

Meeting BC Teacher Needs: A Tool to Support Web 2.0 & LMS Integration with  
Respect to Privacy

by

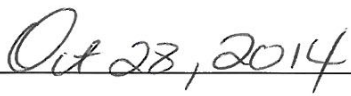
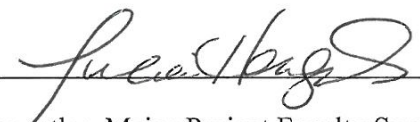
*Breanne Quist*  
*B.Ed., Vancouver Island University, 2011*

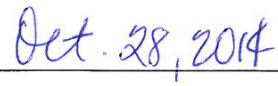
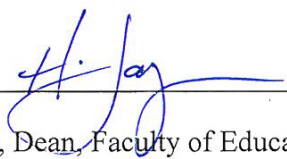
Submitted in partial fulfillment of the  
requirement for the degree of

MASTER OF  
EDUCATION  
(Leadership)

October 28, 2014

We accept the Process Paper as conforming to the required standard.

  
\_\_\_\_\_  
Julia Hengstler, Major Project Faculty Supervisor      Date:  
Faculty of Education,  
Vancouver Island University

  
\_\_\_\_\_  
Harry Janzen, Dean, Faculty of Education,      Date:  
Vancouver Island University

### Acknowledgements

*I would like to acknowledge and express my eternal gratitude to my husband, Nick, and my daughters Aliyah and Sadie, for all of the support and encouragement that they gave me while completing my Master's degree. For the past two years I have taken many different courses all while teaching in the distance education setting and without them helping with meals, keeping the house clean and knowing when to let mommy have her 'office time', I would not have been able to accomplish my goals. Their unending love and support means the world to me and I appreciate them and everything they have done for me more than words can ever express.*

*To my parents, in-laws and sisters who have helped in this journey through encouraging me, supporting me, and probably the most important of all - babysitting; thank you from the bottom of my heart. Taking the girls for a morning so I could focus was a huge part of my success. A special thank you to my mother-in-law and Debbie who helped proofread many documents along the way, the extra sets of eyes seeing things that I missed.*

*Thank you to my colleagues at Anchor Academy for their prayers of encouragement through this process. They allowed me to share what I have learned with them and I am very proud to be able to present them with the information they need to be able to move their teaching online without fear of privacy issues. Also thank you to Brad who proofread and edited for me when my eyes had read so many times that I needed someone fresh.*

*Finally, I would like to thank Julia Hengstler, for her time, energy and expertise while being my advisor. Her knowledge of the topic pushed me to make sure that I knew all the pieces, and knew them well, which is a big part of my success in this final leg of my journey. She has been a great support for me, a mentor in many ways and someone who was able to push me to do my best. My topic for this project was all based on a seed she planted one year ago that has now grown into something much more.*

## TABLE OF CONTENTS

Acknowledgements .....	ii
List of Figures .....	v
Abstract .....	vi
Chapter 1: Introduction .....	1
LMSs .....	2
Web 2.0 .....	3
Research Focus and Intent.....	3
Project Site .....	7
Project Site as EPSS .....	7
Further Considerations.....	10
Chapter 2: Literature Review .....	11
Terminology .....	12
Priming for the Online World .....	13
Personal Information and Risks .....	14
Server Locations .....	15
Learning Management Systems (LMSs) .....	18
Web 2.0 Tools .....	19
Legislation: PIPA, FIPPA & the US Patriot Act .....	21
What Parents and Guardians Need to Know .....	24
Professional Standards .....	30
Conclusion .....	33
Chapter 3: Choosing Initial Tools and LMSs .....	34
Privacy Documentation and Application .....	37

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

The Privacy Compass .....	39
Levels of Risk .....	43
Chapter 4: Field & Beta Testing of the EPSS Site .....	46
Choosing a Database .....	47
In Development .....	49
Future Considerations .....	50
Chapter 5: Next Steps .....	52
Recommendations .....	55
Conclusion .....	57
References .....	60
Appendix A: Web 1.0, 2.0, 3.0: What's the Difference?.....	65
Appendix B: External Canvas Apps.....	66
Appendix C: Hengstler Models.....	67
Appendix D: Sharing Circles.....	68
Appendix E: Canvas Documents.....	69
Appendix F: Kidblog Documents.....	78
Appendix G: Comparison Chart for The Privacy Compass Website.....	90
Appendix H: Website Graphic Set.....	91
Appendix I: Screen Shots of Navigation for The Privacy Compass Website.....	92
Appendix J: eSafety Incident Response Flow Chart.....	93

**List of Figures**

Figure 1.	Sharing circles: A classification framework for online tools.....	8
Figure 2.	Workflow Design for The Privacy Compass.....	39
Figure 3.	Compass icon. ....	41
Figure 4.	The Privacy Compass homepage screen shot.....	41
Figure 5.	Unique visitors to my site.....	46
Figure 6.	Levels of risk exposure. ....	54
Figure 7.	The FIPPA Compliance Continuum.....	55

### **Abstract**

This research project explored privacy concerns in fully online learning environments and developed an electronic performance support system (EPSS) called, “The Privacy Compass for Web 2.0 Tools: Helping Teachers Navigate Challenging Terrain” ([www.privacycompass.ca](http://www.privacycompass.ca)). The project was directed by two major questions: 1) What do teachers need to be aware of and teach their students to keep them safe in the online world? 2) What do parents need to be made aware of and understand when giving informed consent for their child (a minor) to participate in fully online courses? The learning management system, *Canvas*, was explored, as well as other Web 2.0 tools that are able to be easily integrated into the online classroom and utilized by students. With this project, documents were created and an EPSS, The Privacy Compass ([www.privacycompass.ca](http://www.privacycompass.ca)), was established to allow all teachers access to these resources for use in their classrooms – with their students and the parents/guardians.

## Chapter 1

### Introduction

While the expansion of learning management systems (LMSs) and Web 2.0 tools is ever growing, many K-12 teachers are unaware of where these tools and LMSs store their information and the ways in which this information is accessed or transferred. The types of data entered or shared on these tools, as well as the methods of storage and access can present student privacy risks and vulnerabilities. In British Columbia (BC), Canada, teachers using these tools can be legally responsible for reasonably managing these risks and vulnerabilities. Under British Columbian law, the responsibilities of public school teachers are governed by the Freedom of Information and Protection of Privacy Act (FIPPA, RSBC 1996, C-165) while teachers in independent schools are governed by the Personal Information Protection Act (PIPA, SBC 2003, C-63).

For teachers in British Columbia independent schools, these factors raise significant questions. This work will concern itself with 4 key questions:

- What student privacy issues, if any, must teachers in BC independent schools manage when using online learning environments and Web 2.0 tools?
- What type of electronic performance support system (EPSS) might be built to help teachers in a British Columbian independent school use learning management systems and Web 2.0 tools in accordance with the Protection of Information and Privacy Act (PIPA, SBC 2003, C-63)?
- What do teachers need to be aware of when looking at existing legislation and making decisions about using Web 2.0 tools and Learning Management Systems with their students?

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

- What implications, if any, do teacher awareness and existing legislation have for managing the privacy of BC students in independent K-12 schools in regard to the Protection of Information Privacy Act (PIPA, SBC 2003, C-63)?

The focus of this work will be to look at what privacy and legislative concerns teachers need to be aware of when moving from a completely paper based brick-and-mortar classroom to a completely online distance learning classroom. Teachers are responsible for teaching their students (and themselves) about the online world and priming their students for a safe journey through it – as well as giving parents and guardians all of the relevant information when obtaining consent for online learning. Parents and guardians need to be aware of the fact that consent is more than just signing a name on a piece of paper; they should be sure that they know to what they are consenting and the implications.

### **LMSs**

Most online learning environments that teachers are using are LMSs with Web 2.0 tools via embedded websites and applications. An LMS is the infrastructure that delivers and manages instructional content, identifies and assesses individual and organizational learning or training goals, tracks the progress towards meeting those goals, and collects and presents data for supervising the learning process of organization as a whole (Szabo & Flesher, 2002). An LMS delivers content but also handles course registration, course administration, skills gap analysis, tracking, and reporting (Gilhooly, 2001).



### **Web 2.0**

A simple definition of Web 2.0 is the “Read/Write Web” (Web 2.0 Teaching Tools, 2009). Originally, the Internet was a place to locate information - mainly a "Read Only Web" (Web 2.0 Teaching Tools, 2009) As the Internet slowly changed, web sites were developed that let people write, collaborate, and share information, such as Wikipedia and Facebook. (Web 2.0 Teaching Tools, 2009). A chart outlining the differences between Web 1.0, 2.0 and 3.0 can be found in Appendix A.

There are a lot of fears around using social media tools with our students but many teachers are unaware that there are privacy concerns with many Web 2.0 tools. This statement is not to scare teachers and parents/guardians away from using these tools with their students, but rather to inform them that there are items that they should be aware of to help keep the students as safe as possible. Technology is a very useful tool to have and a great way that teachers can reach a vast majority of learners with different learning styles, but it has to be used judiciously. This is why I have selected my topic: Meeting BC Teacher Needs: A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy. A significant portion of this project was committed to the development of -“The Privacy Compass for Web 2.0 Tools: Helping Teachers Navigate Challenging Terrain”, a practical resource to support teachers’ integration of Web 2.0 & LMS with respect to privacy.

### **Research Focus and Intent**

I am currently working as a teacher in a independent K-12 distance learning school in British Columbia, Canada. When thinking about project possibilities, I noticed that many of my colleagues were unaware of the privacy concerns associated with using Web 2.0 and LMSs with

their students. Although none of my colleagues currently use a fully online learning environment, the hope of our school is to slowly start moving in that direction. This process will take time and it starts with small changes. An example of a small change can be demonstrated as teachers in our primary school switch from a library book and reading log system to an online resource such as Reading Eggs (<http://readingeggs.com/> - a paid service and app) where the students' reading progress is tracked online and can be accessed by both the teacher and the parent/guardian of the student. When teachers decide to use a Web 2.0 tool or a LMS they need to be aware of some key privacy and safety points so they are able to accurately relay them to the families that will be using the tools. These key points form the basis on which families decide to give or withhold consent for student participation. Three of the biggest points that need to be addressed in British Columbia before any informed consent can be reasonably given by a parent or guardian are:

- the data storage and location of the LMS or Web 2.0 server,
- the privacy policies that govern the server,
- the nature of student use as envisioned by the teacher.

The location of the server for Web 2.0 tools and LMSs is very important since most are housed where they were developed. Many of these tools have been developed outside of Canada and their servers are also outside Canada. Because they are external to Canada, they are not covered under the same legislation as technology based on Canadian servers. As stated already, Canada has two sets of regulations that govern personal privacy, the first is the Freedom of Information and Personal Privacy Act (FIPPA, RSBC 1996, C-165) and the second is the Protection of Information Privacy Act (PIPA, SBC 2003, C-63). The main difference between the two is that FIPPA (RSBC 1996, C-165) concerns public sectors -including public schools in

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

British Columbia- while PIPA (SBC 2003, C-63) concerns private sectors – and in the case of my master's work, independent schools. When using tools and learning management systems that are not based on Canadian servers, but instead specifically based in the United States, we become subject to the USA Patriot Act (2011). The USA Patriot Act (2011) allows the United States government to access any cloud based content on servers located in the United States, including personally identifying information without the users' knowledge or consent.

Beyond relevant legislation, when using LMSs or Web 2.0 tools, teachers must also concern themselves with an online tool's specific terms of service and privacy policy, as well as any school level policies as these affect how student/user information is stored, accessed and used. An important consideration for teachers, especially when using one tool for multiple years is to make sure to recheck the privacy policy and terms of service for the tool periodically (at least every 6 months) as many companies update these and some do not inform their users of the changes. If a teacher sees too great of a change in these policies, he or she will be required to make a decision about regaining parent or guardian consent or choosing a different tool with similar capabilities, as the previously obtained informed consent for the tool could be invalid.

School policies may be similar from school to school but are rarely identical. Unlike public schools where district-wide policies can provide continuity across a variety of schools, independent schools are not part of a particular school district. Independent schools, more so than public schools, are likely to have differences in their policies from one school to the next. Like the terms of service and privacy policies from a company or website, school policies should grow and change as the years go by--especially as technology is becoming a bigger part of life and learning. Policy changes will occur and should be communicated to the teachers. Once teachers are aware of a change, they will have to make sure that their practices are keeping

within the updated requirements. In the same way that a change in a company policy may be so great that consent previously given is invalid, changes in school policies may affect the nature of the informed consent obtained by teachers. In light of any policy changes, it will be the teachers' responsibility to review previously obtained consent to ensure it is still valid.

The nature of intended student use of tools is another important factor of which parents and guardians need to be made aware and of which teachers need to have a firm understanding. If teachers are not fully sure of why they want to use a certain tool, then the tool will not be used to the greatest potential for helping the students achieve their goals. Clear teacher expectations about the tools, activities to be conducted on them, data to be posted, and associated concerns as well as how they will be managed need to be stated by the teacher from the start. This information should be communicated to the parent/guardian to establish his/her firm understanding. It is only with a clear understanding that parents and guardians are able to give informed consent for their child to use the tool and partake in the activities associated with it. The goal of my project is to provide a support tool for teachers that will:

- support assessing the privacy risks associated with an LMS or Web 2.0 tool under the current BC legal framework of FIPPA (RBSC 1996, C-165) & PIPA (SBC 2003, C-63);
- allow for both teachers and parents/guardians to have a user friendly database to obtain information in a easy to understand format;
- be as current as possible with moderated content posted on a regular basis, with a content review mechanism for accuracy and credibility;
- be a place for others to comment, add to and create their own documentation for LMSs and tools which will be reviewed before being posted for others to use.

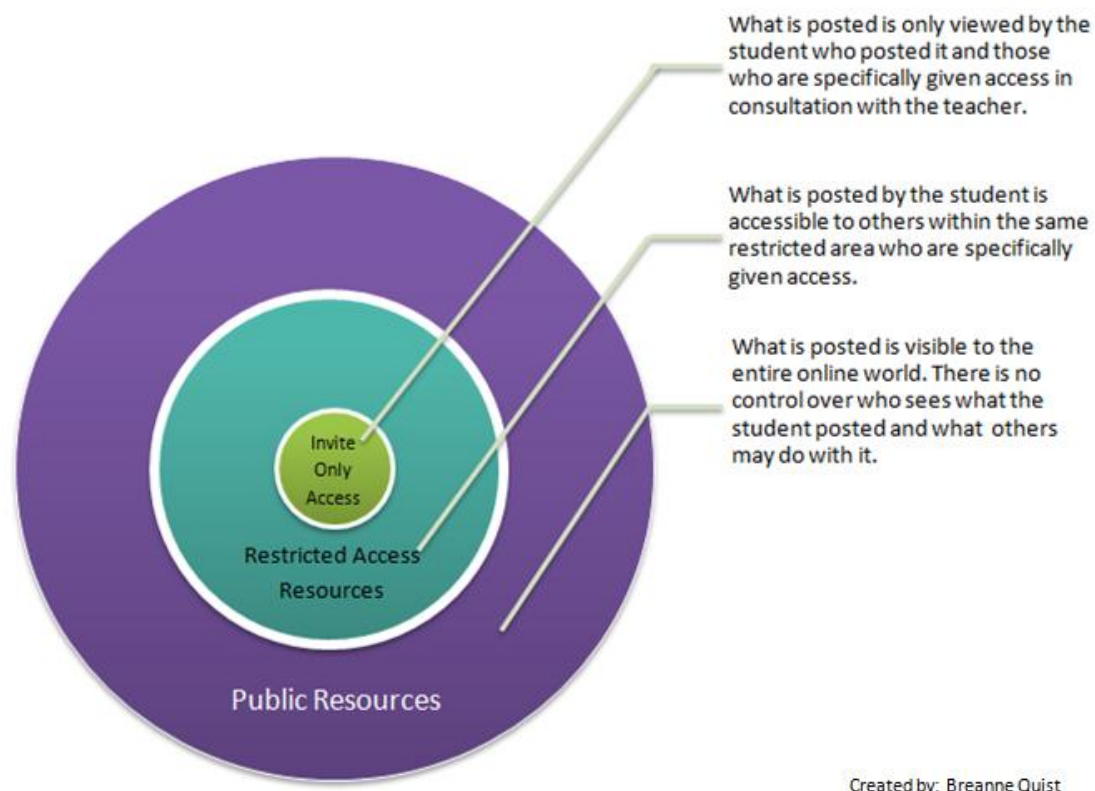
### **Project Site**

The project proposes to create a website which will include parent/guardian background information documents, teacher briefing documents and consent forms for each of the Web 2.0 tools that are used by the teachers in my school as well as the LMS Canvas by Instructure. Canvas will be the initial LMS tool supported by the project as it is the LMS our school is currently using and it allows for a vast amount of Web 2.0 tools and apps to be embedded in it. Some of the apps that can be embedded into Canvas are TeacherTube, Khan Academy, Twitter, and many others (a full list can be seen in Appendix B). The project will compile a list of all tools and websites that are used by my colleagues at my independent school and establish a website of information that can be used by them and shared with others for use in many independent (and public) schools in British Columbia and beyond. The reason I would like to include my colleagues' tool choices in this project is because they would give me a chance to target my initial efforts toward what is most relevant to myself, my colleagues and my school.

