First Nations Education Steering Committee & First Nations Schools Association
Suite #113-100 Park Royal South, West Vancouver, BC
Toll-free in BC: 1-877-422-3672 T: 604-925-6087 F: 604-925-6097

Online Learning Resources: Review and Privacy Considerations

May 7, 2020

Contents

Introduction

This document is intended to support First Nations and First Nations school representatives as they consider how to promote continuous learning opportunities for students in ways that are both effective and responsible.

Student privacy is an important consideration throughout the process. First Nations communities, working with their schools, are encouraged to develop their own privacy policies and protocols outlining how personal and sensitive information will be collected, used, shared, and kept secure as part of school operations. First Nations schools are also encouraged to assess the privacy risks of online learning platforms on a case-by-case basis, consistent with their needs and priorities.

FNESC and FNSA recognize the authority of individual First Nations to decide how best to apply and adapt information within this document to their particular circumstance. While this document is intended to assist First Nations in making determinations related to continuous learning in consideration of relevant privacy implications, the information is not legal advice. First Nations are strongly encouraged to seek independent legal advice about their particular situation should concerns arise, as FNESC and FNSA are not able to provide specific recommendations or support in regards to the privacy obligations of individual First Nations and/or First Nations schools.

Acknowledging that continuous learning will vary significantly from community to community and school to school, FNESC and FNSA are also unable to provide specific recommendations or support to individual First Nations schools regarding the implementation of the educational platforms discussed below. A number of these platforms provide instructions, training, or guidance documents as part of their service package, which may be of value to First Nations schools as they consider options for continuous learning.

We recognize that details about the specific features of the online tools and their privacy policies are likely to evolve over time and we greatly appreciate your suggestions for updates and improvements to this publication.

Continuous Learning in First Nations Schools: Suggestions for Working Remotely

Adapting to the COVID-19 context, First Nations schools in British Columbia are working hard to support students by delivering continued learning opportunities during the suspension of classes. This may mean that teachers and other school staff are working remotely, often from their own homes. As part of this adjustment, it will be important to consider and care for personal and sensitive information, including student information, when working away from the traditional school setting.

While this document does not provide a comprehensive privacy assessment of the various tools available, it does provide general information, tips, and things to consider for a number of the most frequently used platforms.

Recognizing that continued learning will look different from school to school, the First Nations Education Steering Committee (FNESC) and First Nations School Association (FNSA) have compiled the following suggestions and best practices to be used when working remotely.

Working with Technology

While working remotely, it will be important to consider how technology can be used in a way that keeps personal and sensitive information, including student information (e.g. assessments and other educational records), safe and secure. Tips to consider when using technology include:

- Password protect and encrypt all devices (desktop computers, laptops, phones, tablets, USBs, hard drives etc.) used for work or student purposes
- If possible, keep your "work devices" separate from your "personal devices"
- If home-based devices in a household are shared, ensure that access to student materials is restricted to authorized users
- Avoid naming files using a particular student's name. De-identify student information when possible
- Do not leave your device unattended in your workspace, and do not display personal or sensitive information on a screen that someone else might see
- Consider 'auto-lock' features that require you to re-enter your password after a period of inactivity
- Do not leave devices or paper files in your vehicle
- Ensure materials are securely destroy or returned to school when no longer needed
- Report lost or stolen devices in accordance with your school or community privacy policy. If no policy is in place, report to your school principal/administrator as soon as possible

Another important aspect of working with technology includes use of the internet. It is always important to consider the safety and security of personal information while using online platforms.

- Send communications from your school/professional email address instead of your personal email address
- Ensure emails are sent to the correct recipients. Consider your audience and do not send personal or sensitive information to recipients who do not have a reasonable need for it
- Do not post or discuss personal or sensitive student or staff information in a public forum or any other place where it could be inappropriately accessed (e.g. social media settings). Communicate personal and sensitive information in a direct manner and only to those individuals who are entitled to it
- If possible, password protect or encrypt documents containing large amounts of personal or sensitive information prior to emailing them
- Avoid using third-party platforms for storing or transmitting personal or sensitive information if you are not confident in their privacy or security features

Physical Security Measures

Continued learning does not necessarily mean online learning. In some cases, First Nations may deem it appropriate to carry on with 'paper-based' learning activities. Just like in a school, it is important to consider physical security measures when working with personal or sensitive information in hard copy. Tips and best practices include:

- Only remove personal information, including student records or files, from your school if it is necessary in order to deliver educational services

