Google Workspace EDU. This includes Google Mail, Chat, Meet, Jamboard, Keep, Cloud Search, Classroom, Contacts, Drive (inclusive of Docs, Sheets, Drawings, Forms, Slides), Sites, Groups, Vault (Admin use only), & Calendar. It does NOT include other Google Workspace that a user may access through their Google Workspace EDU account, such as Blogger or [YouTube](#), or any other third-party app that a user authorizes through their Google Workspace EDU account. For example, a student who signs into a Chromebook with their @share.epsb.ca account and clicks on Blogger, is essentially authenticated through to the same version of the public Blogger application that any GMail user would use.

- [Google Workspace for Education: Ads & Ad Profiles \(Video\)](#)

## Access to personal information

Access to staff or student Google Workspace accounts is provided through our secure staff (Connect) and student (SchoolZone) portals, and via Google Workspace Apps (e.g. GMail) and Chrome OS devices. Remember that your EPS username and password are all that are needed to access your account, so it is very important to keep your password secure, and to change it regularly. If you want to be more secure, you should also turn on 2-factor authentication (see how here).

The following persons, positions or employee categories have access to **student** data (email, chats, sites, browser history (including [YouTube](#) history, etc.), and through this, to their Google Workspace EDU accounts and information:

- Global access to all Google Workspace EDU (staff or student), account settings (usernames, alias'), user-created sites:
  - 2 senior District Technology technical analysts are the EPS Google Workspace domain administrators. The domain administrators can:
    - Provide access to Central Office staff in event of a Division investigation;
    - View statistics regarding your account, such as information concerning your last login or data storage usage;
    - Reset your account password, suspend or terminate your account access and your ability to modify your account;
- Access or retain information stored as part of your account, including your email, contacts and other information; and,
- Receive account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
- Delete your account and all data associated with that account
- Access to individual staff and student accounts (EPS Network resources):
  - School technicians have access to staff and student accounts at their assigned schools or departments.
  - School Administrators and SIS personnel have access to student accounts at their schools.
  - Teachers have access to student accounts for those students enrolled in their classes.

These persons can:

- Access or retain information stored as part of your account, including your email, contacts and other information; and,
- Receive account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.

Google employees will access your account data only when one of the EPS domain administrators grants Google employees explicit permission to do so for troubleshooting purposes. During the course of

troubleshooting an issue or other investigation, the Google Support team may ask for the creation of a test administrator account, solely to be used to resolve the particular issue at hand.

With Google Workspace EDU, students/staff can export their files when they leave the District. The Google Workspace EDU administrator for Edmonton Public Schools will determine when data will be removed/deleted from our Google Workspace EDU domain. Under normal circumstances accounts will be deleted in October after the user leaves the Division (just in case they come back).

## Age restrictions in Google Workspace for Education

In the public sphere, many Google Workspace products have an under-13 restriction on use. In Edmonton Public Schools' use of Google Workspace EDU, it is our responsibility to ensure that the provisions of *The FOIP Act* are met. This includes ensuring the security of the data, limiting access and notifying parents that the data is stored outside of Canada and subject to U.S. laws. Parental consent under *The FOIP Act* is required when the school Division or school discloses personal information of students to 3rd parties that are outside of the Division (that we have not contracted service to, i.e. Third party apps).

Google Workspace EDU is a program of the Division and we do not ask parent consent for students to access Google Workspace. Per the Google Workspace EDU Agreement, any school administering it acknowledges and agrees that it is solely responsible for compliance with *The FOIP Act*, including, but not limited to, making parents aware of the collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users. If students or school staff are posting information outside of Google Workspace EDU where the general public may have access to the information or third-party applications are collecting personal information, then parent consent is required.

Parents are notified on the [Division FOIP Statement](#) that Edmonton Public Schools uses Google Workspace and/or could be also notified in a school's "Acceptable (or Responsible) Use of Technology agreement" (which makes users and parents aware of the use of Google Workspace and/or other technology services at the school), a post on SchoolZone or an informational letter sent home. All EPS schools have this information included on their public school web pages. For more information on complying with *The FOIP Act*, see <http://www.servicealberta.ca/foip/>.

## Confidential information and how Google handles it

Google operates one of the most robust networks of distributed data centres in the world ([read more](#) in their security and privacy policy site). The protection of the intellectual property on these servers is critically important to us -- in fact, employees at Google, Inc. rely upon the same Apps production environment used by our education customers.

Google brings you the latest technologies and some of the best practices in the industry for network application security and user privacy, as summarized below:

- It's your content, not Google's. Your Google Workspace content belongs to your school, or individual users at your school. Not Google.
- Parents can visit [myaccount.google.com](https://myaccount.google.com) while signed in to their child's Google Workspace for Education account to view and manage the personal information and settings of the account.
- They don't look at your content. Google employees will only access content that you store on Google Workspace for Education when an administrator from your domain grants Google employees explicit permission to do so for troubleshooting.
- They don't share your content. Google does not share personal information with advertisers or other 3rd parties without your consent.
- Google sometimes scans content. And for very good reasons, like spam filtering, anti-virus protection, or malware detection.
- Their systems scan content to make the Google Workspace apps work better for users, enabling unique functionality like powerful search in Gmail and Google Docs. This is completely automated and involves no humans.
- Note that there are a few common-sense exceptions to the points above, like valid legal processes and maintaining the safety and security of our systems. For more information, see Google's detailed [Privacy Policy](#), [Privacy Principles](#), and [Terms of Service](#).
- [Google Workspace for Education: Data Ownership \(Video\)](#)
- [Inside a Google Data Center \(Video\)](#)

The section below is from section 7 of the [Google Workspace for Education Agreement](#):

#### 7. Confidential Information.

7.1 Obligations. The recipient will only use the disclosing party's Confidential Information to exercise the recipient's rights and fulfil its obligations under the Agreement, and will use reasonable care to protect against the disclosure of the disclosing party's Confidential Information. The recipient may disclose Confidential Information only to its Affiliates, employees, agents, or professional advisors ("Delegates") who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep it confidential. The recipient will ensure that its Delegates use the received Confidential Information only to exercise rights and fulfil obligations under this Agreement.