### **Project Site as EPSS**

This project site will function as an electronic performance support system for teachers. An Electronic Performance Support System is, according to Barry Raybould (1992), "a computer-based system that improves worker productivity by providing on-the-job access to integrated information, advice, and learning experiences". With the EPSS that I am striving to create, I will have editable information sheets and templates that could be used with teachers, as well as parents and guardians. The teacher documents explain relevant privacy information and outline potential and risks. This would encourage the teachers to be aware of the relevant privacy concerns under BC legislation, the usefulness of their tools of choice and how to articulate these

to the families with whom they would be working. The teacher's tool context and sample activities content of the EPSS will include a classification of whether the tool is a public tool or a restricted access tool. A public tool would allow users to post and access content shared with anyone in the world including people whom they have never met. A restricted access tool would allow the teacher and/or user to define who can post and access content. (See Figure 1: Sharing circles).



*Figure 1: Sharing circles: A classification framework for online tools. This graphic demonstrates the different levels of risk exposure when using Web 2.0 tools.*

Many teachers will pick a tool or website that other teachers will recommend to them without looking critically at it themselves. I believe that this EPSS would encourage opportunities for critical reflection on the nature and risks of specific tools. Teachers would be

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

able to access the documents, edit them to make them specifically work for their intentions and then send to the parents and guardians of their students. The EPSS will also contain editable consent forms as well as background information about the risks and benefits of using the Web 2.0 tool for the parents/guardians.

The parent/guardian and teacher background information documents will contain pertinent information to review before using – or giving consent to use – tools and websites. The documents will include three pieces for the parents and guardians to consider:

- the tool overview - an explanation of what the tool does, rationale for using it, and sample activities
- the tool's privacy policy or terms of service considerations in respect to the school's policies or BC legislations
- a form to obtain informed consent from a parent/guardian for each student to use the tool or website.

The tool content would include a general description of the tool and the grade ranges and subjects for which it may be considered appropriate. So that learning opportunities are not missed, the document would also include lesson ideas and adaptations for students whose parents/guardians choose not to give consent.

The privacy policy compliance piece will relate each concern back to BC legislation considerations. For the purposes of this project, my intention is that the initial privacy policy content will be tailored to the policies of my school. Since each independent school has its own policies, privacy policy compliance needs will vary from school to school. It is likely that privacy policy support content may need to be tweaked when being accessed by someone at a different school. The privacy policy compliance piece in the parent/guardian documentation will

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

give parents/guardians information about why a tool was chosen, what concerns there may be for consideration before giving consent, and suggestions for how to stay safe when using the resource. At this time, my school is in the process of updating its privacy policy and I will be supporting the school's efforts while completing my project.

Finally, the consent form will clearly outline expectations and guidelines for the tool or website that is being used. For example, the consent form will give a quick overview about suggestions for choosing user names (if applicable), a quick reminder about why the tool is being used, and a list of guidelines for responsible and safe tool use. This form will be about two pages long to allow for the explanation and guidelines to be on one sheet and the consent to be on a separate sheet. The form will be designed to allow parents and guardians to retain a copy of the expectations to refer to whenever necessary.

### **Further Considerations**

As stated previously, one of the purposes of the EPSS is to allow sharing with and adaptations by other teachers from any school or district. As much as it would be nice to have everything line up perfectly when using the forms with many different teachers, these tools will be used for a variety of reasons in many different grades, in many different ways, and therefore it will be necessary for each teacher to adapt the documentation to fit his or her specific situation. The EPSS will provide a great head start for the general teacher and for many, it should require only a small amount of editing prior to use. The forms and content in the initial EPSS will conform to my specific school's privacy policies which are governed by PIPA (SBC 2003, C-63) (as we are a BC independent school) and therefore, there may be additional changes that are



required when used with students and classrooms in a public school governed by FIPPA (RSBC 1996, C-165).

## Chapter 2

### **Literature Review**

Before designing a support tool for teachers to address privacy concerns and considerations in an independent school in British Columbia, it is important to understand the issues and research regarding privacy. For the purposes of this project, I am giving special consideration to independent school teachers moving from a completely paper based brick-and-mortar classroom to a completely online distance learning classroom. In this context, there are 7 major points to consider for this shift to occur:

- 1) Teachers must be responsible for teaching their students (and themselves) about the online world and priming them for a safe journey through it;
- 2) Because of provincial privacy laws, BC teachers need to know where the servers for any online tool are located and the risks which are associated with the location of the server;
- 3) Teachers must be aware of the specific learning management system's (LMS) or Web 2.0 tool's terms of service (ToS) and/or end user licence agreement (EULA);
- 4) The teachers must have determined specific intended uses of the LMS or Web 2.0 tool and data that will be entered into the LMS or tool (profile, content, etc.)
- 5) Teachers must be aware of which current privacy legislation in British Columbia affects their use of LMSs and Web 2.0 tools (i.e. FIPPA, RSBC 1996, C-165 or PIPA,

SBC 2003, C-63) as the legislation impacts public and independent schools in similar but slightly different ways;

6) Parents and guardians need to be prepared by teachers in order to provide informed consent for using online learning technologies such as an LMS or Web 2.0 tool;

7) Independent school teachers need support in moving through the various tasks associated with selecting and using a LMS or Web 2.0 tool in accordance with BC legislation.

### **Terminology**

Before moving into a discussion of what the research says on privacy in online learning environments, some key terms need to be defined and understood. For this review, Web 2.0 tools, Learning Management Systems (LMSs) and cloud computing options are discussed. Web 2.0 tools refer to technology tools which are developed to focus on user collaboration, sharing of content and social networking – creating a learning community opposed to sitting in front of a book and answering questions without any peer interaction. Some examples of Web 2.0 tools are blogs, Facebook, wikis and a broad range of web and mobile apps.

Learning Management Systems (or LMSs) are computer applications (usually web based) that allow the administration of a course in a fully online setting with reporting embedded within. These allow for students to access their learning from anywhere at any time provided they have a computer with internet access. LMSs often allow for Web 2.0 tools (such as wikis and links to external tools) to be embedded within them to offer a broad range of opportunities. Some of the most popular LMSs that are available today are Canvas by Instructure (which will be discussed

in more detail in the Learning Management System section of this chapter), Moodle, Desire to Learn and Blackboard Learn.

Cloud computing is described best by Klassen (2011):

a cloud-based application does not need to be downloaded to a user's computer or institutional servers, and the data used by the application and inputted by the user is housed on servers elsewhere. The application works remotely: it's not physically present, it could be anywhere in the world (hence the term 'in the cloud'). (p. 4)

Some examples of cloud computing tools are Dropbox, Evernote, and Apple's iCloud. Just like LMSs, as long as a student has an electronic device with internet access, they would be able to access the 'cloud'.

### **Priming Students (and Teachers) for the Online World**

Students need to be aware that privacy concerns exist in both face to face and online classrooms, and these concerns can be heightened in an online environment given the digital footprints we leave behind with each interaction. In the online environment, unlike most other environments, once something is shared or posted it can never be fully deleted; any and all interactions online leave a permanent record. Critical for students learning and communicating online is to know when personal information should remain personal and private: "An organization [or teacher] must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks" (PIPA, SBC 2003, c. 63, p. 9, s. 43). Even with guidance and vigilant supervision from teachers and parents/guardians, not all online interactions can be monitored to make sure that personal information is not being shared

inappropriately by students. Both students and parents/guardians must first be informed of the risks associated with creating work online and interacting in an online environment.

### **Personal Information and Risks**

The Office of the Information and Privacy Commissioner for British Columbia [OIPC BC] (2012a) defines personal information as follows:

information that can identify an individual (for example, a person's name, home address, home phone number or ID number). It also means information about an identifiable individual (for example, physical description, educational qualifications or blood type).

(p.4)

When students enroll in a brick-and-mortar or online school they are required to submit personal information to the school to complete the enrollment process. The information that is given to the school is expected to be put in a secure place so that it can be accessed in an appropriate way when needed. This security is not always guaranteed. Recently some Surrey high school students learned that human error sent their attendance records and final grades to all the grade twelve families rather than the intended communication about the B.C. teacher's strike in June, 2014 (CBC News, 2014). The British Columbia Privacy Commissioner was contacted right away and the school sent out an email immediately asking everyone to delete the previous message (CBC News, 2014). Unfortunately, the truth is a digital footprint can never be fully erased. Just as there is information stored in a file cabinet about student registrations, there is also information stored in online school records and a teacher's virtual classroom. All this information must be handled in a way that aligns with British Columbia's privacy legislation.

As teachers, it is our responsibility to inform our students and families how their information is being stored, where it is being stored and what possible actions may be taken with their information (boyd, 2014; Hengstler, 2014a; Hengstler, 2014b; OIPC BC, 2012a). In the case of students, parents/guardians need to have a firm understanding of both the potential benefits and possible security concerns before they can make an informed decision on whether they allow their child to use a tool and what information they allow to be shared with others. Our responsibility as educators is to do our due diligence to ensure that the privacy of our students is protected and that students, parents and guardians have the knowledge to keep it protected in the future. Instilling a respect for a person's identifiable data, the online environment and student interactions within Web 2.0 tools and learning management systems is all we can do. Beyond that, it is the family's responsibility to keep private information private (Unicef, n.d.).

### **Server Locations**

Server locations are another significant factor when looking at privacy in education. Most of the Web 2.0 tools and cloud-based applications that we use are developed and stored on servers. Where the information is stored makes a big difference to the level of privacy. If you look at many of the tools commonly used, you will find the information collected is stored on servers that are located outside of Canada – mostly in the United States of America. Where the information is stored determines the national privacy laws that govern it. A quick look at legislation shows not all countries value privacy the same way that Canada does.

There are some alternatives to server storage outside of Canada which are available. Certain companies allow schools to purchase a tool and load it on the schools' own servers. However, when doing so some capabilities can be lost, support is usually fee based and

the school now has to support the tool taking up valuable space on their own, likely limited, server. Having tools with servers located in the United States as well as other countries is not necessarily a bad thing; it just means that teachers have to be aware of where the information is going, what information can be responsibly shared and what could potentially be done with the information.

Knowing where your information is stored is an important step in implementing an online learning management system and it can help alleviate many problems down the road. Finding the server information is not always an easy thing to do. Many times a website will place its server location information in the policy part of their website but uncovering it takes a lot of effort. A tool that aids in the identification of server information is an app called ‘deep whois’ (this app can be downloaded onto any iOS device by visiting the link here:

<https://itunes.apple.com/ca/app/deep-whois/id328895000?mt=8>). This app allows you access to domain and server location information within a few seconds.

When using tools and learning management systems that are not based on Canadian servers, but instead on servers in another country, use of the software and the data it collects are subject to the laws of the country where the server physically resides. Specifically, in the case of information on servers based in the United States, that information is subject to the USA Patriot Act (2001) (Canadian Internet Policy and Public Interest Clinic [CIPPIC], 2004). The USA Patriot Act (2001) allows the United States government to access any cloud based content located servers in the United States, including personally identifying information without the users’ knowledge or consent (US Law, 2001). Prior to the USA Patriot Act, Canadian information located in the United States was protected by the Mutual Legal Assistance Treaty [“MLAT”] (RSC 1985, C-30). The MLAT (RSC 1985, C-30) between Canada and the United

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

States of America protects information that is stored in Canada from the US government, as it requires the US government to request the information from the Canadian government who then issues a search warrant (Canadian Law, 1985). The USA Patriot Act (2001) allows the United States government the rights to access any information stored on any US servers without needing to notify the person or organization that they are doing so (Banks, 2012).

The Canadian Internet Policy and Public Interest Clinic [CIPPIC] (2004) has identified the differences between the MLAT (RSC 1985, C-30) and the USA Patriot Act (2001). It concludes that “the USA Patriot Act, if enacted in Canada, would violate section 8 of the Charter [Canadian Charter of Rights and Freedoms] (CIPPIC, 2004, 18). Section 8 of the Canadian Charter of Rights and Freedoms states that “everyone has the right to be secure against unreasonable search or seizure” (Canadian Law, 1982). Although there was no literature to be found where companies had sold or used Canadian user data or profiles stored on US-based educational Web 2.0 tools, this risk exists and needs to be acknowledged. The fate of the contentious American non-profit educational database, In Bloom, illustrates this point. InBloom was created as an educational database which stored student information and allowed teachers the ability to give students individualized learning based on the collected data (InBloom, 2013). This service was external to the school districts who were using it and accessed student information to create the individualized learning plans (InBloom, 2013). Because of the data that was collected, many started to worry about how that personal information could be shared, and in 2012, only 2 years after starting, the company decided that it was facing too much criticism and did not have enough public acceptance to make it work; it is no longer a functional education service (InBloom, 2013). Though the cross-border data storage situation is complicated as legislation in Canada differs greatly from that of the United States, in the case of InBloom it is

evident that even United States student data stored on United States servers by United States companies has raised concerns.

### **Learning Management Systems (LMSs)**

When students use an online classroom for their learning, they have to register to allow their teacher to see who is completing the work. Many learning management systems that teachers use only require a minimum amount of information to be provided for enrollment (e.g. name and a email address). This allows students to stay relatively anonymous. For the purpose of this review, the learning management system, Canvas by Instructure (Canvas <http://www.instructure.com/>), was evaluated to see how safe personal student information would be while using it. To be clear, there are two ways in which the Canvas learning system can be accessed: 1) through the cloud (that is accessed remotely on servers based in another location, and in the case of Canvas, the United States); or 2) on local servers (using a school or district server with Canvas software and data hosted locally). As my school uses the cloud option, this review will focus on the use of Canvas' cloud based server option.