- Minimize the amount of hard copy files you keep at home
- Store paper files securely. Use available measures to keep documents safe, including locked drawers or cabinets
- Do not leave documents in your vehicle or unattended in places where they could be inappropriately accessed
- If you no longer need documents containing personal or sensitive information, do not simply throw them away Use a shredder whenever possible. This should always be done in accordance with your school's policies and protocols concerning data or document retention

General Considerations

While adjusting to the unique experience of working remotely, these best practices will help you in continuing to promote a culture of privacy and information security:

- Avoid discussing or sharing personal information with anyone who would not require it under ordinary circumstances
- Avoid working with personal information in public settings. Take precautions to ensure that others cannot view or access personal information you work with
- Do not discuss confidential matters where they can be overheard by unauthorized persons
- Report any known or suspected privacy breaches, including lost or stolen files, in accordance with your school or community privacy policy. If no policy is in place, report to your school principal/administrator as soon as possible

Learning Management Systems

Privacy Considerations for Learning Management Systems

General privacy considerations for the use of Learning Management Systems include:

- School-wide guidelines or an "acceptable use policy" for school staff members should be developed for the use of Learning Management Systems. Clear, consistent guidelines should be established, including features that should and should not be used (e.g. distributing and collecting class assignments, video-based instruction, communicating with parents, etc.). It may be advisable to craft an acceptable use policy for students as well
- School-level administrators of Learning Management Systems should establish appropriate role-based access privileges for both staff and students. Information stored on a Learning Management System should be password protected or encrypted and user access should be restricted on a 'need-to-know' basis
- Personal information should only be collected, used, or shared through a Learning Management System when it is reasonably necessary to do so in order to deliver an educational service;
- Schools should consider whether to seek consent from staff and students when utilizing a Learning Management System. When consent is sought, there should be clear plans in place for how to address situations in which consent is refused;

- Provide clear written or electronic notices to students, parents, and staff about what learning platforms will be used, and be transparent about how personal information will be collected used and disclosed using these tools
- Notices should identify features of the platform that will be utilized (e.g. videoconferencing, student email addresses, online file storage, associated apps) the kinds of personal information that will be collected or shared (e.g. recordings of students, student grades, student assessments, student communications), as well as the reason for collection or sharing
- Avoid learning platforms that involve the collection, use or disclosure of student information by third party providers for the provider's own purposes. Ensure that notices advise parents and students which third party providers will be involved in providing online learning tools, what information is provided to third party providers and how it will be used while users interact with it, as identified in the platform's privacy policy
    - For example, G Suite for Education and Microsoft Teams collect personal information from students interacting with their platforms. This can include information required to sign up for the platform (e.g. name), information related to how students interact with the platform, information about a student's location, and information that a student chooses to share. Some features of Learning Management Systems also allow students to share information with others or publicly. These features should be carefully considered by schools before they are enabled
- Notices should also identify whether or not a student's personal information will be stored outside of Canada. Consider communicating highly sensitive information about students through secure conventional means. Special needs assessments, medical or educational history, student grades, etc. should be communicated directly to the students and parents/guardians they pertain to. Since Learning Management Systems offered through third party providers often involve storage of the contents of communications, it may be advisable to communicate sensitive information via email or telephone
- The storage of student personal information on the Learning Management System should be minimized. It is not recommended that video conferences be recorded and saved where students are involved, unless there is clear reason or benefit for doing so. If sessions are recorded, ensure that students, staff and parents are advised.
- Any photos, videos, or other recordings of students should not be stored on 'Cloud' platforms. Recordings should only be saved to local storage devices
- Determine whether or not information recorded to a Learning Management System can be deleted when it is no longer needed. Consider in advance how to manage the transition plan for removing information stored on Learning Management Systems when in-class activities resume
- All student accounts linked to the Learning Management System should be password protected, encouraging students to use secure multi-factor passwords
- Where parents are not comfortable with a particular Learning Management System, alternative methods for the delivery of educational services should be available

It is advisable to research products, including Learning Management Systems, as much as possible prior to using them. Privacy and security sections of company websites provide valuable information on how information is collected, used, shared, and stored.

Ensure that you have carefully reviewed the terms of use or contracts in place with online providers, and that you clearly understand the school's obligations and risks.   Be aware that many providers use standard form contracts that seek to shift risk onto their customers in the event of a data breach by limiting or excluding liability or seeking indemnification. In the event of a data breach, these provisions will have an impact on a school's overall risk and liability. While providers are often not willing to change these standard terms, it is still important for schools to understand potential risks. If there are concerns, they should be raised with your school's legal advisors and/or insurers to understand what coverage or risk mitigation strategies may be available.