7.2 Required Disclosure. Notwithstanding any provision to the contrary in this Agreement, the recipient or its Affiliate may also disclose Confidential Information to the extent required by applicable Legal Process; provided that the recipient or its Affiliate uses commercially reasonable efforts to (a) promptly notify the other party before any such disclosure of its Confidential Information, and (b) comply with the other party's reasonable requests regarding its efforts to oppose the disclosure. Notwithstanding the foregoing, subsections (a) and (b) above will not apply if the recipient determines that complying with (a) and (b) could (i) result in a violation of Legal Process; (ii) obstruct a governmental investigation; or (iii) lead to death or serious physical harm to an individual.

## Google's Privacy Principles

Google provides many resources for students and parents. For some of these, see <http://www.google.com/goodtoknow/>.

EPSB also provides teachers, administrators and parents with great resources as well as our [own Digital Citizenship site](#).

## Privacy of student data on Chromebooks ([from Google](#)):

### Google Workspace for Education Core Services

The Google Workspace [Core Services](#) -- Gmail, Calendar, Classroom, Drive, Docs, Sheets, Slides, Contacts, Groups, Vault, Meet, Chat, Jamboard, and Classroom -- are the heart of Google's educational offering to schools. Students' personal data in these Core Services is only used to provide the services themselves, so students can do things like communicate using email and collaborate on assignments using Google Docs. There are no ads in these Core Services, and student data in these services is not used for advertising purposes.

## Awareness of terms of use and privacy information for users

Edmonton Public Schools will make all reasonable efforts to ensure that all Google Workspace users (staff and students) are made aware of the Division's acceptable use guidelines.

Our responsibility under *The FOIP Act* is to ensure that EPS has made reasonable security arrangements to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. In addition EPS needs to inform users as to what information we're collecting and which information Google may use and have access to, and that their data including e-mail will be stored outside of Canada and subject to foreign laws. For example, in order to set up students with Google accounts to be accessed through SchoolZone, we have set up synchronization between our Active Directory (AD) and Google.

This page is linked within the Google Workspace tab in SchoolZone for parents and students.

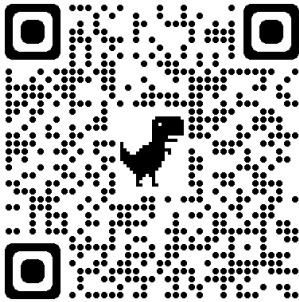
## Our data, US laws, and storage on US servers

Currently Google only has [two data centres in Canada](#). Google has many geographically dispersed data centres to ensure that there is a high degree of redundancy. As well, they are located throughout the world to reduce risks in the event of a failure in one of the data centres. Due to Edmonton's geographic location, EPS data will be located on servers in the U.S.. The impact of foreign legislation on privacy is a concern whenever data storage is outsourced outside of Canada or to a non-Canadian company. *The FOIP Act* recognizes this, and while it does not restrict or prohibit this kind of outsourcing, it does require

that public bodies such as ours ensure that reasonable steps are taken to mitigate privacy risks.

The [USA Freedom Act](#) (replaced the Patriot Act) is a high profile example of the kind of foreign legislation people are most often concerned about. While the Act does allow American Courts to order US companies to provide them with limited information when necessary for a specific counter-terrorism investigation, Patriot Act orders are exceedingly rare. The ownership of EPS data stored in Google servers remains with Edmonton Public Schools, regardless of the physical location of the data. Google's policies and procedures require that the EPSB be notified if access to our information is requested, except when specifically prohibited by law.

*(From City of Edmonton- with thanks.)*



*View this document on the web.*

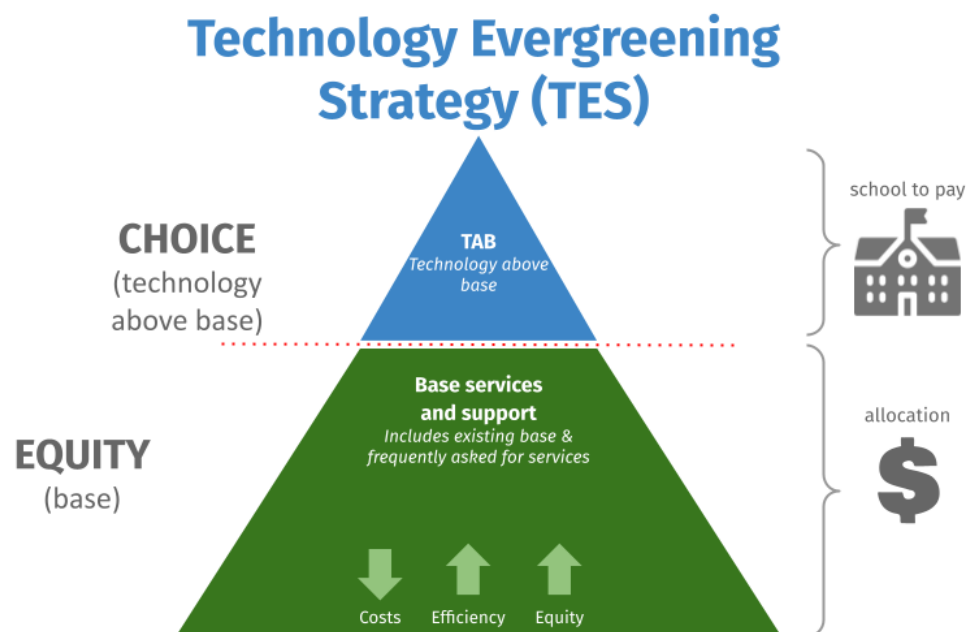
# Technology Evergreening Strategy

## Guiding Principles

Division Technology Policy (DK.BP) states that “[t]he Board supports a learning and teaching environment in which Division students and staff have equitable access to devices, applications, infrastructure and networks that facilitate the effective integration of technology.”