When a teacher registers with Canvas she is required to state her organization type, title within the organization, the organization name, the teacher's name, the teacher's (or school's) phone number, the teacher's email and the teacher's location, only as specific as which continent (Instructure, 2014). Canvas' privacy policy is easy to understand, and they clearly state that they are committed to protecting the user's privacy (Canvas privacy terms can be found at <http://www.instructure.com/policies/privacy-policy-instructure>). Once a teacher has created an online classroom, the teacher is able to invite students to join – by invitation is the only way anyone is able to access a particular class.



## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

When a student receives a Canvas invitation from a teacher, the student registers using the ‘join code’ that was obtained through the email address the student registered with Canvas. Along with the code and email, a student is required to contribute her full name, a user name and a password. Canvas does not require students to give up any more personal information and they are able to create an ambiguous username so they can keep their identity protected if need be. Only the teacher has access to the email addresses of those students enrolled and through that email list the teacher is able to distinguish the identity of each student.

### **Web 2.0 Tools**

“Web 2.0, a term we use almost every day, is an ambiguous concept that refers both to a large and shifting set of technological tools and to an approach to the socially and technologically integrated use of technology” (Light and Polin, 2010). Web 2.0 tools are an educational resource which has become increasingly popular in recent years. Light and Polin (2010) conducted a research study and their results were interesting. They found that overall “these tools show potential to transform many aspects of teaching when [Web 2.0] teachers are thoughtful about how they use the tools and they are blended with careful instructional designs” (Light & Polin, 2010). This statement by Light & Polin (2010) implies that the teachers who know the capabilities of a tool or how best to incorporate Web 2.0 with their students will have the greatest success. Teachers who are unaware of the full capabilities of a tool have a gap in their knowledge and that gap can leave room for doubt, as well as security and privacy risks. This limits teachers’ ability to use a tool to its full potential and by extension the students’ learning potential with the tool can be similarly affected.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Web 2.0 tools are used for a variety of reasons. For example, tools such as DropBox ([www.dropbox.com/](http://www.dropbox.com/)) allow students to upload their assignments to share with their teachers instead of printing and mailing the assignment. Dropbox can be particularly useful in sharing large files as often email accounts have size limits when emailing attachments. For example, Gmail ([www.gmail.com](http://www.gmail.com)), a popular email service, has an attachment size limit of 25 GB and Hotmail ([www.hotmail.com](http://www.hotmail.com)) has a limit of 15 GB. Dropbox ([www.dropbox.com](http://www.dropbox.com)) has no file size limit for a single file; as long as you have enough room in your dropbox, you can upload a file of whatever size you choose (Dropbox, n.d.). Videos tend to be large files. Another option for students to share videos would be to give students access to uploading videos on YouTube ([www.youtube.com](http://www.youtube.com)). A teacher could use these videos to check in on student progress (such as reviewing a video of a student playing the piano or at a dance recital, etc.) and give a more accurate mark for the assignment. Video can also be a useful tool for capturing student responses to reading, current events, etc. Other Web 2.0 tools such as Prezi ([www.prezi.com](http://www.prezi.com)) allow students to create and share their presentations. Prezi is a more dynamic presentation tool than Microsoft PowerPoint. With Prezi the content is arranged on a virtual canvas and the creator defines a path through the canvas which can zoom in and out of various details. This gives a broader option than the linear static presentation allowed by Microsoft PowerPoint, and is free for students who do not have a presentation application on their personal computer.

Light and Polin (2010) also say that educators are using Web 2.0 tools to promote new avenues of communication among teachers, students, and the community in ways that can strengthen the community of learners. When thinking about fully online learning environments, creating a sense of community would be one of the biggest challenges that the teacher would face. Online teachers usually have as many, if not more, students than in a face-to-face

classroom. If the class is not designed for individual asynchronous learners, these teachers need to figure out a way to have the students connect as a learning community. When incorporating Web 2.0 tools into an online classroom, we are opening our students up to the world of self-expression and giving them a voice: we just need to make sure they are doing it in a way that reasonably manages their privacy in developmentally appropriate ways.

### **Legislation: PIPA, FIPPA & the US Patriot Act**

There are two different acts that are associated with the privacy protection legislation in British Columbia. Your personal information in certain circumstances will be covered under one of the acts but not both at the same time. As a simplified explanation, PIPA (SBC 2003, C-63) is the Personal Information Protection Act which in the area of education is associated with independent schools. In the wider scope, PIPA (SBC 2003, C-63) outlines the protection of privacy rules for an individual person, but also an unincorporated association, a trade union, a trust or a not for profit organization (BC Law, 2014b). FIPPA (RSBC 1996, C-165), on the other hand, is the Freedom of Information and Protection of Privacy Act which in the area of education governs public schools but more widely includes a ministry of the government of British Columbia, a local public body, an agency, board, commission, corporation, or office (BC Law, 2014a).

In the context of this review, PIPA (SBC 2003, C-63) will be looked at more critically to provide an overall picture of independent school expectations when dealing with student privacy. PIPA (SBC 2003, C-63) describes rules for private organizations when dealing with personal information. Two of the major aspects of legislation are that: “an organization is responsible for the personal information under its control, including personal information that is not in the

custody of the organization” and that “an organization must not [require] an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service” (PIPA SBC 2003, C-63). This again goes back to the teacher and the parent/guardian knowing what information is required and more importantly, why certain information is required for educational activities.

Parental/guardian and student consent for educational activities needs to be informed. In the case of an online learning environment this means the school or teacher must disclose the purpose for collecting the information before gaining consent and granting LMS access for students to complete work. For example, if a teacher wishes to use the LMS Canvas with her students, she must inform both the student and parent/guardian (if their child is a minor in age) that the information required is for the purpose of setting up an account to be able to access the classroom and what type of information is required. The teacher also needs to be aware of who is being taught in the online classroom so that young children are not placed in the same online classroom area as adults without specific permission. We as teachers and parents/guardians need to take all appropriate measures to make sure that we keep our students safe, whether they are young children or teenagers. When appropriate, as in the case of Canvas, the parent or guardian consent needs to indicate that the servers for the classroom data are located outside of Canada. The parent or guardian must be informed that the USA Patriot Act (2001) may entitle the US government to search through student profile data and work that is posted online (BC Law, 2003). It would be the teacher’s job in this case, to determine the data reasonably and safely necessary to complete an educational activity, with whom it can be shared, and to weigh the risks of storing that data on a US server. For example, inputting data for a family tree assignment complete with relatives (grandparents, parents, siblings, etc) full names with birthdates and

locations of births can present far more risk than writing a report on students' favourite sports or activities, including such information as what position they play, when they started to play the sport and why they enjoy it. Once the teacher is aware of the personal data required, and has gained consent for the specific activity, the teacher needs to ensure that the personal information shared on the system stays within the prescribed bounds agreed to in the consent form. Under the Electronic Transactions Act (SBC 2001, C-10), the consent form could be submitted through traditional mail as a printed copy, or electronic means such as through fax or an email service located on Canadian servers.

While “The Freedom of Information and Protection of Privacy Act (FIPPA) [and Personal Information Protection Act (PIPA) for independent organizations] mandates that no personally identifying information of British Columbians can be collected without their knowledge and consent, and that such information not be used for anything other than the purpose for which it was originally collected” (Klassen, 2011), the USA Patriot Act (2001) varies greatly from PIPA (SBC 2003, C-63) and FIPPA (RSBC 1996, C-165). The critical difference is that the US Patriot Act (2001) allows the United States government to search any information stored on a United States server at any time without giving notice to the individuals whose data is searched.

A firm understanding of PIPA (SBC 2003, C-63), FIPPA (RSBC 1996, C-165) and the USA Patriot Act (2001) needs to be in place for all teachers when using learning management systems. This understanding is needed so teachers do not create assignments that have personally identifiable markers that can put people at unnecessary risk, such as a genealogy project. By restricting personal information used on the learning management system, a search of the course

(if ever completed) would only show basic information such as completion dates for projects, assignments and grades given.

It should also be mentioned that each organization or school dealing with personal information is required to have a designated staff member responsible for ensuring that the information remains secure. This person, in theory, would know the most about the privacy laws and the protocol to follow should an incident occur where the privacy of an individual were breached. Teachers must also be aware that if at any time, after giving consent, someone wishes to withdraw it, they may do so at any time and the organization is required to inform the individual of the likely consequences of withdrawing his or her consent (PIPA, SBC 2003, C-63). When using Canvas, a withdrawal of consent for using the limited personal information needed (email address and name) would result in an immediate withdrawal from the course as it would prevent the student from logging in without an email address. However, the student could use a false name without having to be removed from the course.

### **What Parents and Guardians Need to Know**

In the past few years, many education opportunities have shifted to an online learning environment and technology-based platforms. As we continue to learn more about the capabilities of computer programs and apps, the online classroom will continue to have a larger presence in a students' learning every year. Maeroff (2003) describes this best when he states: "[developments] in online learning in just a little more than ten years forces one to conclude that this is a sea of change, not a fad" (p. 2). As stated previously, consent for online activities, whether using Web 2.0 tools or LMSs is something that needs to be in place before any online education occurs. This consent not only covers the school and teachers in situations where legal

action may be taken but also ensures that the families understand the major benefit and risk factors to consider when using online tools and resources, including the risks presented by any server locations which are outside of Canada.

Clear expectations for participating in the online classroom or using the online resources should be set out by the teacher in a way that is easy for the students to understand. Also any questions from the parents or guardians should be addressed before consent is given. Kerr, Barrigar, Brurkell, and Black, (2006) state that:

Although data protection laws around the globe generally require consent prior to the collection, use, or disclosure of most personal information, it is our contention that privacy laws based on Fair Information Practice Principles (FIPPs) must be understood as setting higher thresholds for obtaining consent than would otherwise be afforded. (p.7)

The best explanation of FIPPs found was published by the National Strategy for Trusted Identities in Cyberspace (n.d.), the author states:

In brief, the Fair Information Practice Principles are:

- **Transparency:** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions. Teachers should instill in students and their families an expectation that tools and services should clearly communicate to the user what personal information they collect, and how they will use it prior to obtaining consent, instead of blindly asking them to check a box.



When using online tools, rarely are you required to provide anything more than your name and email address. If you are using a tool that requires your physical location or address (for anything other than shipping information) this should raise some concern. It should also be stated that now more than ever, you should be aware of apps that are being used and how they are being used. Some apps allow you to ‘tag’ your physical location while using them, such as Twitter, Facebook, Instagram, etc. If the location services option is enabled, this would provide much more personally identifiable information than if it were disabled or deleted. The option of location services would not necessarily give your name or description but it would give your physical location at that given time which is a huge identifying mark if someone were trying to locate you. Overtime, such data can show patterns of behaviour that can be used to predict what people will do or where they will be. This clearly presents risks.

Teachers, parents, guardians and users of Web 2.0 resources need to understand the terms of use for each platform with which they have an account. The goal of my project is to make parents, guardians and teachers aware of the key privacy points for tools to be used in the classroom. Each Web 2.0 tool and LMS that are used are created with Terms of Service (ToS) or End User Licence Agreements (EULA) documents associated with them. The companies who create these documents usually have a step in the sign-up process where you have to agree to the terms before you can use their services. Although usually easy to find, Terms of Service documents are not always easy to understand. This is where creating documents that identify key privacy considerations and updating them every few months would help clarify key issues and make them easier to understand. Companies usually have two different ways of updating their terms: 1) they directly notify their users via email or notification within the tool or LMS; or 2)

they can change their terms without notifying their users which puts the onus on the user to constantly check for updates and changes.

Although there are many benefits to using Web 2.0 tools and LMSs in any classroom, teachers need to be aware that some parents and guardians will not give their consent for their child to use these tools. This is when alternate activities need to be in place to give these students similar learning opportunities. Parents and guardians may withhold consent for a variety of reasons and are not required to make those reasons known. Teachers may also want to advise parents and guardians to withhold consent if they know that there are concerns with the student. Students who are in the middle of a custody battle, students who are in the care of someone other than a family member at the decision of the court or government, and those students who have been a victim of some type of aggression are just a few examples where extra caution may be needed or withholding consent may be advised.

One final piece that students, parents and guardians need to be aware of is something that boyd (2014) states very well: “...even messages that were crafted to be publicly accessible were not necessarily posted with the thought that they would reappear through a search engine” (p. 12). Often students posting content online believe they are beyond the searchlight only to find out later that they aren’t. People say and do very different things when they believe others are not watching. Everyone needs to be aware that even ‘private’ messages and photos may turn up in a more public way than originally planned. This can be demonstrated with someone posting a picture to Facebook or writing a status post without having high privacy settings. The lack of high privacy settings allow their friends to re-share the photo or post so that instead of the original post being seen by the person’s 100 friends, there is a possibility that it may be shared exponentially by friends and friends of friends.

Educators need to communicate with our students that once you post something online there is no ‘take-back’, your digital footprint has been made (Hengstler, 2011; boyd, 2014). Digital footprints are described by Richardson (2008) as “online portfolios of who we are, what we do, and by association, what we know” (p. 16). Informing students about good privacy settings is how we can enable them and give them the tools to help themselves stay protected. How students view privacy settings and sharing personal, identifiable information will change with age. While a 6 year old may not post her “real name” on a blog, a 17 year old writing an academic blog may want her name associated with the work to help create a positive digital footprint that can be shared with prospective employers and university admissions. Each group of students that are taught in the online world will have different needs and challenges. As teachers, we are not going to use the same tools with a grade one class as we would use with a grade twelve class because the maturity levels and comprehension / rational thinking skills are very different between the two groups. With grade one the tools used may be reading logs and activities websites and tools while in grade twelve wikis, blogs and Twitter might have a bigger role in the student learning.

When we choose different tools and resources to use with certain age groups and classrooms, we also have to modify our expectations and guidelines accordingly. Hengstler (2013) does a good job of summarizing and showcasing the different student scaffolding levels in her Scaffolding Participation and Student Scaffolding models (see Appendix C). To summarize her models, students start out as users who have age-appropriate activities through a parent, guardian or teacher on a class account and move toward participation on their own within a contained setting where all the participants are known and then finally they have enough digital awareness to have full participation, including participation in open systems where school or

district permissions as well as parental/guardian permission are also given. Another way

Hengstler (2014 c) states this is that students will move through three phases. These phases are:

1. Digital by proxy - students work will be posted through their parent or teacher using parent or teacher accounts;
2. Digitally coached - when a parent/guardian decides that risks of a certain tool can be managed by their child and the digital footprint they leave won't be damaging to them later in life;
3. Digitally independent - when a parent decides that their child has the knowledge and maturity to stay safe in online environments and choose for themselves what is posted using their own account.

## **Professional Standards**

In British Columbia, there are two general bodies that guide professional standards for teachers both in public and independent schools, the British Columbia Teachers' Federation (BCTF) and the Teacher Regulation Branch (TRB) of the British Columbia Ministry of Education. The BCTF has set out a members' guide for all teachers with a valid BC teacher license. This guide helps teachers to know what is expected of them and also what they can expect from BCTF in terms of support. This document lacks specific information regarding the use of online tools. At the time during which the guide was written, there was an extensive labour strike in the public schools. It is possible this section of the guide may have been overlooked. Even so, there are some pieces from the guide that would support and lead teachers to professional conduct when using online tools. The following responsibilities can be found on page 132 of the Members' Guide to the BCTF (2014):

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

- The teacher respects the confidential nature of information concerning students and may give it only to authorized persons or agencies directly concerned with their welfare. The teacher follows legal requirements in reporting child protection issues.
- [The teacher is] mindful of the student's safety, the student's right to equality of opportunity and successful learning experiences, and is considerate of the child's personal circumstances.
- In relation to parents or guardians, the [teacher] co-operates with the home whenever possible.
- The [teacher] takes appropriate steps to protect the rights of the student.