Carefully review the privacy policies, terms of use and contracts with third party providers. Since these policies could change over time, it may be advisable to review them on a regular basis. Be wary of providers that seek to use user personal information for secondary purposes, collect more student information than necessary, and do not provide the school with rights to terminate and/or require that student data be deleted. As an example, the "core services" offered by G Suite for Education (Gmail, Calendar, Classroom, Jamboard, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Meet and Vault) do not collect, sell or share a student's personal information for advertising purposes. Google also does not own customer data as part of G Suite's core services. Additional services offered by Google, including Maps, Blogger, and YouTube, will share information with third parties in some circumstances, such as when a student posts content. Because it can be difficult for students to understand when their information is being shared or becoming public, it may be advisable to restrict the use of these additional services. It is also important to provide guidance to students about the safe and appropriate use of online services.

Two main Learning Management Systems are being used by K-12 schools in BC: G Suite for Education and Microsoft Teams. Both platforms are relatively easy for teachers and students to use and both allow videoconferencing so that teachers can deliver individual, small group, or whole-class instruction. Teachers can deliver instruction, create assignments, give students real-time feedback, and assess completed assignments all within the platform. Teachers can also communicate and share updates with parents through the systems. They also allow for school staff collaboration and the integration of other online learning tools.

G Suite for Education

G Suite for Education is a Learning Management System used by many First Nations schools in BC. Features that schools may find useful include:

- videoconferencing
- creating and completing assignments within Google Classrooms
- the ability for teachers to provide students with real-time feedback on their assignments
- creating rubrics
- maintaining gradebooks
- posting resources
- collaborating with school staff

Other apps can be integrated into G Suite for Education and shared through the platform. The steps for signing up for G Suite for Education include verifying that you are a school and that you own a web domain for your school.

Videoconferencing		Yes
Student/Staff Email		Yes
Assessment	Formative	Yes

	Summative	Yes
Staff Collaboration		Yes
Parent Communication		Yes
Ease of Implementation		Moderate

Microsoft Office 365 for Education (Microsoft Teams)

Microsoft Office 365 for Education (Microsoft Teams) is a Learning Management System that is very similar to Google Classrooms. Basic access to Microsoft Teams is free (and will be sufficient for most schools); however, to access the more advanced options there are per user fees. Options included with a basic subscription that schools may find useful are the same as those described for Google Classrooms.

To implement Microsoft Teams, schools need to register for Microsoft 365 for Education. If your school owns a domain you can register through the administrative portal or use the domain provided by Microsoft (for example all staff would be assigned and email/login staffname@schoolname.onmicrosoft.com)

Videoconferencing		Yes
Student/Staff Email		Yes
Assessment	Formative	Yes
	Summative	Yes
Staff Collaboration		Yes
Parent Communication		Yes
Ease of Implementation		Moderate

ePortfolio Platforms

Privacy Considerations for ePortfolio Platforms

The privacy considerations for ePortfolio platforms are similar to those of Learning Management Systems. When adopting an ePortfolio platform, schools should consider the use of guidelines and consent forms. Personal information collected through the platform should be minimized, and all user accounts should be password protected. Additional considerations for each platform are provided below.

There are many ePortfolio platforms available to schools and these platforms allow teachers to upload assignments that may include detailed instructions, resources to complete the assignment, and samples of completed work. Students can then upload samples of their work to be assessed. Teachers then provide the student with comments on the work they completed. Teachers can also share the student ePortfolios with families. These platforms often allow messaging between the teacher and the student and the teacher and the family. The disadvantage of an ePortfolio relative to a Learning Management System like Google Classroom or Microsoft Teams is that they do not allow videoconferencing with students and they do not allow teachers to give feedback to students until students submit their assignment.

Class Dojo

ClassDojo is an online platform that is primarily focused on improving communication with students and parents about student learning. Features of this platform include an online portfolio where students and teachers can post samples of student work and teachers can post resources on the Class Story page. The platform also includes tools for classroom management when schools are back in session. This platform does not allow videoconferencing or staff collaboration. ClassDojo is free for teachers and it has an easy sign-up process. There are helpful videos embedded within the teacher portal to assist teachers in setting up ClassDojo.