To maintain equity of access to technology, increase efficiency and reduce administrative workload, we have shifted to an enterprise approach (through central allocation of funds) so that:

1. Staff computers and network infrastructure is supplied and supported for central departments.
2. A base level of access to student devices, staff computers, classroom projection systems, print devices and network infrastructure is supplied and supported for all schools. Schools may purchase additional technology beyond the base level of technology supplied, but would not need to budget for TES support for most hardware beyond the base level.



# Goals

## Equitable Access to Technology for Learning

All staff and students should have access to the technologies they need for teaching and learning. Access to surplus funds has allowed the Division to achieve relative equity of access to technologies for teaching and learning. Every school meets the Division ratios regarding Chromebooks, all staff have reliable workstations, and all classrooms have a working, mounted projector. Technology and Information Management now maintains this equity by employing a strategic approach to evergreening and supporting technology.

## Reducing Costs

Past experience has shown that when we purchase known quantities in large volumes we will see prices lower than our already well-negotiated contracts. We purchase technology hardware using a planned, strategic approach, realizing overall cost savings for the Division.

Support costs to the Division are reduced over time as we employ the evergreening model, which maintains a fleet of reliable devices for all users.

## Creating Efficiencies

We aim to increase efficiency through logistical improvements, scheduling installations year-round and reducing support time and administrative workload in schools (resulting in lower costs):

- a. Managing technology hardware at an enterprise level allows TIM to plan and execute replacements in a coordinated manner, involving school staff, TIM Technicians, Distribution Centre staff, and Integrated Infrastructure Services personnel.
- b. The historical ad hoc approach to purchasing and deploying technology led to difficulty in scheduling technical and maintenance staff; the planned approach will allow us to optimally staff and plan for year-round deployment.
- c. Setting a base level of technology and shifting from cost-recovery to allocation for technical support reduces administrative workload since principals and other school staff do not have to plan and budget for replacements of core technologies, a base level of student-devices, or technical support.



# Collection and use of personal information by Edmonton Public Schools

Edmonton Public Schools collects, uses and discloses personal information of students and parents as outlined under the provisions of the *Education Act* and in accordance with Section 33(c) of the *Freedom of Information and Protection of Privacy Act (FOIP)*.

This is required for educational purposes and to support a safe and respectful learning and working environment for students and staff. For the purposes outlined above, consent is not required to gather and share this information.

We may use student information, including name, grade, image or contact information to:

- provide educational programming to students
- confirm their absence or for emergencies
- include in internal communications such as, individual, class, team or club photos or videos—which may appear in the school calendar, newsletter, yearbook or SchoolZone
- show on artwork or other material on display at the school or another Edmonton Public Schools' site
- identify students' name for honour rolls, scholarships or event programs
- create and manage student network IDs
- share information with Alberta Education

These are some examples and not intended to be an all-inclusive list.

## Using Google and other educational platforms

Edmonton Public Schools uses Google Workspace to communicate and collaborate online. Students and staff use Workspace tools like Gmail, Google Meet, Docs and Drive. A Google Workspace account is created for students when they register for school. Records and files created in Google Workspace are stored on servers located outside of Canada and are subject to foreign laws.

Edmonton Public Schools has a number of educational platforms that are licensed by the Division. This includes Mathletics, Raz-Kids, WeVideo, Pear Deck, SmartLearning and more. Your school can tell you which platforms they are using.

## Monitoring for safety

Edmonton Public Schools uses monitoring software when students and staff are signed into their school accounts during school hours. This software ensures each student and staff member is provided with a respectful and safe learning environment. Content-filtering software runs whenever a student is using their school account.

## Activities or events open to the public

Students may attend or participate in activities where the general public, including media, is present. Examples include sports events, concerts, cultural programs, clubs, field trips, graduation or other ceremonies.

If students are recorded in photos or videos, Edmonton Public Schools cannot control or prevent the distribution of these photos, videos, images or other personal information.

## Complete the consent form

Parents can complete the *FOIP Consent Form* in SchoolZone to let us know how their child's information may be used outside of Edmonton Public Schools. The form can be updated any time during the school year.

The school or classroom teacher will keep you informed as to how your child's information may be used outside of school.

## More information

Contact the school principal if you have any questions or concerns about the collection or intended uses of this information. You can also reach the Division FOIP Coordinator at [foip@epsb.ca](mailto:foip@epsb.ca) or **780-429-8350**.



# Frequently asked questions

## about the collection and use of personal information

### **Why am I being asked for personal information about me and my child on the school's registration form?**

The school requires this information for educational purposes and to support a safe and respectful learning and working environment of students and staff. This is required by the *Education Act* and Alberta's *Freedom of Information and Protection of Privacy (FOIP) Act*.

In addition, we are required to provide relevant information to Alberta Education as required by the *Education Act*.

### **Will pictures or videos be made of my child without my permission?**

School staff may take pictures or videos for use within the Division, school or posting to SchoolZone.