The underlying theme of all of the statements from the BCTF guide all point in one direction – the teacher has a responsibility to keep his or her students safe. With respect to LMSs and Web 2.0 tools, this is done by giving parents and guardians all the information that is needed to make an informed consent choice. This presupposes that the teacher communicates the reasonably expected possibilities, drawbacks, and privacy concerns associated with the LMS or Web 2.0 tool she/he would like to use. In other words, the teacher has “the responsibility to exercise professional autonomy in determining the methods of instruction and the planning and presentation of course material” (BCTF 2014, p. 19) so long as they understand how to use it safely and properly.

Educators in British Columbia also are governed by the Teacher Regulation Branch (TRB) who sets standards for teachers to follow. In 2013, the TRB released the “Independent school teacher conduct & competence standards” as well as the public school teacher conduct & competence standards. When looking at the two documents, there are no significant differences but there are some points that need to be followed by teachers working in all classroom settings

and especially online classrooms. A brief overview of the eight standards from the TRB (2013) are:

1. Educators value and care for all students and act in their best interest.
2. Educators are role models who act ethically and honestly.
3. Educators understand and apply knowledge of student growth and development.
4. Educators value the involvement and support of parents, guardians, families and communities in schools.
5. Educators implement effective practices in areas of classroom management, planning, instruction, assessment, evaluation and reporting.
6. Educators have broad knowledge bases and understand the subject areas they teach.
7. Educators engage in career-long learning.
8. Educators contribute to the profession.

As stated previously, all of these standards apply for all teachers, no matter the school setting but some need to be highlighted for the purpose of online learning environments. For example, where teachers are required to care for all students and act in their best interest, they need to understand the range of capabilities of online resources. It is through such understanding that teachers are then able to make informed choices whether the benefits of the tool outweigh the risks. Teachers are also expected to act as role models for students. If teachers practice good digital citizenship in their online classrooms and teach students about what being a good (and safe) digital citizen looks like, teachers are then doing their due diligence in keeping students safe. One last standard that I believe to be very important specifically in online learning is the standard where educators are expected to implement effective practices in areas of classroom management, planning, instruction, assessment, evaluation and reporting. When teachers use the

online resources available to enrich student learning, they are opening up new ways for students to view different media (text, video, audio), present their learning and understanding (moving away from solely relying on worksheets and tests) and allow them to engage with each new concept that is introduced.

### **Conclusion**

Informed consent is one of the top priorities for teachers wishing to use LMSs and Web 2.0 tools based on servers outside of Canada and specifically in the United States. The ability to remain fully within Canadian borders with online content would be challenging for someone wishing to have a fully online classroom with complete functionality. In order to obtain informed consent, a teacher has a number of steps to complete. She must first understand all the terms of service and privacy policy of the tool or LMS. Once the teacher understands the terms of using the tool or LMS she has selected for educational use, she must decide whether the benefits outweigh the risks and decide to what extent the resource will be used. Once the learning objectives are clear, the teacher relays the policies and intended use information to the families in a way that is easy for them to understand. The teacher should also have the full policies available for parents/guardians and students to read if they wish. Parents/guardians will be able to give informed consent once the student and legal guardian understand the terms of service, the reason why the tool will be used, as well as the potential risks and how they will be managed.

As Ferrier (2011) puts it so well, “Instead of teaching students to be afraid of what others can learn about them online, let's teach them how digital footprints can quickly connect them to the individuals, ideas, and opportunities that they care most about” (p. 93).

## Chapter 3

### **Choosing Initial Tools and LMSs to Focus on**

I currently work as a distributed learning teacher in British Columbia, when I started this project I collected the enrollment numbers for each of the Web 2.0 Tools that have students using them. When I was compiling the tools and resources for this project, I focused on ones that would have the most benefit to myself and my colleagues who also work at my school. To collect potential tools for evaluation and inclusion in the Electronic Performance Support System (EPSS), I had my colleagues email me a list of online resources that they currently use with their students. From that list, I chose the ones that were mentioned most often. From this list, I decided to select both public and restricted access tools and resources (for more information on these classifications, see Appendix D).

I chose both public and restricted access resources because I believe that authentic learning happens when we interact not only with the information provided to us, but also when we are able to explore that information and share it with others. When referring to public tools, these would be tools such as Twitter and blogs where users post content that is then visible to anyone who knows their username or has access to their website. Restricted access resources are LMSs such as Canvas where the user needs to be invited in to a certain area where content is posted either solely for the user, and/or for people to whom the user gives access.

There were two main selection criteria for the public tools (such as Twitter and Pinterest): 1) it was a tool that can be used with our school's LMS, Canvas; 2) colleagues were willing to share relevant selected resources for these tools that would help decrease project site development time. In effect, these shared resources would be the first collaborative pieces



contributed to the EPSS. The initial phase of the EPSS contained documents for Canvas, Edmodo, Kidblog, Mathseeds, Office 365, Pinterest, Reading Eggs, Reading Eggspress, Twiducate and Twitter. (Refer to Appendices E and F for examples of documentation found in the Privacy Compass). This selection of Web 2.0 tools and LMSs has something for every grade level and most of these tools can be used for more than one subject. The diversity of resources chosen allowed others to have access to resources that would help them, even though the EPSS is still in its emerging stages.

Although Office 365 is not a Web 2.0 tool that is shared with others, it was chosen because the content that is typed and uploaded or saved by the student remains in the cloud (as it is a cloud version of Microsoft Office) and therefore, my school felt that informed consent was necessary for anyone using this tool. Twitter and Pinterest were chosen as they were resources that had already been partially created prior to this project. They are also important as the EPSS should not shy away from including open tools such as these. Open tools are not scary things, they just need to be understood and students need to be taught the proper cyber safety when using them. Edmodo, Kidblog and Twiducate were added as their documentation had already been partially developed by my academic colleagues and they gave me permission to modify them for use in the EPSS.

Once these documents were created, it was evident that there was a lack of resources for Web 2.0 tools to use with primary students. Currently, most web based tools and LMSs are geared toward the 13 years and up population. As many teachers at my school use Reading Eggs with their students, this directed my efforts in creating the related EPSS documents for this Web 2.0 tool. While compiling the information from the Reading Eggs website, I noticed that the two other sister sites, Reading Eggspress and Mathseeds, had the same privacy policies and terms of

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

service. I was able to leverage this similarity to quickly create documentation for Reading Eggspress and Mathseeds. This expanded the tool choices and subject materials for primary teachers.

As an initial step toward developing the EPSS, I collected related documents in my school's database for other teachers to access. As that database is a password protected system for employees only, I also needed to house the content in a second location for more public access. Weebly ([www.weebly.com](http://www.weebly.com)) was chosen as the secondary location to be accessed by others external to my school. Weebly is a free to use website (with paid upgrades available) that allows anyone to create an account and start building a web presence, whether a blog, an online store, or a new website. Weebly was chosen because it allows for many people to simultaneously view content and also allows for commenting on the provided content. The EPSS is envisioned to enable user comments. Such comments will support future users looking for policy alignments within particular schools or districts. An example of comments that I hope to receive are "I have checked with my school and I know that this resource evaluation complies with school district XX" or "This tool needs to be used in a slightly different way to be used in SD XY. You will need modify it for..." In the Weebly location, I posted a request for potential collaborators or contributors. I shared the review mechanism I created to assess tools and services, and directed potential collaborators to send any documents they create to me for review, uploading and sharing with others.

### **Privacy Documentation and Application**

The privacy documents that I have created to use within this EPSS are the main body of my work. These are what teachers can use with their students and how teachers will ensure that

parents and guardians have enough knowledge about the Web 2.0 tool or LMS to make an informed decision about giving or withholding consent. Some of the documents that are currently in the EPSS have been created by colleagues and I have modified them with the original authors' consent.

The purpose of these documents is to have an exemplar for teachers. Teachers can modify the documents in a way that works for them and their students. It is expected that these documents will change over time. By providing an initial benchmark, this EPSS can allow teachers to become more aware of the privacy risks and take proactive, preventative steps to avoid them. As Hengstler (2011) would say, the EPSS will support teachers in going from ostriches to eagles to get their heads out of the sand, to stop ignoring the technology hoping it will go away, to move toward preparing ourselves for using it and to take it as far as possible with as much information as possible.

The data in the documents was tagged with metadata in hopes of framing it in a searchable database architecture. These tags would be used to generate comparison charts based on a user's selected criteria. This generated chart would show all the Web 2.0 tools and LMSs that have been previously vetted. This means if a teacher is looking for a tool that may work for a grade 3 social studies class, she can search by "primary grades" and "social studies". The EPSS would then generate a chart with all the tools that have been suggested or 'tagged' for that subject and age group. I have also structured the metadata to tag the location (province, country) and school (public or independent) of the person who vetted the tool and/or created the documents. This was done in hopes that this type of information will support teachers' decisions to use a specific tool in a specific context.

The intended way for a user to work through the EPSS is to have the teacher first read through the Teacher Documents. The Teacher Documents provide necessary privacy information relevant to a specific tool. These documents support teachers' decisions to use or avoid a specific tool. The EPSS is also structured to allow parents/guardians to look through the contents and read the parent/guardian information for themselves. Parents/guardians may be curious about a particular tool or may desire information when they believe the teacher may not have given sufficient information before obtaining consent. Lesson ideas are provided to support teachers who would like to start implementing Web 2.0 Tools with their students but are not sure how to start or what subjects to use it with. These lesson ideas present a very small sample of the immense learning possibilities with a given tool.

Once teachers understand what the associated risks are with a selected tool and what they specifically intend to use the tool for, teachers should then look at the Parent Documents to make sure that all information is relevant to their situation. With appropriate administrative review or approval, the Parent Documents can be adapted as necessary to a particular school's context. The goal of communication with the parents/guardian is to have them understand: what the tool is; the educational rationale for using the tool; the specific ways the tool will be used; the reasonably foreseeable privacy risks, and how they will be managed, and the possible alternative activities should consent be withheld. The consent form can be modified to include a selection of information from the Teacher Documents as well. The consent form is sent to the parents and guardians to sign and return to the teacher. (See Figure 2: Workflow design for The Privacy Compass.)

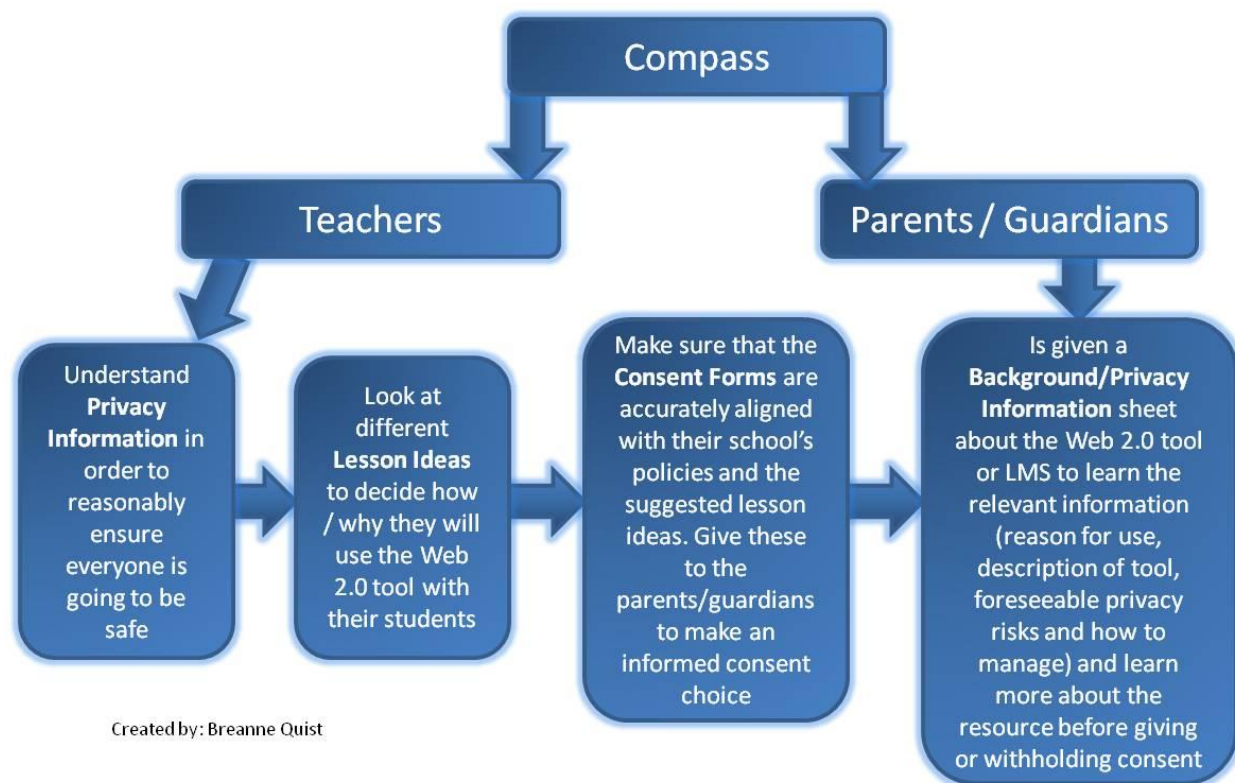
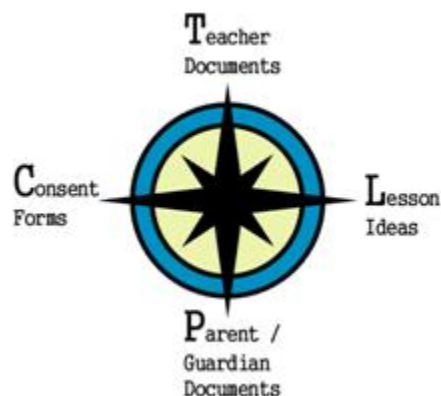


Figure 2: Workflow design for The Privacy Compass. This chart shows the intended use of the Privacy Compass.

## The Privacy Compass

Choosing the title for my tool was one of the last things that was done with this project. The title of the project went through many different versions before the final one. A name would be chosen and used but after further modification of the resources, I would find that the name no longer suited the reality of what it was. Most names seemed to be very specific to a certain area (British Columbia or Canada) and my main goal was to make this a tool that could be utilized by any teacher anywhere; this is when the final title was created: The Privacy Compass for Web 2.0 Tools: Helping Teachers Navigate Challenging Terrain. I chose to use the wording Web 2.0 Tools as this is a term that is becoming more well known and it leaves the door open for the Privacy Compass to address a wide range of tools.

Once I had decided on the Compass title, creating the Compass was the next step. The compass image gives users a visual when using the EPSS because a compass is inherently understood to guide people. When you look at a compass, the first thing most people look for is N or north. For this reason, I made sure that the teacher was placed at the north end of the compass. This is significant as the teachers using the compass need to have a firm understanding of their specific tool selection before they can propose it to their students and the parents and guardians of their students. The teacher is the one ultimately deciding if they will use a Web 2.0 tool with their students and after that it is the individual choice of a parent or guardian as to whether they will give their child permission. For this reason, the parent or guardian is located on the south side of the compass. Placing consent forms and lesson ideas on the compass were the last orientations of the Compass. In Western culture, reading moves left to right, this orientation which determined the west side of the compass would be seen first. In my estimation, the consent forms are more important than the lesson ideas. This guided my decision to place the Consent Forms on the west side of the compass, leaving the east for Lesson Ideas.



*Figure 3:* Compass icon. This icon was creating to give teachers direction while using The Privacy Compass.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

The website is divided into 5 sections, some with sub sections.