Videoconferencing		No
Student/Staff Email		No
Assessment	Formative	No
	Summative	Yes
Staff Collaboration		No
Parent Communication		Yes
Ease of Implementation		Easy

Privacy Considerations: ClassDojo

- ClassDojo requires parental consent for the use of its services, either directly from parents or as part of a commitment from school staff to obtain parental consent
- ClassDojo uses some encryption technology to protect personally identifiable information
- ClassDojo is clear that information provided to the platform is owned by students, parents, and schools
- ClassDojo stores information outside of Canada. However, ClassDojo claims to "provide privacy protection that is consistent with Canada's private sector privacy laws."

Seesaw

Seesaw is an online platform that is primarily focused on improving communication with students and parents about student learning. Teachers can post assignments (this includes uploading relevant files) on the platform and students can submit their work through the student portal. It has limited assessment options but teachers can post comments on student work and assign a grade. This platform does not allow videoconferencing or collaboration amongst school staff. Seesaw is free for teachers and it has an easy sign-up process.

Videoconferencing		No
Student/Staff Email		No
Assessment	Formative	No
	Summative	Yes
Staff Collaboration		No
Parent Communication		Yes
Ease of Implementation		Easy

Privacy Considerations: Seesaw

- Seesaw requires parental consent for the use of its services
- Seesaw is clear that they do not own information provided to the platform by users
- Seesaw uses some encryption technology to protect personally identifiable information
- Seesaw stores information outside of Canada. Teachers have significant control over who can view student content uploaded to the platform

Edmodo

Edmodo is an online platform that is primarily focused on improving communication with students and parents about student learning. Teachers can post assignments (this includes uploading relevant files) on the platform and students can also submit their work through the student portal. It has limited assessment options but teachers can post comments on student work and assign a grade. This platform does not allow videoconferencing or collaboration amongst school staff. Edmodo is free for teachers and it has an easy sign-up process.

Videoconferencing		No
Student/Staff Email		No
Assessment	Formative	No
	Summative	Yes
Staff Collaboration		No
Parent Communication		Yes
Ease of Implementation		Easy

Privacy Considerations: Edmodo

- Edmodo requires parental consent for the use of its services. Schools/teachers must agree to obtain parental consent as part of Edmodo's Terms of Service
- While Edmodo makes use of encryption for purchasing processes, it is not clear if encryption is utilized to protect student information. This may be a concern given the sensitivity of student information collected by Edmodo (e.g. assessment data)
- Edmodo is not clear about who "owns" data collected through the platform
- Edmodo stores information outside of Canada

Videoconferencing

Privacy Considerations for Videoconferencing Platforms

As schools transition to online learning, videoconferencing platforms have become increasingly popular. It is recommended that schools consider the following guidelines when delivering education services through any videoconferencing platform:

- Only download and install videoconferencing platforms from official company websites. Ensure you are using the most current version of the software
- Look for and enable encryption features, where possible. The WebEx platform uses 'end-to-end' encryption, which is generally considered a high standard of data security
- When hosting meetings via videoconference, use a licensed version of the platform if possible
- Password protect videoconference sessions and do not publicly post meeting links. Activate controls that allow the "host" to control who has access to meetings.
- Know where your mute button is; this will come in handy if you experience an uninvited guest
- It is not recommended that video conferences be recorded and saved where students are involved, unless there is clear need and explicit consent to do so

- If possible, disable the "join before host" feature on videoconferencing platforms
- Students should not be hosts or co-hosts of videoconference sessions
- It is not advisable to transfer files through videoconferencing platforms
- The sharing of personal or sensitive information or videoconference should be minimized. Remember that anything appearing on screen, including documents, could be photographed, though this should be discouraged
- When participating in videoconference sessions, it is recommended that the use of the private chat feature be minimized as those chats may be accessible to the host after the meeting has finished. Consider features that allow participants to chat only with the host
- There are several different videoconferencing apps available for little to no cost right now. Both G Suite for Education and Microsoft Teams have their own videoconferencing software built into their platform. Microsoft Teams will also let you integrate other videoconferencing apps into the platform. Most videoconferencing apps allow you to record your meeting. Schools can use videoconferencing platforms to allow teachers to deliver instruction to individual students, small groups or a whole class. Videoconferencing platforms allow school staff to meet and collaborate as well