### **Will my child's picture or name be on the Internet?**

Their information may be posted on SchoolZone, a secure website used by schools and Division parents. SchoolZone cannot be accessed by anyone outside the school community. Parents are reminded to not copy, download or share pictures or videos from SchoolZone

Their information may also be posted on public websites or shared outside the school community by the Division if you gave consent on the FOIP Consent Form. Your school or classroom teacher will provide additional information as required.

### **Can I consent to my child's information being used for educational platforms but not on social media?**

Yes. You can let us know on the FOIP Consent Form. If you have questions about the educational platforms that your child's teacher is using, contact the school or the teacher.

### **Does my child have to have a Google account?**

Yes. Google Workspace is the Division's communication platform. This allows students to access Google tools like Google Classroom, Gmail, Meet and Drive. Your child's Google account may also be used to sign in to external educational platforms.

Visit [bit.ly/DivisionGoogleWorkspace](https://bit.ly/DivisionGoogleWorkspace) to learn about Google Workspace at Edmonton Public Schools.

### **How is YouTube used in Edmonton Public Schools?**

Students who are signed into YouTube using their Google Workspace account (at school or home) can view YouTube content that has been approved by Google's AI-enabled filter or by Division staff. Visit [bit.ly/DivisionYouTube](https://bit.ly/DivisionYouTube) to learn about safety features for YouTube.

### **Can other students see my child's email address?**

Currently students' email address, name and grade may be visible internally to other staff and students through email contacts. Students may upload a photo or icon if they choose, but this is not required.

### **What if the media come to the school?**

Your child will not be recorded by the media unless you signed the Media Consent Form. Your child's school will tell you if a media event is happening.

## EPS Encryption Guide

### When and how to use encryption.

When sending sensitive personal information and/or confidential information outside of the Division, staff should use encryption.

Email and attachments sent **internally**, to other EPS staff, are already sent securely through our normal EPS Google Mail and additional encryption is not required for these messages, however, ensuring that you have the **correct** individual is key. Some tips to ensure that you have the correct individual:

- Internally, check on Connect the individual's email address and location (copy & paste email address).
- Always double-check email addresses that are Autofilled from Google.
- External address - copy and paste from a confirmed email address or reply to a confirmed email address. If you have to type an email address from another source, send a test email to confirm that you have the correct email address, let the recipient know that you are sending a test email and ask them to confirm that they have received it.

In some circumstances, it may be appropriate to encrypt a particularly sensitive document and attach it to an email even when it is being sent to an internal email address.

If an email attachment is being sent outside of the Division, and it contains sensitive personal information of students or staff information it may need to be encrypted (e.g. Alberta Education, ASEBP, AHS, another school district, home email addresses, etc.) Key considerations include:

- Send a test email to confirm the recipient's email address and ask for a confirmation. If you don't receive a confirmation, follow up (phone) before sending the documents.
- Provide the password over the phone or to a different email address.
- Never send the encrypted document in the same email as the password.
- If required, staff can encrypt confidential documents within the Division for an extra layer of security if needed. For example, the results of an internal investigation report.

### What is encryption?

Encryption is a process that changes data from its original format into a new format that requires a password or key to translate it back.

### When should encryption be used?

Encryption should be used when sending sensitive personal information **outside** of the Division via email or saving personal information to a portable device (i.e. laptop, memory stick). The volume and type of information determine if encryption should be used. For example:

- The more information is included, the more sensitive the email or its attachments become such as a spreadsheet that includes; student name, grade, school, EPSB or AB Education ID number, demographic information, medical information, family status, etc. This list would be considered sensitive and confidential and would require encryption. Compared to a class list that only had a student's name, however, a spreadsheet listing ALL students should be encrypted due to the volume of information.

- Confidential reports such as psychological assessments, medical reports, the complete student record, etc.

## DIVISION ENCRYPTION TOOLS

**Google Mail Encryption (GME)** Email Encryption for select EPS staff provides the ability to securely send encrypted emails and attachments as easy as sending any other mail. If Email Encryption has been enabled for you, simply include [encrypted] in the subject line. Click on this link to learn more about [Google Mail Encryption \(Zix\)](#).

### Google Confidential Mode

Staff can send messages and attachments with Gmail's **confidential mode** to help protect sensitive information from unauthorized access. You can use **confidential mode** to set an expiration date for messages or revoke access at any time. Be aware that recipients of the confidential message will **not** have options to forward, copy, print, and download. Click on this link: [Send & open confidential emails](#) for more information.

### Encrypting PDF documents

You can easily encrypt individual PDF documents. By encrypting the documents, if an email was inadvertently sent to the wrong individual, the document will not be able to be opened without the password provided the password was given to the recipient by other means such as phone, through an alternate email address, etc (i.e. phone, different email address, etc.) Once the document is encrypted you can attach it to an email. Note: Passwords can also be removed from PDFs when no longer required. Click on this link to learn how to [encrypt a PDF document](#).

## CREATING & MANAGING PASSWORDS

If you are regularly sharing data with an external organization the most secure way to do this is to have a secure file-sharing system. If that is not an option, using encryption is required.

If you are sending the same type of document to various people, a formula for creating a password is recommended. For example: Department Name+Report Name+Initials+Year = FOIPReleasepkgMH2020. Once again keep track of the password and to whom it was sent.

It is always a good idea to have some type of formula even if you only send documents occasionally. For example: Department Name+Document name+recipient initials = FOIPAssessmentMH. Once again keep track of the password and who you sent it to. You could also use a favourite phrase and customize it. For example InspireKids2day2021!