*Figure 4:* The Privacy Compass homepage screen shot. This screen shot shows the different headings on the website as well as the mountain graphic which is embedded on the top of each page.

The home page has information about The Privacy Compass and how to use it. The Compass itself includes the alphabetical list of the tools reviewed so far, the comparison chart (See Appendix G) for all the tools currently in the database, and a submission form for anyone who would like to add to the database. I decided to use icons to go along with all of the documents to give a clear visual for the user to identify instead of solely scrolling through text-based document names. (These icons can be found in Appendix H). The website has a section called Additional Resources with a glossary of terms; eSafety resources; links to relevant legislations, sites and publications such as PIPA (SBC 2003, C-63), FIPPA (SBC 1996, C-165), Federation of Independent School Associations, British Columbia (FISA BC) and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC); and finally, further reading and resources to help teachers integrate the Web 2.0 tools into their practice. The last two navigation sections are a biography with information about me and my master's work, along with a contact

page to make it simple for anyone to get in touch with me. (To see the full layout of the drop down navigation menu, refer to Appendix I).

The website was created to be as user friendly as possible in order to encourage users to refer back to it whenever they are considering a new Web 2.0 Tool or LMS to use with their students. This Compass was designed to help many teachers navigate through the world of Web 2.0 tools without feeling overwhelmed about having to search for all of the relevant information themselves.

Some school districts or independent schools will choose to allow or disallow certain Web 2.0 tools for the entire teacher population. This practice is more commonly referred to as ‘whitelisting’ or ‘blacklisting’. This practice can either eliminates the risk altogether or greatly increase it. If a district has decided that a tool is allowable for all their teachers, they usually include a very simple consent form without much information going to the parent or guardian about the potential risks. When this is the case, there is a greater chance for the teacher to encounter problems with improper use if they do not understand all pieces involved. Even if eSafety courses have been taken by the students, if a district has banned a certain tool for all teachers without weighing the risks and benefits, learning opportunities can be missed. Such blanket decisions are usually made due to fear of privacy risks. This Compass was designed so the documents could be modified to fit with certain school or district policies. The central idea behind the creation of the Compass was to support the teachers and schools who are moving forward in LMS and Web 2.0 use.

### **Levels of Risk**



The permissions needed for the Web 2.0 Tools and LMSs will not be the same for every school or district. The permissions needed depend on specific activities that will be completed using the Web 2.0 Tools. When a teacher gains consent from a parent or guardian, she will have to clearly articulate the reasoning for using the tool and how it will be used. For example, a teacher may want to use Twitter to “tweet” about current events. Some teachers may use Twitter to have students ‘tweet’ via a class account where there is a shared password. Another teacher has students create their own accounts from which to tweet. The first situation would keep the students safer but at the same time, the students could login to the account at any time (at home without the teacher supervision) and tweet things that may be inappropriate. As there could be up to thirty people sharing the account, it could be challenging to figure out who originally sent the inappropriate tweet. In the second example, the students are responsible for their own tweets but is their Twitter streams are public anyone can potentially them and send them private messages (although users’ accounts can be reported and blocked). In the second example, there is this potential for contact with external people which can cause concern.

Teachers, parents and guardians also need to be aware that certain Web 2.0 tools and LMSs have different levels of risk exposure. In chapter one, the Sharing Circles graphic (Appendix D) was used to explain that in a simple graphic form. In the Sharing circles framework, Web 2.0 tools are classified according to three levels of content sharing:

- Invite only access: What is posted is only viewed by the student who posted it and those who are specifically given access in consultation with the teacher. The consultation with the teacher is critical. Although the student owns all the rights to the work, it should only be shared in situations where it is deemed appropriate and necessary by the teacher. An

example of an Invite-only tool reviewed in the EPSS would be Office 365 where students only see their own information but have the ability to share with others if needed.

- **Restricted Access:** What is posted by the student is accessible to others within a defined restricted user group who are specifically given access. This is usually when a teacher sets up a class account and then all students who have gained parental or guardian consent are given access. Examples of this type of resource reviewed in the EPSS would be Canvas or Kidblog. In both tools, a teacher has to create a private classroom area and then invite students to join by sending an email or giving an access code.
- **Public Access:** What is posted is visible to the entire online world. There is no control over who sees what the student posted and what others may do with it. Examples of this type of tool reviewed in the EPSS would be Twitter or Pinterest where students post their own work, or something that interests them and everyone else is able to view it.

I have encountered some challenges in applying my Sharing Circles classification system to Web 2.0 tools. The best example of this challenge is the classification the Web 2.0 tool Pinterest. For the most part, anything you pin on Pinterest is visible to the entire Pinterest community (and also in Google searches) but if an individual creates a ‘secret board’ then it becomes an invite only resource because only the user (and those they share it with) can see what is posted on the secret board. Pinterest can therefore be both “Invite-only” and “Public”. Further refinement of this classification system will be necessary.

Within The Privacy Compass, I also made sure to include the eSafety Incident Response chart (adapted by J. Hengstler, 2013 from Kent County Council). This chart shows what steps need to be taken in the case of inappropriate activity within a Web 2.0 tool, LMS, or on the internet in general. There is a black and white copy of this chart for easier printing on any

machine, or a colour copy. This chart was originally adapted by J. Hengstler (2013) specifically for the British Columbian (Canada) context from work done by Kent County Council. It is currently in use in schools such as the Cultus Lake Community School, Chilliwack School District (33), British Columbia (Hengstler, Krivel-Zacks, & Kroeker, 2014). I have modified this chart slightly and included two file format versions on the EPSS site. There is a PDF version so that others can print it out quickly and hand write in all relevant phone numbers and contact information. There is also a Word document format so that the information can be neatly typed into the chart in before printing. This eSafety Incident Report chart quickly allows the user to see what steps need to be taken to provide the most support and safety for everyone involved when a potential risk has been encountered. (For a graphic of this chart, refer to Appendix J).

## Chapter 4

### **Field & Beta Testing of the EPSS Site**

Though the EPSS site has been “live” since its early stages on Weebly (with varying titles in the heading), I did not publicly announce its existence until mid October 2014. Several people accessed it before I publicly announced it and have used the information they have gained from the documents. I had some users email me once they had looked at the tool. All users who contacted me with suggestions commented on the ease of use of the website and the ability to easily move through all the different navigation tabs. While users found the comparison chart

easy to follow, they expressed a desire to be able to only view the tools they are specifically interested in, versus all of them at once. I have taken this into consideration and this functionality should be incorporated into future versions.

My early website statistics showed very few visits between mid September (when I established the Weebly presence) and early October 2014. (See Figure 5: Unique visitors to my site).



*Figure 5: Unique visitors to my site. This graph shows the unique visitors to my site one month prior to my public launch and the first four days after the public launch.*

Six hours after the public launch, my website statistics showed over 250 unique IP addresses had accessed the EPSS site. This number grew to 341 people seven hours after launch. I owe credit to certain individuals who tweeted or retweeted about my project and have many followers such as @jhengstler, @rlabonte, @glenhansman, and @BCTF. The fact that these individuals took action to share the EPSS as a resource with others, points to the importance of the work. I have to admit that I am completely humbled by the amount of support I have already received and this only encourages and inspires me to continue my work. I hope to make it an internationally recognized resource. Four days after launch, the website has reached 780 unique visitors. Figure 5: Unique Visitors to My Site shows the span of visits from one month prior to

the public launch to the first four days after the public launch. The figure reveals the interest evidenced in the EPSS from September 20, 2014 (0) to a mid October high of almost 400 unique visitors. As of October 22, 2014 the EPSS surpassed 1000 unique visitors. I revealed this site to my administration. When I shared this information with them, they realized the significance of it; consequently, our staff training with The Privacy Compass has been scheduled for immediate implementation from a previously scheduled day in May 2015.

### **Choosing a Database**

After I had chosen the tools and LMSs that I wanted to focus on for The Privacy Compass, I started looking at databases frameworks that would be feasible for me to learn by myself and use as a starting point. My initial work was to identify a database architecture I could manage as a proof of concept. Ease of set-up was a big part of my selection criteria. I sent out a tweet, via Twitter, to ask as many people as possible for database recommendations. Many different people recommended MySQL (although there were a few other databases recommended as well). MySQL was attractive because they had a free ‘community edition’ with paid editions if I chose to grow this database in the future. As many people had suggested MySQL to me I believed that I would be able to effectively establish and deploy a database on MySQL for the EPSS. After many frustrating hours, I determined that MySQL would not work for me. I also toyed with the idea of using ZenCart as I had previous experience with it, however it has more of an e-commerce orientation so that was not a viable choice for the project either.

I resorted to searching the internet to see what Google would suggest. I found the company Caspio and decided to experiment with the product Caspio Bridge. An attractive feature was the large number of tutorial videos available for self-support. Although I could not

set metadata tags as easily as I could with ZenCart, I was still able to input all my required metadata and make it searchable in the way I wanted people to be able to search through the database. The features I liked most about Caspio Bridge were that it was free to use, there was nothing to install, and I could embed my search form and documents right into my EPSS website ([www.breannequist.weebly.com](http://www.breannequist.weebly.com) or [www.privacycompass.ca](http://www.privacycompass.ca)) without much effort. The database displayed well embedded in my site; however, after a few days, I found that my 'free trial' had expired. The company required my credit card information to continue using the software so that I could be charged automatically if I went over my free allotment. While I was able to pilot a database infrastructure for the EPSS site, for now the search function has been moved to 'in development' until I gain further support for this project site in either technical support, funding, or both.

### **In Development**

Since I was not researching users and there was no collection of user data, ethical reviews were not necessary. Ethical considerations were used when teachers requested that certain Web 2.0 tools be included in the documents, as they needed the documents to be produced in order to start using certain resources with their students. It would be useful to have a poll option where (during a time period that is appropriate) a poll is conducted to see where documentation development efforts could be focused. Such a poll would allow for a majority vote opposed to randomly selecting Web 2.0 tools for documentation development. If a resource did not have the

majority vote, the documentation could still be created by someone who is in need of them and then submitted for review before being added to The Privacy Compass.

In my future work for my school I will be developing documentation for Rosetta Stone and Weebly. I chose these two tools because they are currently used by my school colleagues and documentation is necessary. My school currently uses Rosetta Stone for some second language courses and although it is not a high risk Web 2.0 tool, the proper documentation is needed to have informed consent from the parents and guardians of the users. With Weebly, the documentation development has been started a colleague as she required it for her classroom. Once the Weebly documentation is completed it will be moderated by myself and then uploaded into The Privacy Compass. In future work some form of voting and collaborative submission will determine the next tools added to The Privacy Compass.

### **Future Considerations**

In order to support teachers' responsible and reasonable use of LMSs and Web 2.0 tools in compliance with PIPA (SBC 2003, C-63) and FIPPA (RSBC 1996, C-165), my hope is that this project will further develop to include a searchable database for quick and easy access to specific types of tool documentation. In the current iteration, the project provides tool documentation in the form of 3 files: a teacher document, a parent and guardian document and a consent form (occasionally there is a fourth file for lesson plans if creating lessons with the tool is possible). If this content were to be put in a database with metadata tags then people who accessed this database would be able to more specifically target the information they seek,

thereby enabling them to more readily select and use LMSs and Web 2.0 tools. Parents and guardians would also be able to use The Privacy Compass. For example, parents and guardians who wanted to know the parent/guardian information for a particular tool could search the database for the relevant parent/guardian document. Teachers who only wanted to adapt an exemplar consent form for a specific tool could search the database for one that could be easily modified for their needs. While the current tool count is at 10, as the project develops it will be more difficult to search through 50, 100, or more sets of documentation. A search function and database structure with metadata are necessary.

Once the search function is a possibility, it would be my hope that a ‘click to compare’ option would follow soon after. This option would function similar to one you would find on a retail website when you are trying to decide between two versions of the same product. With this option, a user would be able to click on the resources he or she is interested in using and then compare them to each other to see if any are more useful than others for a particular reason.

The Privacy Compass could later expand to include documentation that describes privacy or other issues encountered when using a specific a tool. As each website and tool change their terms of service and privacy policies at unknown intervals, a revision schedule would be hard to maintain. A 6 month cycle for review of tool privacy policies and terms of service would be necessary to determine if the existing documentation in the database was still applicable and/or whether it required edits. As the number of tools in The Privacy Compass grows, it may be impossible for any single person to keep up with changes in terms, privacy risks, etc. More resources and support would be required. Ultimately, it would be up to the teacher using The Privacy Compass documents to make sure that the ones they are using have a compilation date



that matches the most recent terms of service date for the tool. If these dates do not match, a comments function and moderated content could help to update the EPSS documentation.

On the website for the Privacy Compass there is a database submission tab. There, users will find the document submission template used to evaluate a LMSs or Web 2.0 tool.

Completed templates could then be submitted to me. When I receive submissions I will moderate the content to make sure that it is acceptable, accurate and applicable. I will then be able to add it to the EPSS and grow it faster than if I were to create all the documents by myself. After talking with others who have started to use The Privacy Compass, I found that the template was necessary to keep all documentation similar and easy to understand. With this in mind, the parent documents have the same headings throughout so that parents and guardians who have seen a few documents can easily find any information that they are searching for without having to read the entire thing each time.

## Chapter 5

### **Next Steps**

There are several key areas in which I would like to extend this project work over the next year:

- expanding number of tools for which there is available documentation
- moving content to a database structure that will be searchable
- disseminating the project's website and tool, The Privacy Compass
- expanding the regional and national scope of The Privacy Compass

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

One extension activity is to create or solicit more documentation on different LMSs and Web 2.0 tools to be included in The Privacy Compass. While including every Web 2.0 tool or LMS created will never be possible (there are many in existence already and new ones are being created all the time), the goal of The Privacy Compass should be to provide a strong base of documentation for popular tools for educational use. The addition of submission documentation will allow for others to contribute documentation for tools not currently covered in The Privacy Compass.

I would also like to connect with students in the Online Learning and Teaching Diploma (OLTD) course, OLTD 506 (Special Topics: Social Media), currently taught by J. Hengstler in Vancouver Island University's Faculty of Education. In Hengstler's course, students are asked to develop documentation for social media tools, much along the lines of the tool documentation in The Privacy Compass. My documentation prototypes for The Privacy Compass were an outgrowth of the work I began in OLTD 506. When I began this EPSS project and developed The Privacy Compass, some of my cohort mates shared their OLTD 506 tool documentation with me. I was able to readily adapt their documentation for use in The Privacy Compass. If Hengstler's course continues to require creation of social media tool documentation for use in BC classrooms, a collaboration with The Privacy Compass could provide a way for Hengstler's OLTD 506 students to share and showcase their work while benefitting other teachers and expanding available documentation in The Privacy Compass.

Another step in the evolution of this project is to transition the information into a database infrastructure and make it searchable. While I was able to do a proof of concept, it is clear that the project requires someone with technical expertise in databases for this to occur. I would need to solicit the in-kind human resource contributions, or funding from a partner group

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

to make the database transition. I will be looking for partners to contribute to this project or to provide funding to find the right people to do what is needed. Funding for The Privacy Compass or in-kind support would be needed to quickly scale this project to a larger database, as I cannot currently commit the necessary time to this development aspect of the project.

A further step for this project is to find partners who are willing and able to disseminate this work to a larger audience and have as many teachers aware of it and using it as possible. There has already been interest from the Canadian eLearning Network to introduce it across Canada; hopefully this will increase the number of Canadian teachers in BC and beyond who are aware of The Privacy Compass and are willing to use it. I am also going to conferences across BC and Ontario to raise awareness about The Privacy Compass as a tool to support teachers' responsible use of LMSs and Web 2.0 tools while navigating privacy concerns..