Platform	Cost	Meeting Size	Meeting Recording Available	Can Screen Share	Has Chat Function	Can Call in From Phone
Zoom	Free	1-100	Yes	Yes	Yes	Yes
WebEx	Free	1-25	Yes	Yes	Yes	Yes
Google Hangouts (G Suite for Education)	Free (currently and will be in the future)	1-250	Yes	Yes	Yes	Yes
Microsoft Teams	Basic access for free ($2.50-$8.00/month fee for additional features and functionality)	1-250	Yes	Yes	Yes	Yes

Privacy Considerations: Zoom

As reported in the news, a number of privacy concerns have been raised regarding the Zoom videoconferencing platform. While Zoom has pledged to address its security and privacy issues, the following tips should be considered in addition to those described above:

- Official Zoom licenses are available to BC First Nations schools and should be utilized. For questions regarding the Zoom license, please contact jenniferw@fnesc.ca
- Consider making Zoom meetings 'invite only'
- Disable the file transfer feature
- Lock your Zoom sessions after they begin to prevent unwanted guests. However this may present problems for latecomers

- Use the waiting room feature to control who can join your sessions
- When sessions are finished, use the 'end meeting for all' feature to ensure students can't continue conferencing unattended
- Disable 'allow removed participants to rejoin,' the feature that allows participants to rejoin the meeting if they are removed by the host

While Zoom's privacy issues have been highly publicized, it should be noted that many of the concerns raised apply to other videoconferencing platforms as well and no platform can be fully safe and secure at all times. Schools should be considerate in the use of any and all videoconferencing platforms, keeping in mind that videos and images of students are very sensitive.

For additional information on videoconferencing platforms, see the following resources created by Safer Schools Together (SST):

- Increased Safety in a Remote Learning World – Guidelines
- Increased Safety in a Remote Learning World – Using Zoom, MS Teams and Google Classroom
- Zoom – Creating Safe Remote Teaching & Learning Spaces (video)
- Zoom – Keeping it Private and Practical Tips for Remote Teaching (video)
- Zoom Settings for Education – Quick Reference Sheet

Online Quiz Generators

Privacy Considerations for Online Quiz Generators

Given their more limited functionality, online quiz generators typically collect less personal information from users relative to larger platforms operated by Google or Microsoft. Unfortunately, quiz generators are less transparent about the authority students, parents, and schools retain over their data, and generally do not make use of strong security features (e.g. encryption).

Several different websites create online quizzes that can be shared with students. Many of these sites include pre-generated quizzes that teachers can use or teachers can create their own based on the learning standards being taught. Many quiz generating sites also integrate into Learning Management Systems.

- Kahoot!
- Classmarker
- Quizlet

Social Media Platforms

Privacy Considerations for Social Media Platforms

Exercise caution if using social media platforms for the delivery of educational services. The use of these tools requires careful consideration given the amount of personal information these platforms typically collect and make available to others. Of particular concern is the possibility for social media content to become accessible to non-school personnel and ultimately the public.

It is not be advisable to collect or share personal information, particularly sensitive information about students and staff, over social media platforms. Instead, social media platforms may be better suited for broad communications.

Social media can be a powerful tool to both communicate and share resources. However, there are considerations to make before starting a school Facebook page or Instagram account. Remember that while many families access Facebook this does not mean all families will have access to the information you are sharing. It may be beneficial to share the information in several different ways to ensure everyone gets the message.

Privacy Considerations: Facebook

Facebook is a social media platform that both students and school staff may already be using for non-professional purposes. Given Facebook's popularity, it may be appealing as a tool for communicating with students or parents. It should also be noted that Facebook is not currently available to individuals under the age of 13.

Schools should be extremely considerate in their use of Facebook for educational purposes. Specific concerns related to the platform include:

- Information posted to or transmitted through Facebook may stay on or be saved to the platform. This may mean that posts or communications could become permanent
- Given that Facebook is widely used for personal purposes, the use of Facebook for education could mean that personal and professional information end up in the same place, increasing the risk that a privacy breach could include significant amounts of highly sensitive information
- If information on Facebook is not properly cared for, it could become available to a large number of people

The use of Facebook should therefore be approached with exceeding caution. School staff making use of Facebook should consider the following suggestions:

- It may be advisable for school staff to create a Facebook account specific to the purposes of their professional duties
- Private groups should be used whenever possible. Student information and sensitive school information should never be posted publicly
- The kind of information relayed over Facebook should be carefully considered. It may be advisable to use alternative means to communicate personal or sensitive information to parents and staff (e.g. telephone or email)