TIP: When applying the password, save it as a new file with an extension of "PW" so you know it is password protected. When a PDF has a password applied to it, the document will be encrypted when saved. If you don't want your original to be encrypted, you will want to save it as a new file. For example "Confidential Encryption Report" is the original file, once the encryption is applied you will want to save it as a new file "Confidential Encryption Report - PW". This way you always have the original unencrypted document to access. In addition, you can remove the password by clicking on the Security Tab/select Security Method/No Security, save the changes.

### What else?

Turn off the feature in Gmail settings to automatically add new contacts for auto-complete. Go to “Create Contacts in Autocomplete” in the Gmail setting and select “I’ll add contacts myself”. One should always consider adding individuals for auto-complete with who they regularly correspond.

Personal information should never be stored on a portable device (i.e. laptop, memory stick) without encryption.

### Privacy Breach

All staff are responsible for ensuring the confidentiality and safety of the personal information they have access to. A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. In our division, this usually occurs because of errant e-mails, lost or stolen laptops, documents and personal information not stored on encrypted devices or are left unattended as well as paper documents left unattended, handed out randomly, etc.

Privacy breaches must be reported to your supervisor, who will contact the Division FOIP Coordinator for assistance. The following resources are available in the event of a privacy breach.

- [Privacy Breaches and Transporting Personal Information](#)
- [Best Practice in the Event of a Privacy Breach](#)

### Other Resources:

- CN.AR – [Creation, Use, and Maintenance of Division Information](#)
- CN.BP – [Managing Division Information](#)
- [Encryption Guidelines for Human Resources](#)



# Student Rights and Responsibilities 2022-2023

**School Name**

Street Address, Edmonton, AB Postal Code

Phone: 780-XXX-XXXX

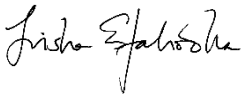
Email: [schoolname@epsb.ca](mailto:schoolname@epsb.ca)Website: [school.epsb.ca](http://school.epsb.ca)Principal: **Principal Name**Updated: **Date**

## Our Commitment to High Quality Learning Environments

At Edmonton Public Schools, we are deeply committed to the success and well-being of our students. Each student deserves a welcoming, inclusive, safe and healthy learning environment that supports their learning, respects diversity, and nurtures a sense of belonging.

As a Division, we have established clear behaviour expectations for all students, from Kindergarten to Grade 12. The expectations are outlined in the Board's [Student Behaviour and Conduct Policy](#) which was developed in consultation with students, parents, staff and community members. The policy outlines the rights and responsibilities of students and our expectations for student conduct, and the potential responses when students demonstrate unacceptable behaviour.

The role of parents and families in their child's education plays a vital role in promoting positive student behaviour. Partnerships with families continue to make a difference for our students and staff. By working together, we will ensure our students learn the importance of good character and conduct, and our schools will remain safe and secure places to learn and thrive.



Trisha Estabrooks  
Board Chair

## Student Success and Safety—Our Highest Priorities

It is our shared responsibility to ensure that each student can learn and realize their potential within a safe and caring learning environment. In addition to teaching the necessary learning outcomes, our schools are places where students can develop the character and skills needed to become responsible, respectful, compassionate and successful citizens.

School staff use the *Education Act*, S.A. 2012, c.E-03, Board Policy [HG.BP—Student Behaviour and Conduct](#) and Administrative Regulation [HG.AR—Student Behaviour and Conduct](#) as the basis for creating this **Student Rights and Responsibilities** document. This document is designed to communicate expectations, and balances the overarching rights and responsibilities that are communicated in our policy with the unique context of each school. The expectations and processes outlined in this document are implemented by principals in collaboration with school staff, parents and local communities.

Ensuring each student can thrive in a safe, productive and welcoming learning environment is essential to our work in improving student achievement and high school completion rates. By working together to promote positive attitudes and responsible, respectful behaviour in our schools, we believe students will receive the greatest benefit during their educational journey.



Darrel Robertson  
Superintendent of Schools

## Supporting Student Success

Members of the Edmonton Public Schools community, including students, parents, staff and trustees, have a shared responsibility to help students be successful in school. Safety and well-being is fundamental to our students thriving as learners, and experiencing success and fulfillment both at school and in their lives. This *Student Rights and Responsibilities* document has been created to communicate clear expectations for how our students are expected to behave in order to ensure they become the best students and citizens they can be.

### Parents support their child's success and positive behaviour by:

- taking an active role in their child's personal and academic success
- reviewing expectations outlined in this document with their child and helping them develop the skills required to meet the school's expectations
- helping them to attend school regularly and punctually
- encouraging and modelling collaborative, positive and respectful relationships with others in the school community
- contributing to a welcoming, caring, respectful, and safe learning environment
- reporting to the school any circumstances which may impact student safety

### Students are responsible for their behaviour and effort, and are expected to:

- contribute a welcoming, caring, inclusive, respectful and safe learning environment that commits to anti-racism and equity
- learn, practice and demonstrate positive personal and interpersonal skills and attributes
- use their abilities and talents to gain maximum learning benefit from their school experience
- attend school regularly and punctually
- be accountable for behaviour which impacts others in the school, whether or not the behaviour occurs within the school building or during the school day or by electronic means

### School staff will help your child succeed by:

- providing a welcoming, caring, respectful, inclusive and safe learning environment that respects diversity, commits to anti-racism and equity, and fosters a sense of belonging
- ensuring that students and parents understand the school's expectations for student behaviour
- establishing supports and processes at the school to proactively guide positive student behaviour
- helping students develop and practice the skills and attributes to meet these expectations
- working with students, parents and other school staff to address behaviour concerns, including implementing appropriate responses to address inappropriate student behaviour

To support a shared understanding of the language and intent of this document, refer to the [glossary](#) for a definition of terms.