In the coming months, I will be adding a risk assessment to each Web 2.0 Tool or LMS in The Privacy Compass., I have already created a 5 level privacy risk framework. Figure 6 shows the current prototype for the risk levels framework (See Figure 6: Levels of Risk Exposure).

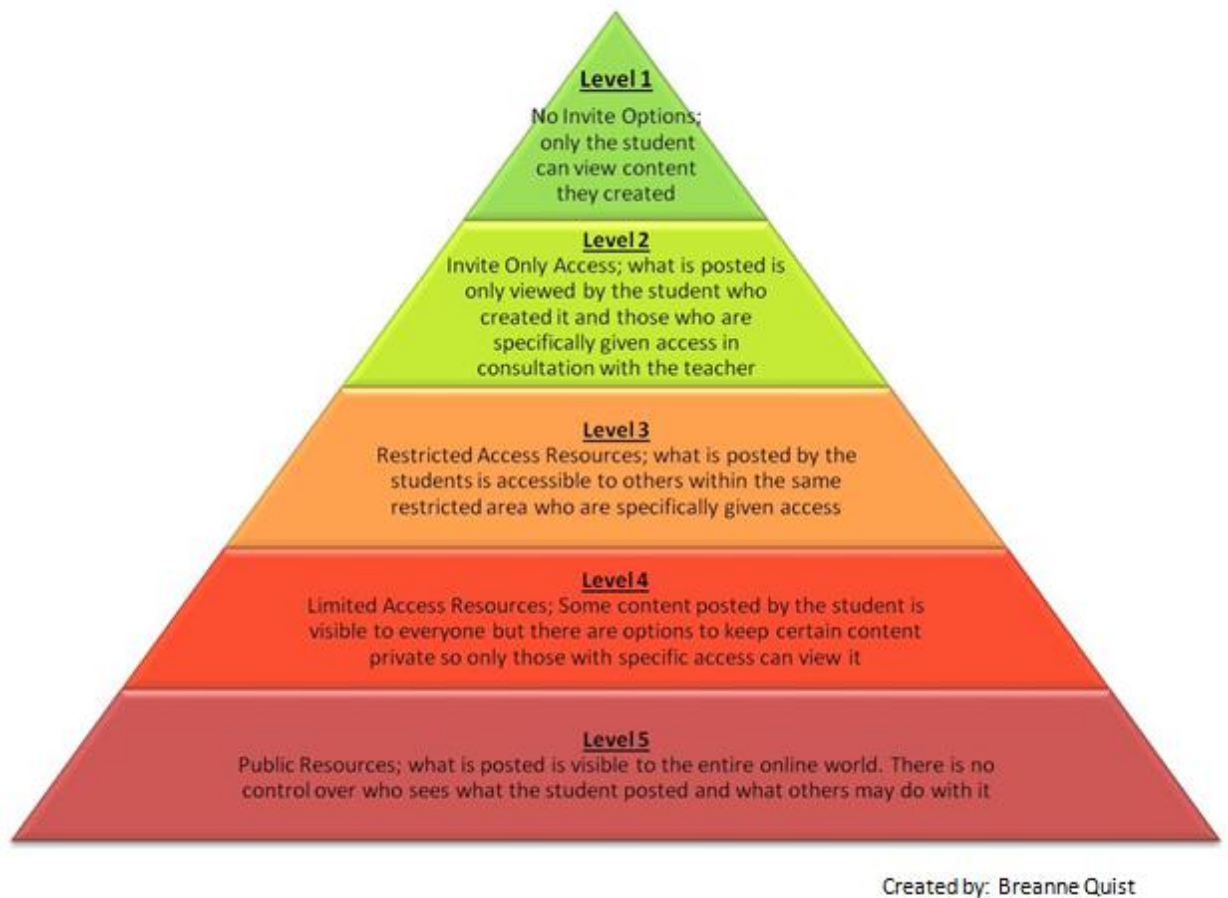


Figure 6: Levels of risk exposure.

While the framework will need further refinement, the idea is that a privacy risk assessment would be conducted and a tool in The Privacy Compass would be tagged with relevant metadata regarding its risk level classification and linking to a description of the classification.

## Recommendations

If partners such as the Canadian eLearning Network, the British Columbia Ministry of Education, or British Columbia Teachers' Federation were to support this project, it would allow for further development of The Privacy Compass. I would like to do additional work to investigate how, if at all, teacher willingness to use Web 2.0 tools and LMSs could be affected by exposure to and use of The Privacy Compass. Teachers could be assessed both pre- and post use of The Privacy Compass for placement along J. Hengstler's (2014) FIPPA Compliance Continuum. (See Figure 7: The FIPPA Compliance Continuum).



Figure 7: The FIPPA Compliance Continuum. (J. Hengstler, 2014: Graphic used with permission of the author).

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Such a study could also be done on a small scale during conferences and seminars where information and use of The Privacy Compass were shared. Attendees could volunteer as participants, state where they are currently on the FIPPA Compliance Continuum (Hengstler, 2014) before attending the seminar and then state where they think they are once they have completed the session. This data could then be examined to determine if there was a perceived change after exposure to The Privacy Compass.

While conferences and seminars will be a way to inform the public about this tool, it will only be heard by those in attendance - those who deem it of high enough importance to attend. To be able to reach a bigger audience, it would be useful to have the British Columbia Teachers' Federation and British Columbia public school districts recommending use of The Privacy Compass. If districts and teaching groups are able to share this resource with their members, this could signal that privacy considerations while using LMSs and Web 2.0 tools with students is important and that The Privacy Compass is a useful resource to support this work. Having the Privacy Compass included as a recommended teacher resource could be of particular use for teachers who currently avoid using online tools with students because of the 'unknown' risks. Through reading and using the documents provided by The Privacy Compass, those risks could then become known and minimized with methods provided to reasonably manage those risks

My immediate extension work with The Privacy Compass is to start presenting on it at professional development days in my school as well as others around British Columbia. I will also apply to present on this work at conferences. Social media is another great way to quickly disseminate information about The Privacy Compass to a vast audience. By leveraging some of my 'followers' on Twitter, I believe I will be able to exponentially expand my audience over the

course of a few days. For example, within the first week of my public release of The Privacy Compass, my more influential followers re-tweeted the link allowing me to reach approximately 10 000 people through their networks of followers.

### **Conclusion**

The idea for this tool began in my post-graduate work in the first cohort of the Online Teaching and Learning (OLTD) program at Vancouver Island University's Faculty of Education. Specifically, I created the prototype documentation as an assignment in J. Hengstler's OLTD 506: Special Topics-Social Media course. At that time, my cohort-mates created similar documents for other social media tools. After the course, J. Hengstler suggested via social media that it would be useful to have a central location to share this type of work with other teachers in British Columbia. To our combined knowledge, no one took up that challenge. The Privacy Compass was inspired by this call to action.

Firstly, this tool met a very real and very important need for my own school to provide documentation for the LMSs and Web 2.0 tools that my colleagues and I use with our students. The relevance and need for this tool at my own school is clear: our introduction of The Privacy Compass had been scheduled for a May session, but when my work was shared with an administrator, the school-based training on The Privacy Compass has been moved up significantly. That others are interested in this work is evident as well. Before the official public launch, I began to receive emails about the content in the website. Within six hours of the official launch more than 250 unique IP addresses accessed the project website. Within a week of public release, The Privacy Compass received well over one thousand visits from unique IP addresses. Numbers continue to increase.

When I first started this project, I did so with four guiding questions in mind. I first looked at what student privacy issues, if any, teachers in BC independent schools must manage when using online learning environments and Web 2.0 tools. The necessary information formed the basis for the teacher information documents in The Privacy Compass- learn the tool, know the risks. Once teachers can clearly articulate the risks, they are able to move on to review and adapt the parent documents. Teachers can communicate to parents/guardians why the tool is being used, how it should still be used, the reasonably foreseeable risks and how the risks will be managed. The teachers are also prepared to offer alternative activities for the students whose parents/guardians choose to withhold consent.

Secondly, I looked at what type of electronic performance support system (EPSS) might be built to help teachers in a British Columbian independent school use learning management systems and Web 2.0 tools in accordance with the Protection of Information and Privacy Act (PIPA, SBC 2003, C-63). I believe that The Privacy Compass addresses concerns that would be found when examining LMSs and Web 2.0 tools through a PIPA (SBC 2003, C-63) lens. While initially I intended to address PIPA (SBC 2003, C-63) and FIPPA (RSBC 1996, C-165) concerns with The Privacy Compass, I believe the current design of The Privacy Compass would also allow for other countries to adapt the work to their own legislative and policy requirements. This is supported by the provision of the documentation as editable Word documents as well as the easy to print PDF versions. Ideally, the eSafety incident response form (adapted by J. Hengstler, 2013, from work done by Kent County Council, UK) provided in The Privacy Compass is meant to be used along with the tool documentation to provide a protocol to follow in case student or



teacher safety has been compromised. It will give a uniform way for the school, teacher, student and parent/guardian to deal with particular situations that can arise when using LMSs or Web 2.0 tools.

Ultimately, although a lot of the literature reviewed and legislation referred to in this paper concerns Canadian and specifically British Columbia legislation (PIPA SBC 2003, C-63; FIPPA RSBC 1996, C-165), the EPSS tool developed for this project could be utilized in many other places. The Privacy Compass is something to be used, added to, modified and shared globally to support increased teacher use and understanding of LMSs and Web 2.0 tools. In the end, The Privacy Compass seeks to increase awareness, allay fears, while supporting student privacy and safety by identifying and managing privacy risks.

## References

Banks, T. (2012). Cloud computing and the USA Patriot Act: Canadian implications. *Privacy and Data Security Law: Coverage and commentary on developments in data protection*.

Retrieved from <http://www.privacyanddatasecuritylaw.com/cloud-computing-and-the-usa-patriot-act-canadian-implications>

British Columbia Teachers' Federation (BCTF). (2014). Members' guide to the BC Teachers' Federation. Retrieved from

<https://www.bctf.ca/uploadedFiles/public/AboutUs/MembersGuide/guide.pdf>

boyd, d. (2014). Privacy: why do youth share so publicly? *It's complicated: the social lives of networked teens*. Yale University Press. retrieved from

<http://www.danah.org/books/ItsComplicated.pdf>

Canadian Charter of Rights and Freedoms, Constitution Act, Statutes of Canada (1982, C-11).

Retrieved from <http://laws-lois.justice.gc.ca/eng/const/page-15.html>

Canadian Internet Policy and Public Interest Clinic (CIPPIC). (2004). The USA Patriot Act and its effect on the privacy of B.C. citizen's personal information in the context of government outsourcing of data administration. *British Columbia Privacy Commissioner*. Ottawa, ON.

Retrieved from

<https://www.cippic.ca/sites/default/files/privacy/USAPatriotAct%20Submission.pdf>

CBC News (2014). Clayton Heights students' marks accidentally mass emailed. Retrieved from:

<http://www.cbc.ca/m/touch/canada/britishcolumbia/story/1.2685735>

Clement, A., & Obar, J. (2014) Keeping internet users in the know or in the dark: Data privacy transparency of Canadian internet service providers. IXmaps.ca & New Transparency Projects.

Dropbox (n.d) Is there a limit or maximum to how big my files can be? Retrieved from:

<https://www.dropbox.com/help/5>

Electronic Transactions Act (ELA), Statutes of British Columbia (2001, C-10). Retrieved from

[http://www.bclaws.ca/civix/document/id/complete/statreg/01010\\_01](http://www.bclaws.ca/civix/document/id/complete/statreg/01010_01)

Ferriter, W. (2011) Digitally speaking/positive digital footprints. *The Transition Years* (vol. 68, pages 92-93). Retrieved from <http://www.ascd.org/publications/educational-leadership/apr11/vol68/num07/Positive-Digital-Footprints.aspx>

Freedom of Information Protection of Privacy Act (FIPPA), Revised Statutes of British Columbia (1996, C-165). Retrieved from [http://www.bclaws.ca/civix/document/LOC/complete/statreg/--%20F%20--/Freedom%20of%20Information%20and%20Protection%20of%20Privacy%20Act%20\[RSBC%201996\]%20c.%20165/00\\_Act/96165\\_01.xml](http://www.bclaws.ca/civix/document/LOC/complete/statreg/--%20F%20--/Freedom%20of%20Information%20and%20Protection%20of%20Privacy%20Act%20[RSBC%201996]%20c.%20165/00_Act/96165_01.xml)

Hengstler, J. (2014). The Compliance Continuum: FIPPA & BC Public Educators' Use of Social Media & the Cloud. Retrieved from [https://www.dropbox.com/s/ridcqq14a7k9543/Compliance\\_Continuum\\_5\\_06\\_14-1.pdf](https://www.dropbox.com/s/ridcqq14a7k9543/Compliance_Continuum_5_06_14-1.pdf)

Hengstler, J. (2014). A K-12 Primer for British Columbia Teachers Posting Students' Work Online. Retrieved from <http://jhengstler.wordpress.com/2013/05/17/a-k-12-primer-for-british-columbia-teachers-posting-students-work-online/>

Hengstler, J. (2014). Raising techno-responsible kids: Story 2. Retrieved from: <http://jhengstler.wordpress.com/2014/02/27/raising-techno-responsible-kids-story-2/>

Hengstler, J. (2011). Managing digital footprints: Ostriches v. eagles. In S. Hirtz & K. Kelly (Eds.), *Education for a digital world 2.0* (2nd ed.) (Vol. 1, Part One: Emerging technologies and practices). Open School/Crown Publications: Queen's Printer for British Columbia, Canada. Retrieved from [http://www.viu.ca/education/faculty\\_publications/hengstler/EducationforDigitalWorld2.0\\_1\\_jh89.pdf](http://www.viu.ca/education/faculty_publications/hengstler/EducationforDigitalWorld2.0_1_jh89.pdf)

Hengstler, J., Krivel-Zacks, G., & Kroeker, E. (2014). Duty to report: Case study, questions & analysis. *Adminfo* (June 2014) . Retrieved from <http://bit.ly/1lz8sNL>

Instructure (2014). Instructure paid canvas privacy policy. Retrieved from <http://www.instructure.com/policies/privacy-policy-instructure>

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Kerr, I., Barrigar, J., Burkell, J., & Black, K. (2006). Soft surveillance, hard consent. *Personally Yours*, vol. 6. Retrieved from [http://iankerr.ca/wp-content/uploads/2011/08/soft\\_surveillance\\_hard\\_consent.pdf](http://iankerr.ca/wp-content/uploads/2011/08/soft_surveillance_hard_consent.pdf)

Kerr, I., Barrigar, J., & Burkell, J. (2006). Let's not get psyched out of privacy: Reflections on withdrawing consent to the collections, use and disclosure of personal information. *Canadian Business Law Journal*.