## Our Belief and Commitment

At <School Name> we believe:

The section:

- captures the school's overarching commitment to providing a welcoming, caring, respectful, inclusive and safe learning environment that respects diversity, commits to anti-racism and equity, and fosters a sense of belonging
- articulates broad aspirations for positive student behaviour and an environment conducive to learning
- introduces a broad perspective on the schools' overall approach to student behaviour and conduct
- should be brief and positive in tone

Refer to the Implementation Guide for suggestions and examples for this section.

### Optional

If desired, the area below can be used to add further information or images related to your school Belief Statement.

Some examples for this space include:

- school logo or mascot
- motto
- vision and mission statement
- a specific school focus or program (e.g., Leader in Me, 7 Habits etc.)
- related image or quote to supplement the Belief Statement

## Rights and Responsibilities

Our school Division recognizes the following fundamental rights and responsibilities:

All students have the right to be treated with dignity, respect and fairness by other staff and students.

Students, parents, staff and trustees have a shared responsibility to create and support welcoming, caring, respectful, inclusive and safe learning environments.

All members of our school community are expected to respect diversity and not engage in any form of bullying, harassment, threats, intimidation or discrimination on the basis of race, religious beliefs, colour, gender, gender identity, gender expression, physical disability, mental disability, ancestry, place of origin, marital status, source of income, family status or sexual orientation.

Students and parents have a right to be informed about Division and school expectations for student behaviour. To support this right, all schools' Student Rights and Responsibilities documents will be posted on SchoolZone and on school websites.

### Anti-Racism and Equity

All members of the Edmonton Public Schools community:

- have the right to learn and work in an environment that:
  - is free of discrimination, prejudice, and racism
  - recognizes diversity as a strength
  - supports each individual to be included and feel represented in their greater school community, and
- have the responsibility to:
  - demonstrate respect for diverse cultural perspectives, traditions, languages, beliefs and values
  - learn and work together as a part of the broader school community to end racism and discrimination
  - report, not participate in, and not tolerate acts of racism or discrimination.

These rights and responsibilities are communicated in the *Alberta Human Rights Act* and the *Education Act* and are reinforced in Division policies and regulations which are publicly available and include [AE.BP—Welcoming, Inclusive, Safe and Healthy Learning and Working Environments](#), [HG.BP—Student Behaviour and Conduct](#), [HG.AR—Student Behaviour and Conduct](#), [HFA.AR—Sexual Orientation and Gender Identity](#) and [HAAB.BP – Anti-Racism and Equity](#).

**Optional**

At <School Name>, everyone in our school community has the right to learn and work in an environment that is respectful, inclusive, safe, healthy and focused on learning and success. In order to preserve these rights, students must also be aware of their individual responsibilities.

Insert general or specific statements about any additional student rights and responsibilities within the school here.

Refer to the Implementation Guide for guidelines and examples to complete this section.

## Student Behaviour Expectations

To ensure that <School Name> is a positive learning environment for everyone, all students are expected to comply with expectations set by our school Division and mandated by the *Education Act*, as well as school rules which are in place for the benefit of all members of our school community. These expectations apply to all students in the school community, including while learning and engaging with others both in-person and online.

Board Policy [HG.BP – Student Behaviour and Conduct](#) and Administrative Regulation [HG.AR – Student Behaviour and Conduct](#) outline that students are expected to behave in accordance with section 31 of the *Education Act* which states that, a student, as a partner in education, has the responsibility to:

- attend school regularly and punctually,
- be ready to learn and actively engage in and diligently pursue the student’s education,
- ensure the student’s conduct contributes to a welcoming, caring, respectful and safe learning, environment that respects diversity and fosters a sense of belonging,
- respect the rights of others in the school,
- refrain from, report and not tolerate bullying or bullying behaviour directed toward others in the school, whether or not it occurs within the school building, during the school day or by electronic means,
- comply with rules of the school and the policies of the Board,
- cooperate fully with everyone authorized by the Board to provide education programs and other services,
- be accountable to the student’s teachers and other school staff for the student’s conduct, and
- positively contribute to the student’s school and community.

Furthermore, students are expected to:

- resolve conflict or seek assistance to resolve conflict in a peaceful, safe, and non-threatening manner that is conducive to learning and growth. Strategies for addressing conflict between students may include counselling, mediation, or forms of restorative practice.
- use school and personal technology appropriately and ethically
- ensure that they conduct themselves with academic integrity and refrain from and report all incidents of academic misconduct including, but not limited to, cheating and plagiarizing.

### Regular Attendance – It’s the Law

Regular attendance is strongly linked to student academic success and a student’s sense of belonging at school. The *Education Act* reminds parents and students that students are expected to attend school and be punctual every day. Students are only considered to be excused from attending school if they must be away due to:

- sickness or other unavoidable cause
- the day being recognized as a religious holiday by the religious denomination that the child belongs to
- suspension or expulsion
- an exemption from compulsory attendance granted by the Board for a defined period of time

### Expectations for Student Attire

At Edmonton Public Schools, students are expected to dress in a manner that reflects a welcoming, respectful, inclusive, safe and healthy learning environment. School expectations for student attire take into account a student's right to fairness, dignity and respect, and will not discriminate against students based on race, gender, gender identity, gender expression, sexual orientation, ethnicity, religion, cultural observance, socio-economic status, or body type. Some examples of this are durags, turbans, hijabs and burkas.

Student safety and wellbeing are our highest priorities. Students are also expected to refrain from wearing, carrying, or displaying any clothing or accessories which pose a safety hazard. Students are not permitted to wear lanyards around their neck.

### Student Responsibilities in Relation to Public Health

The Division's first priority is always to ensure the health and wellbeing of students and staff. Students are expected to abide by protocols and expectations that are established at the school, Division, or provincial level for K-12 education, in relation to public health.

These expectations will be communicated to students, parents, and staff by the school administration in a timely manner, and may be updated over the course of the school year in relation to a public health concern as advised by Alberta Health Services.

### Optional

**In addition to the Division expectations outlined above, students at <School Name> are expected to:**

Schools may insert general or specific statements about any additional student behaviour expectations within the school here.

Refer to the Implementation Guide for instructions and examples for this section.

**\*Note:** Schools **may choose** to add additional text to this "Student Behaviour Expectations" section **and/or** the "Rights and Responsibilities" section of this document. **At least one** of the two sections must be completed with school specific expectations.

School Name

## Responsible and Ethical Use of Technology

Our Division is committed to assisting students to become ethical, informed digital citizens. We strive to ensure that appropriate and responsible technology use supports high quality teaching and learning, while also ensuring a respectful, inclusive, and safe learning and working environment.

Technology refers to any computer, software, network, or internet access on any electronic device, including those owned by the student or the Division. Division technology is intended for educational purposes and cannot be used for purposes that are illegal, unethical, disrespectful, hateful, inappropriate, or that cause harm.

Students are accountable for their behaviour when using technology, including when a student's online behaviour outside of the school building or beyond the school day impacts others in the school community. A range of responses as outlined in [HG.BP – Student Behaviour and Conduct](#) and [HG.AR – Student Behaviour and Conduct](#), including loss of technology privileges, may be put in place to address unacceptable use of technology.

**As digital citizens, students have the following responsibilities:**

- **Demonstrate respect and integrity**
  - understand that expectations for conduct and academic integrity while online, including when using personal devices and outside of school hours, are consistent with school and Division expectations (for example, students should only join online classes in which they are enrolled)
  - use good judgment and participate appropriately in online environments such as meetings, chats, and other applications, and when posting or sharing digital content
  - communicate in a manner that is appropriate, respectful and inclusive at all times
  
- **Be safe and secure**
  - protect passwords and personal information of self and others including photos, name, age, address and other contact information
  - students must ensure they log in only to their assigned EPSB account, and log off devices and meetings when finished
  - obtain permission before downloading files, including games, music, and movies
  - report, and refrain from searching, viewing, downloading, or sharing, any illegal or inappropriate content
  - do not record or share any audio or video of in-person or online classrooms or other learning activities
  - obtain consent before photographing, recording, or sharing a photo or recording of another person
  
- **Respect and protect property**
  - demonstrate proper care and security of personal and Division technology
  - understand that students are responsible for the care and security of personal devices brought to school

**Optional**

**In addition to the Division expectations outlined above, students at <School Name> are expected to:**

Schools may insert general or specific statements about any additional student behaviour expectations regarding responsible use of technology within the school here. This could include any school level technology agreements or guidelines that have been established.



## Unacceptable Behaviour

Any behaviour, whether or not it occurs on school property, or within the school day, which disrupts the educational atmosphere of the school or which interferes with the rights of others to learn, to be respected or to feel safe is unacceptable.

As outlined in Board Policy [HG.BP – Student Behaviour and Conduct](#) and Administrative Regulation [HG.AR – Student Behaviour and Conduct](#) and supported by the *Education Act*, unacceptable behaviour includes, but is not limited to:

- behaviours that interfere with the learning of others and/or the school environment
- behaviours that create unsafe conditions
- acts of bullying, harassment, threats, or intimidations whether it be in person, indirectly, or by electronic means
- physical violence
- retribution against any person who has intervened to prevent or report bullying or any other incident or safety concern
- possession, use, or distribution of substances restricted by federal, provincial, municipal, Division or school authorities
- any illegal activity such as:
  - possession, use, or distribution of illegal substances
  - possession of a weapon or use of a weapon (or replica) to threaten, intimidate or harm others
  - possession, use, display, or distribution of offensive messages, videos or images
  - theft or possession of stolen property
- any breach of rules and expectations established by Division administrative regulations or a school-based code of conduct
- failure to comply with *Education Act*, section 31 regarding student responsibilities

**Bullying and Conflict**

Bullying is defined in the *Education Act* as repeated and hostile or demeaning behaviour by an individual in the school community where the behaviour is intended to cause harm, fear or distress to one or more other individuals in the school community, including psychological harm or harm to an individual's reputation. Bullying also includes the distribution of an intimate image of another person knowing that the person depicted in the image did not consent to the distribution, or being reckless as to whether or not that person consented to the distribution.

**Bullying** can take different forms:

- physical (e.g., pushing, hitting)
- verbal (e.g., name-calling, threats)
- social (e.g., exclusion, rumours)
- electronic (e.g., using technology to harass or threaten)

**Conflict** occurs when there is a breakdown in relationships between individuals that results from a disagreement or misunderstanding. While conflicts may require adult intervention, they are considered to be a natural part of how students learn to navigate relationships.

All students are expected to refrain from, report and not tolerate bullying or bullying behaviour directed toward others in the school, whether or not it occurs within the school building, during the school day or by electronic means. Students are also expected to resolve conflict or seek assistance to resolve conflict in a peaceful, safe, and non-threatening manner that is conducive to learning and growth. School staff can help address conflict between students using strategies that may include counselling, mediation, consequences and/or forms of restorative practice.

**Optional**

Additional school information about unacceptable behaviour may be included here.