Klassen, V. (2011) Privacy and cloud-based educational technology in British Columbia. Vancouver BC: BC Campus. Retrieved from <http://www.bccampus.ca/files/2013/08/Background-Paper-Privacy-and-Ed-Tech.pdf>

Lemke, C., Coughlin, E., Garcia, L., Reifsneider, D., & Baas, J. (2009). *Leadership for web 2.0 in education: Promise and reality*. Culver City, CA: Metiri Group. Commissioned by CoSN through support from the John D. and Catherine T. MacArthur Foundation. Retrieved from [http://www.ena.com/wp-content/uploads/2010/11/3COSN\\_Web\\_2.0.pdf](http://www.ena.com/wp-content/uploads/2010/11/3COSN_Web_2.0.pdf)

Light, D. & Polin D. (2010). Integrating web 2.0 tools into the classroom: Changing the culture of learning. EDC Center for Children and Technology. New York, NY. Retrieved from: <http://cct.edc.org/sites/cct.edc.org/files/publications/Integrating%20Web2.0.PDF>

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). *Digital footprints: Online identity management and search in the age of transparency*. PEW Internet & American Life Project. Retrieved from: [http://www.pewinternet.org/~media/Files/Reports/2007/PIP\\_Digital\\_Footprints.pdf.pdf](http://www.pewinternet.org/~media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf)

Maeroff, G. (2003) *A classroom of one: How online learning is changing our schools and colleges*. Palgrave MacMillan: New York, N.Y.

Ministry of Education Teacher Regulation Branch (2013). Independent school teacher conduct & competence standards. Retrieved from: [http://www.bcteacherregulation.ca/documents/AboutUs/Standards/edu\\_stds\\_IS.pdf](http://www.bcteacherregulation.ca/documents/AboutUs/Standards/edu_stds_IS.pdf)

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Mutual Legal Assistance in Criminal Matters Act (MLAT), Revised Statutes of Canada (1985, c30, 4<sup>th</sup> supp). Retrieved from <http://laws-lois.justice.gc.ca/eng/acts/M-13.6/page-1.html>

National Strategy for Trusted Identities in Cyberspace. (n.d.) Appendix A: Fair information practice principles (FIPPs). Retrieved from: <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>

Office of the Information and Privacy Commissioner for British Columbia (OIPC BC). (2012a). *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations. Chapter 63*. Victoria, BC

Office of the Information and Privacy Commissioner for British Columbia (OIPC BC). (2012b). *Privacy Breaches: Tools and Resources*. Victoria, BC.

Office of the Information and Privacy Commissioner of Canada (OIPC Canada). (2012a). *Guidelines for Online Consent*. Retrieved from [http://www.priv.gc.ca/information/pub/ar-vr/pipeda\\_sa\\_tool\\_200807\\_e.pdf](http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf)

Office of the Information and Privacy Commissioner of Canada (OIPC Canada). (2012b). *Archived - PIPEDA Self-Assessment Tool*. Retrieved from [https://www.priv.gc.ca/information/pub/ar-vr/pipeda\\_sa\\_tool\\_200807\\_e.asp](https://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp)

Personal Information Protection Act (PIPA), Statutes of British Columbia (2003, C-63). Retrieved from [http://www.bclaws.ca/Recon/document/ID/freeside/00\\_03063\\_01](http://www.bclaws.ca/Recon/document/ID/freeside/00_03063_01)

Portal, P., Cooper, S., & Southwell, J. (2011). Privacy guide for faculty using 3rd party web technology (social media) in public post-secondary courses. Retrieved from <http://www.bccampus.ca/files/2013/08/PrivacyGuideforUsing3rdPartyWebTechnologyinPublicPost-SecondaryCoursesRevisedFeb2011.pdf>

Raybould, B. (1991). An EPSS case study: Prime computer. Handout given at the Electronic Performance Support Conference, Atlanta, GA, 1992.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Richardson, W. (2008). Footprints in the digital age. *Educational Leadership*, 66(3). Retrieved from [www.ascd.org/publications/educational-leadership/nov08/vol66/num03/Footprints-in-the-Digital-Age.aspx](http://www.ascd.org/publications/educational-leadership/nov08/vol66/num03/Footprints-in-the-Digital-Age.aspx)

Strichenberger, I. (2013). InBloom notification. *InBloom Landing Page*. Retrieved from: <https://www.inbloom.org/> (No longer a functional site by the completion of this document)

Unicef (n.d.) A Summary of the United Nations Convention on the Rights of the Child. Retrieved from [http://www.unicef.org/crc/files/Rights\\_overview.pdf](http://www.unicef.org/crc/files/Rights_overview.pdf)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. (US Public Law 107-56, October 26, 2001). Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>

Web 2.0 Teaching Tools (2009). Web 2.0 teaching tools: Motivate and engage students. Retrieved from <http://www.web2teachingtools.com/>

## Appendix

### Appendix A: Web 1.0, 2.0, 3.0: What's the Difference?

	Web 1.0	Web 2.0	Web 3.0
Meaning is...	Dictated	Socially constructed	Socially constructed & contextually reinvented
Technology is...	Confiscated at the classroom door	Chosen by the teacher and students to be integrated where possible	Everywhere
The classroom is composed of...	Digital refugees	Digital immigrants	Digital universe
Teaching is done...	Teacher to student	Teacher to student, student to student & student to teacher	Teacher to student, student to student & student to teacher
Schools are located...	In a building	In a building or online	Everywhere
Parents view school as...	Daycare	A place for them to learn too	A place for them to learn too
Teachers are...	Licensed professionals	Licensed professionals with an ability to adapt to new situations	Everybody, everywhere
Industry views graduates as...	Assembly line workers	Inquiry minded individuals in a knowledge community	As co-workers or entrepreneurs

This chart has been adapted from the one originally created by Dr. John Moravec, Ph.D: <http://www.mnasa.org/cms/lib6/MN07001305/Centricity/Domain/44/Moravec%20Spring%20Conference%202013.pdf> (Used under Creative Commons Licence)

# A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

## Appendix B: External Canvas Apps








## Appendix C: Hengstler Scaffolding Models

# Student Scaffolding?

(Hengstler Model)

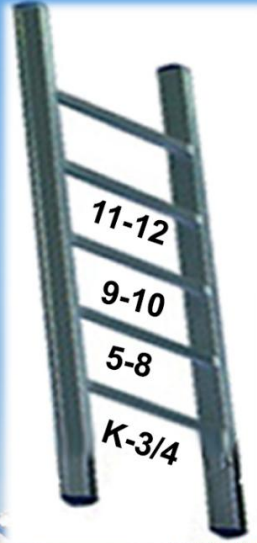
Observe & Learn:	Contained & Corrected:	Open Access:
 <small>Microsoft Clip Art</small>	 <small>Microsoft Clip Art</small>	 <small>"Kayaking on BC Lake" (vassilaparkstaff, 2005, CC Attribution License)</small>
<ul style="list-style-type: none"><li>• Watch knowledgeable adults in conscious articulated use</li><li>• Age-appropriate participation through adult</li></ul>	<ul style="list-style-type: none"><li>• Limited → increasing participation in contained systems</li><li>• Participants controlled &amp; known</li></ul>	<ul style="list-style-type: none"><li>• Skills embedded to adequately gauge &amp; manage risk</li><li>• Full participation</li></ul>

Copyright: Julia Hengstler; Reproduction & redistribution only by permission of the author

Hengstler, J. (2013). Student Scaffolding? Graphic used with permission of the author.

# Scaffolding Participation:

## Area & Connections (Hengstler Model)

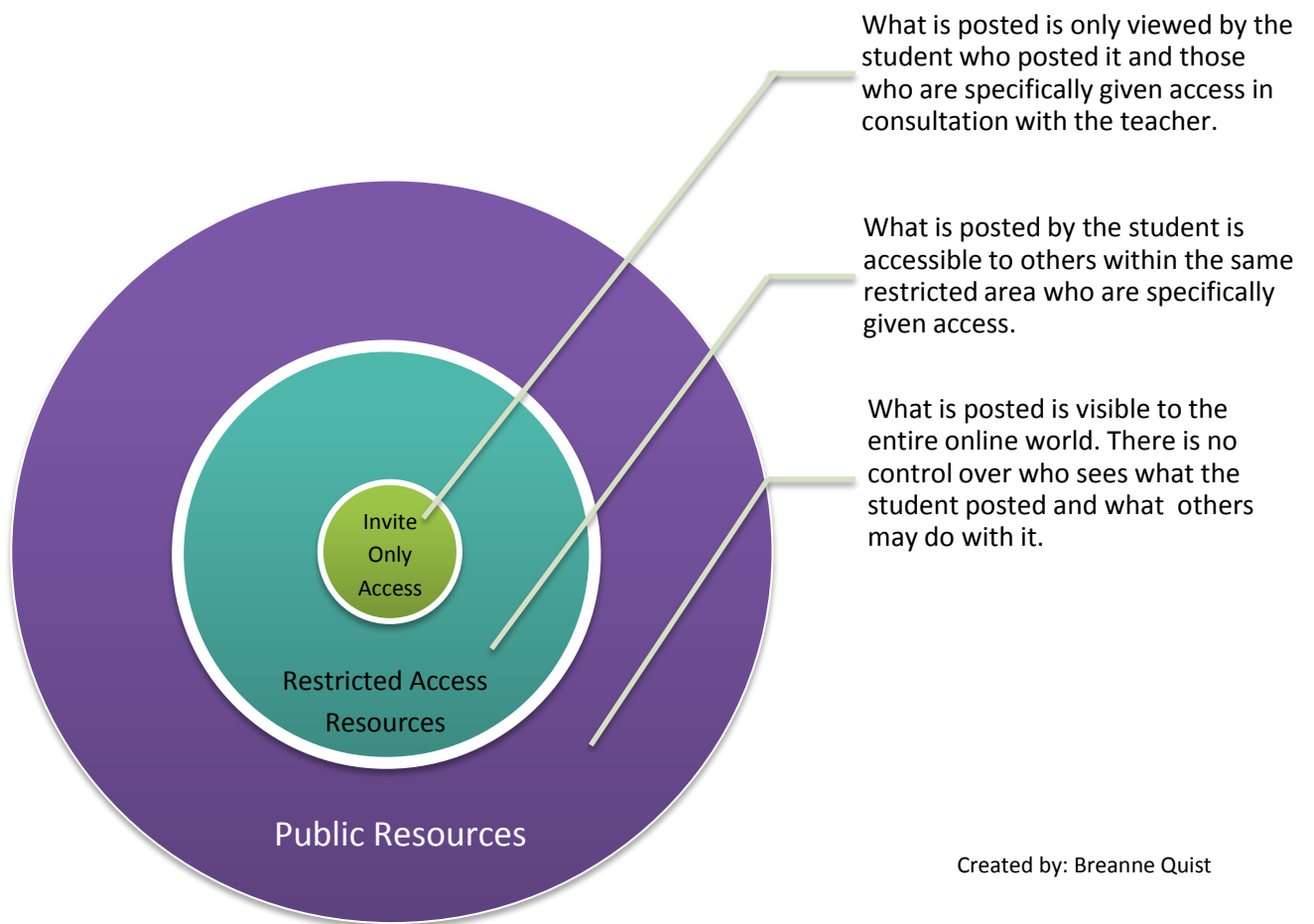


- 11-12: fenced systems; monitored use of open systems approved by school; no sharing of unauthorized personal/identifying data
- 9-10: fenced systems; limited participation in open systems; connections to be authorized by guidelines or teacher; no sharing of personal/identifying data
- 5-8: fenced systems; students network only with people known to them & within system; potential teacher or class accounts connect externally
- K-3/4: via teacher or 'class' accounts; closely monitored by teacher; limited external connections

Copyright: Julia Hengstler; Reproduction & redistribution only by permission of the author

Hengstler, J. (2013). Scaffolding Participation: Area & Connections. Graphic used with permission of the author.

## Appendix D: Sharing Circles: A Classification Framework for Online Tools



## Appendix E: Canvas Documents: Documentation Authored by B. Quist

### Teacher Document



**Overview:** Canvas by Instructure (more commonly known as Canvas) is a Learning Management System (LMS) that is available as a cloud based or server based LMS. Canvas provides an extensive and open API that they publish to the world, making it easy for third-party apps to plug into Canvas. Canvas has made an explicit commitment to their user's privacy; they conduct regular internal audits and even contract independent security specialists to perform and publish a public security audit. The interface is well laid out; there are many customization options and it is free!

### Privacy Points for Teachers

(from the Privacy Policy: <http://www.canvaslms.com/policies/privacy-policy> and Terms of Use: <http://www.canvaslms.com/policies/terms-of-use>)

- Users are solely responsible for ensuring that they and their school are compliant with all laws and regulations related to disclosing to Instructure the personal information of the students they invite to create accounts.
- When users enroll their students into a course it is assumed that they have provided the necessary notice and obtained the appropriate consents from the students, or from the parents of the student, if the student is younger than 18.
- As a part of the Instructor Account creation process, users are asked (a) whether they will be providing their course to students under 13, and (b) whether they are a teacher or administrator at a school (for example, a K-6 public elementary school). Users will only be permitted to provide a course to students under 13 if they are a teacher or administrator at a school.
- Users acknowledge that all content, including the Instructure Properties, are the sole responsibility of the party from whom such content originated. This means that users, and not Instructure, are entirely responsible for all content that they upload, post, email, transmit or otherwise make available through the Instructure Properties .
- Instructure, Inc. has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements and the TRUSTed Cloud Program Requirements including transparency, accountability and choice regarding the collection and use of their user's personal information. The TRUSTe program covers only information that is collected through these sites: <http://www.instructure.com>, <http://canvas.instructure.com>, <http://www.canvas.net> and the associated services. The TRUSTe Program does not cover

information that may be collected through mobile applications, or information collected offline.

- Instructure collects information from their users, such as first and last name, gender, email and mailing addresses, professional title, company name, and password when someone creates an account to log in to their network. They also may retain information on their user's behalf, such as files and messages that users store using their account. If a user provides them feedback or contacts them via email, they will collect the user's name and email address, as well as any other content included in the email. When users participate in one of their surveys, they may collect additional profile information. They also collect other types of personal information and demographic information that users provide to them voluntarily.
- Instructure offers users choices regarding the collection, use, and sharing of their personal information. When users receive newsletters or promotional communications from them, they may "opt-out" by following the unsubscribe instructions provided in emails they receive from them.
- Most web browsers are set to accept cookies by default. If a user prefers, they can typically remove and reject cookies from Canvas with their browser settings. If users remove or reject their cookies, it will affect how Canvas and their services work for them.
- "Flash Cookies" are used to store user preferences such as volume control or to display content based upon what they view on their websites to personalize the user's visit. Third party partners who provide certain features on their websites, such as videos, may place Flash cookies on the user's device. They may use Flash cookies to track user's web browsing activity and to display personalized advertising. Flash cookies are different from other cookies because of the amount of and type of data collected, and the way in which it is stored. Cookie management tools provided by browsers usually will not remove Flash cookies.
  - To learn more about Flash cookies, who has placed Flash cookies on your device, and how to manage privacy and storage settings for Flash cookies click here: [http://www.macromedia.com/support/documentation/en/flashplayer/help/settings\\_manager.html#117118](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html#117118).
- Canvas does not control the privacy practices of the third parties who place or track Flash cookies and their privacy policy does not cover their practices. Users should visit the privacy policies of companies who place Flash cookies to understand their practices.
- Canvas uses analytics services to help analyze how users use the Site and Apps. These services use cookies and scripts to collect and store information such as how users interact with their Apps, errors users encounter when using their apps, device identifiers, how often users visit the Site, what pages they visit, and what other sites they used prior to coming to the Site. Canvas uses the information they get from Google Analytics only

to improve their Site, Apps, and Services. Canvas does not tie the information gathered using third party analytics to your personally identifiable information.