## School Responses to Unacceptable Behaviour

Our Division acknowledges the importance of responsive discipline which involves a continuum of interventions that aim to build a sense of community in schools, facilitate healthy relationships, support behavioural changes, repair harm, and hold students accountable.

Edmonton Public Schools' Board Policy [HG.BP – Student Behaviour and Conduct](#) and Administrative Regulation [HG.AR – Student Behaviour and Conduct](#) outline the following:

Unacceptable behaviour may be grounds for disciplinary action which provides the student with an opportunity for critical learning and reflection in the areas of personal accountability and responsibility, the development of empathy, as well as communication, conflict resolution, and social skills development.

The specific circumstances of the situation and of the student are taken into account when determining appropriate responses to unacceptable behaviour.

When a student engages in unacceptable behaviour, consequences and responses may include, but are not limited to:

- temporary assignment of a student to an alternate supervised area within the school
- temporary assignment of a student to an alternate learning location
- short term removal of privileges
- interventions such as positive behaviour supports, contracts, counselling, restorative practices
- replacement or reimbursement for loss of, or damage to property
- in-school or out-of-school suspension
- referral to Attendance Board
- recommendation for expulsion

At <school name>, we are committed to ensuring that our school is a safe and productive learning environment. Where necessary, interventions or disciplinary action may be used to address unacceptable behaviour by students.

Describe how your school will respond to unacceptable student behaviour in this section. Refer to the Implementation Guide for important guidelines and examples for this section.

Edmonton Public Schools is helping to shape the future in every one of our classrooms. We're focused on ensuring each student learns to their full potential and develops the ability, passion and imagination to pursue their dreams and contribute to their community.



# Cyber Aware and Secure Campaign

---

“Our commitment to high-quality public education serves the community and empowers each student to live a life of dignity, fulfilment, empathy and possibility.” Our students and parents depend on and trust us to provide the high quality learning opportunities in a safe and secure environment. The security of their personal information (and our reputation) depends on our ability to effectively secure our information systems and the information of our students and families. To support and achieve that goal, Cyber Security Services (CSS) focuses on three pillars of cyber security:

- Hardening the Division’s cyber security posture
- Increasing information stakeholder awareness
- Shifting security posture from reactive to proactive

## Vision of Cyber Security Services (CSS)

*CSS mitigates cyber risks to enable students, teachers and staff to engage, work, innovate and explore safely with technology.*

A growing number of damaging cyber incidents in educational organizations are due to people falling for scams and malicious activity. This is not only due to cyber attackers actively targeting our staff, but with the growing adoption and complexity of technology to include working from home and the use of Cloud services, the risks related to mistakes made by staff or students have increased. Human risk has become the fastest growing risk to our Division, which technical controls alone cannot address. Every staff member who uses the Division’s networks, internet or technology forms part of the solution to the risks of cyber crime when they are aware of the human risks and know how to minimize them. This understanding can be increased by awareness training, practice and strategic evaluation.

Ransomware attacks continue to increase as a risk to educational organizations, and a successful attack can cripple unprepared organizations by halting operations. Successful ransomware attacks routinely cost over \$1.5 million to resolve. 82 per cent of beaches involved a person falling victim to cyber crime, including phishing and social engineering. Microsoft’s digital defense report indicates a 50 per cent reduction in employee susceptibility to phishing after training. As part of a layered defense against the increased risks of cyber crime, staff who understand the human risks and the strategies to address them are part of the shield of protection around Division systems and information.

## Cyber Aware and Secure campaign

### Training

All staff who work with the Division's systems as part of their job receive monthly essential training over the course of the school year, spread out into a number of three to five minute engagements. Each of these engagements includes a short video presentation about one specific cyber security topic followed by a question that tests for understanding and engagement. The training is emailed monthly to each staff member who is to receive the training, and a central dashboard tracks the completion rates and improvement in phishing awareness. Division-developed videos, made by students and teachers, are included in the training. Schools and central departments who achieve a certain level of response are acknowledged. Supporting materials based on the topic are shared and promoted, including posters, awards and small prizes.

### Phishing Training

Over the course of the school year, four phishing simulations are conducted with all Division staff. The purpose of the simulations is to allow staff a chance to practice what they have learned. The results will be kept secure and will only be disclosed to supervisors if additional training is needed. The results of the phishing simulations, combined with the metrics from the training, are used to refine and improve the training.

### Stories

Staff-provided stories, focused on the effect of cyber crime on their own personal lives, will be a focus of monthly articles in Connect. The purpose of stories increases engagement and understanding. Engaging newsletters with a focus on cyber security topics are produced monthly for staff. Additional materials and drop-in events focus on personal cyber risk and how to reduce the risk to staff in their personal lives.

### [Connect Cyber Security Services page](#)

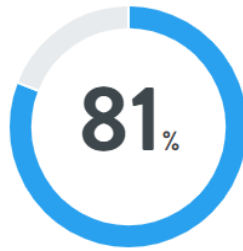
Content relevant to staff is featured on an interactive Cyber Security Services page found under "employee essentials".

### Metrics of the Cyber Aware and Secure Campaign (April 18, 2023)

Completion of training and correct responses - all Division staff



Module Completion



Correct Responses

### Division Staff attitudes towards cyber security awareness

1. I understand how security threats can impact the organization.

POSITIVE



- 64%
- 29%
- 2%
- 0%
- 5%

2. I understand how security threats can impact my family.

VERY POSITIVE



- 66%
- 28%
- 2%
- 0%
- 3%

3. I know what steps I can take to help prevent security breaches.

POSITIVE



- 36%
- 52%
- 9%
- 1%
- 2%

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

### Phishing simulation #5 for all staff