- Please see the following links for more information about Google Analytics:  
[http://www.google.com/privacy\\_ads.html](http://www.google.com/privacy_ads.html), <http://www.google.com/privacy.html>,  
and <http://www.google.com/analytics/tos.html>.
- Canvas may share user's personal information with third party service providers for the sole purpose of providing the user with the services that they offer them through their website. For example, they may share data with service providers who host their websites or provide email services on their behalf.
- Instructure may disclose information about their users if they believe such disclosure is necessary to (a) comply with laws or to respond to lawful requests and legal process; or (b) protect or defend the rights, safety, or property of Instructure, users of the Services, or any person including to enforce our agreements, policies, and terms of use, or (c) in an emergency to protect the personal safety of any person.
- Canvas may share information about their users in connection with or during negotiation of any merger, financing, acquisition, bankruptcy, dissolution, transaction or proceeding involving sale, transfer, divestiture or disclosure of all or a portion of their business or assets to another company. In the event that information is shared in this manner, notice will be posted on their site.
- Users may change some of their personal information in their account by editing their profile within Canvas. Users may also request changes or deletions by emailing Canvas. They will respond to user's requests, when permitted by law, within 30 days. They will retain user's information for as long as their account is active or as needed to provide them services. They will retain and use user information as necessary to comply with their legal obligations, resolve disputes, and enforce our agreements. They may be unable to delete information that resides in their archives.
- Instructure may change their Privacy Policy and Terms of Service from time to time. If they make any changes to the Policies, they will change the "Last Updated" date on the affected documents. If such changes are material, a notice of the changes will be posted on the Canvas home screen along with the revised Privacy Policy, or Terms of Service prior to the change becoming effective. Visit their policy pages from time to time for the latest on their privacy practices.
- Instructure welcomes your comments or questions. You can email them at [privacy@instructure.com](mailto:privacy@instructure.com) or contact them at the following address or phone number:

Instructure, Inc.  
6330 S 3000 E, STE 700  
Salt Lake City, UT 84121  
(801) 869.5000

## **Parent Document**

### **What is Canvas?**

Canvas by Instructure (more commonly known as Canvas) is a Learning Management System (LMS) that is available as a cloud based or server based LMS. Canvas provides an extensive and open API that they publish to the world, making it easy for third-party apps to plug into Canvas. Canvas has made an explicit commitment to their user's privacy; they conduct regular internal audits and even contract independent security specialists to perform and publish a public security audit. The interface is well laid out and there are many customization options.

### **Why am I using Canvas?**

In an effort to bring our students together and connect with each other to create a sense of community, we will be using Canvas. Canvas allows your child to connect with other students in a password protected, invite only area where the teacher has full moderation abilities and can check on everything that is happening.

You child will be using Canvas to:

- access assignments
- upload completed assignments
- have discussions in the forum
- complete tests
- ask questions / email their teacher
- use external tools and websites when necessary to gain more understanding

### **Risks that could arise**

Because Canvas is hosted “in the cloud” it is important for parents to understand some key points:

- The cloud is everywhere. This means that you are able to access it from any device that is connected to the internet, you also need to be aware that others can also do the same so keeping your password private is essential.
- The cloud stores your information so that you don't have to. This means that there will be much more room on your device because once something is uploaded on to the cloud it will remain there and be accessible.

### **What's 'personal information'?**

“People have different standards of what they consider ‘personal’ information. Sharing over social media has done a fair bit to reset our expectation. Regardless of personal definition, if the information, data, or content could be used to identify you, it's ‘personal information’ – though professional or business contact information may be treated separately.” 1(Henglstler, 2013). A student's personal information could include: name, date of birth, address, telephone number,

email address, educational information, and anything that identifies an individual, including photographs. If any information, data or content could be used to identify you it is then qualified as “personal information”.

### **Why is BC so sensitive to privacy laws regarding data?**

“Shortly after the 9/11 attacks on the US in 2001, the American government enacted the United States Patriot Act that allowed the United States government to search private and public data housed on servers on United States soil. At the time, The British Columbia Medical Services Plan was hosting our provincial medical records in the United States. Unions in British Columbia expressed concern over the ability of the American government to search through British Columbian’s personal medical records and histories. Ultimately, the rule is: if you transfer or authorize the transfer of your personal information outside of Canada, that data is subject to the laws and practices of the country where it sits – be it the United States, China, or India. (Remember that minors, under the legal care of an adult, cannot authorize such a transfer.) Not all locations have similar notions about your right to privacy. Since cloud computing is a relatively new technology, the laws and best practices governing it are still changing and there is a need to stay current.”<sup>1</sup> (Hengstler, 2013)

### **Why is a consent form necessary?**

Various provinces in Canada – and other jurisdictions across the world – have enacted laws to protect personal privacy. In BC, the Personal Information Protection Act (PIPA) covers all independent schools. It is one of the most defined privacy protection frameworks in Canada. PIPA states that ‘private bodies’ such as independent schools have defined legal requirements for handling your personal information when it is within their ‘custody’ and ‘control’. Generally, private bodies must make sure that your personal information cannot be stored or accessed outside of Canada without your expressed permission – ‘consent’ (Note: there are certain expectations in the law like data covered by treaties, etc.). PIPA states that your consent must be in writing, state to whom your personal information may be disclosed, and how your information will be used. Also, if you post personal information about others, their permission must also be secured.

### **What if I don’t want to consent?**

You have the right as a parent/guardian to withhold consent to your child using Canvas. Alternate activities will be provided to students in the event that parents/caregivers choose to withhold consent and that selection of an alternate activity will not affect a student’s grade.

While no internet-based experience can ever be 100% risk-free, know that I will take every reasonable measure to manage expected risks.

<sup>[1]</sup> Julia Hengstler is the Educational Technologist with the Faculty of Education at Vancouver Island University & an Instructor in Educational Technology. Please visit this site for more background information about her: [http://www.viu.ca/education/faculty/profiles/hengstler\\_j.asp](http://www.viu.ca/education/faculty/profiles/hengstler_j.asp)

### **Informed Consent**

In an effort to bring our students together and connect with each other to create a sense of community, we will be using the learning management system (LMS) Canvas by Instructure. Canvas has made an explicit commitment to their user's privacy; they conduct regular internal audits and even contract independent security specialists to perform and publish a public security audit. Canvas allows your child to connect with other students in a password protected, "invite-only" area where the teacher has full moderation abilities and can check on everything that is happening.

Your child will be using Canvas to:

- access assignments
- upload completed assignments
- have discussions in the forum
- complete tests
- ask questions / email their teacher
- use external tools and websites when necessary to gain more understanding

Canvas will be used for some or all courses that your child is enrolled in this year and it is expected that s/he use it properly following the guidelines below.

1. Keep your real name, address, or email / phone number private. Basically, anything that can identify you (or anyone else) and where to find you (or them) should be kept private as those who need to know the information (the teacher and peers in your class) will already know it.
2. Everything that is posted online has a 'digital footprint' this means, once something is posted online, it is online for good. Put thought into what you are posting and make sure it is acceptable.
3. At all times treat other people with respect and dignity. We are an inclusive class. If something a classmate posts, causes you concern, contact the teacher immediately but do not post a negative comment back to them.
4. You must have permission to post any videos or pictures that you have taken which contain other people (or yourself). You must obtain the consent of the other person (who is shown in the picture or video) and a parent's consent if the person is 13 years of age or younger.
5. Do not give your password to anyone. If you give out your password, things may be posted on your behalf that you do not approve of.
6. If you believe your account has been compromised or hacked, report this immediately to your parent and the teacher.

Please keep page one for future reference and complete page 2 to be returned to me for my records. Thank you.

**Teacher Name**

**Contact Information**



## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Please choose one of the following, (Note: if you feel that you do not have enough information to make an informed decision, please contact me to discuss further):

☐ My child and I agree to the rules for using Canvas and my child will be making his or her own account. My child's preferred email to use is: \_\_\_\_\_

☐ My child and I agree to the rules for using Canvas but I do not feel comfortable having my child using his or her own account, I prefer my child to use my email to register for an account. My email address is: \_\_\_\_\_

☐ I do not agree to the use of Canvas and I am aware it may result in a course withdrawal.

We understand the privacy risks and management strategies as they have been shared with us.

\_\_\_\_\_  
Parent/Guardian Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Student Signature

\_\_\_\_\_  
Date

Received by teacher on: \_\_\_\_\_

Running Footer on the document: Changes may occur; this document is current as of terms of service on July 29, 2014. Check with your own school to make sure it meets your school's privacy policy. Review completed by Breanne Quist.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

### Metadata

Tool / Resource Name: Canvas

URL: <https://canvas.instructure.com/login>

LMS or Web 2.0 Tool: LMS

Location of Reviewer: British Columbia, Canada

Reviewer affiliation:

Public School	
Independent School	X
Public Organization	
Private Organization	
Other	

Enrollment Requirements:

First name	X
Last name	X
User name	X
Email address	X
Street address	
Postal code	
Phone number	
School / Organization	
Age	
Password	X

Required user information that is displayed

User name	X
Email	X
Name	
Avatar	
Location	

Tool Category:

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Instructional	X
Informational	X
Presentation	
Storage	X
Game	
Other	

Grade level:

Primary (K-3)	
Intermediate (4-6)	
Middle School (7-9)	X
High School (10-12)	X

Subjects / Courses:

Math	X
English	X
Science	X
Social Studies	X
PE	X
Health and Careers	X
Fine Arts	X
Applied Skills	X

General information

Open / Closed	Closed
Server location	US. Can be stored locally for a fee.
Tool privacy policy URL	<a href="http://www.canvaslms.com/policies/privacy-policy">http://www.canvaslms.com/policies/privacy-policy</a> Last updated Feb 28, 2014
Tool terms of service URL	<a href="http://www.canvaslms.com/policies/terms-of-use-fft">http://www.canvaslms.com/policies/terms-of-use-fft</a> Last updated Feb 28, 2014
Minimum age requirement	13
iOS app	X

## **Appendix F: Kidblog Documents: Adapted by B. Quist from Documentation Provided by T. Cameron**

### **Teacher Documents**



**Overview:** Kidblog is designed for K-12 teachers who want to provide each student with an individual blog. Students publish posts and participate in academic discussions within a secure classroom blogging community. Teachers maintain complete control over student blogs and user accounts. For further information please visit: <http://kidblog.org/why-kidblog/>

### **Privacy Points for Teachers**

(Adapted from the Privacy Policy: <http://kidblog.org/home/privacy-policy/> and Terms of Service: <http://kidblog.org/home/terms-of-service/>)

- Only adults may register to use the Website with full administrative privileges. Use of Kidblog by anyone under age 18 must be done under adult supervision. Kidblog is intended for administrative use by teachers, students, librarians, administrators, parents, and anyone else involved in education as a teaching tool. The adult that registers (or maintaining/moderating) a “class account” (and subsequently creating and/or adding students/users to the account) (a “Member”) is responsible for obtaining permission of a parent or guardian of any members under 13 who use the Website through class account. Kidblog does not intend that anyone under age 18 register as a Member. If a user is under age 18 and register as a Member, they are violating the terms.
- All Members of Kidblog shall receive a password and an account. Members are entirely responsible for any and all activities which occur under their account whether authorized or not authorized. The Member agrees to notify Kidblog of any unauthorized use of the Member’s account or any other breach of security known to the Member. The Member’s right to use Kidblog is personal to the Member. The Member agrees not to resell or make any commercial use of the Website without the express written consent of Kidblog.
- Kidblog’s website may include links to other websites on the internet that are owned and operated by third parties. members acknowledge that Kidblog is not responsible for the availability of, or the content located on or through, any third-party website. Members should contact the site administrator or webmaster for those third-party websites if they have any concerns regarding such links or the content located on such sites. Kidblog has no control over any third party websites and they encourage their Members and Users to be careful when visiting other websites.
- Kidblog is operated and provided from their offices in the State of Minnesota. As such, their terms of service are governed by the laws of the State of Minnesota. No conflict of laws provisions of any jurisdiction will apply to their terms. They make no representation

that their website or other services are appropriate, legal or available for use in other legal jurisdictions.

- Kidblog respects the intellectual property rights of others, and requires that the people who use their website do the same. It is their policy to respond promptly to any claims that intellectual property rights are being violated via Kidblog. If a member believes that a work that they own or have rights to has been copied and made accessible on kidblog.org in violation of their rights, they may notify Kidblog by providing their copyright agent with the relevant information in writing.
- Kidblog retains the right, at their sole discretion, to refuse service to anyone, for any reason, at any time. Such termination may be effected without prior notice in Kidblog's sole business discretion. Kidblog shall not be liable to any User or other party for any such termination. Kidblog reserves the right to delete or save a User's content upon a termination in its sole discretion.
- By using Kidblog members agree to the collection and use of information in the manner described in their privacy policy. If they make material changes to their policy, they will notify the members via kidblog.org, by email, by means of a notice the next time the member logs in to Kidblog, or by means of a notice on their homepage or main page.
- To make their privacy policy easy to find, they have placed a link to it at the bottom of each page of their website.
- Members are responsible for reviewing <http://kidblog.org/home/privacy-policy/> periodically for any modification to their privacy policy. Any access or use of Kidblog by a member after notice of revisions or additions to their privacy policy shall constitute and be deemed to be their agreement to such revisions or additions.
- Members provide personal information to Kidblog when they register to use the services and when they request information from Kidblog. The personal information Kidblog collects from users registering for the service is:
  - Display Name (this name is displayed to other users)
  - Username
  - Password
  - Email Address
  - Class Name (a "class" is a group of users defined by user registering for the Service)
- The user registering for Kidblog can also define the members of a class and grant usage user access to the Service by issuing usernames and passwords to additional users.
- In addition to the personal information members supply, Kidblog may automatically collect non-personal information to evaluate how the Service is used. They collect non-personal data to make their services work better for users. The technologies they use to

gather this non-personal information may include IP addresses, web browser cookies, clear gifs, browser detection, and weblog information.

- Kidblog collects personally identifiable information from registered users so that they may have secure access to the website. Users are responsible for safeguarding their own usernames, passwords, and email addresses. If a user's registration or account information security has been breached, the user can contact Kidblog for assistance.
- Members may modify their browser preferences to accept all cookies, be notified when a cookie is set, or reject all cookies. If a member modifies their browser to reject certain or all cookies, they may not be able to use certain features of Kidblog.
- Access to a member's personally identifiable information and all data they store on kidblog.org is limited to authorized Kidblog staff and is restricted by password protection mechanisms. Although total security does not exist on the internet, Kidblog will make commercially reasonable efforts to safeguard the information that their members submit.
- Kidblog.org is not intended for use by unsupervised children. Only adults are authorized to register and create accounts with administrative privileges. Only accounts with administrative privileges may grant children access to the website.
- Kidblog will not knowingly collect any personally identifiable information from children under the age of 13.
- Kidblog reserves the right to disclose a members personally identifiable information as required by law and when they believe that disclosure is necessary to protect their rights and/or comply with a judicial proceeding, court order, or legal process served on us.
- Kidblog.org does not currently contain links to other websites. Kidblog is not responsible for the privacy practices of any other websites. They encourage their members to be aware when they leave the website, and to read the privacy statements of each website that collects personally identifiable information.

Kidblog, Inc.  
2869 W 71 1/2 Street  
Richfield, MN 55423  
Phone: 612-703-7405.

## **Parent Documents**

Dear parents/guardians,

I wanted to provide you with further information regarding Kidblog to aid in your decision to give consent for your child to use Kidblog. Please read the following and if possible visit the links provided.

### **What is Kidblog?**

Kidblog is designed for K-12 teachers who want to provide each student with an individual blog. Students publish posts and participate in academic discussions within a secure classroom blogging community. Teachers maintain complete control over student blogs and user accounts.

For further information please visit: <http://kidblog.org/why-kidblog/>

What is blogging? A blog is a website for which an individual or a group frequently generates text, photographs, video or audio files, and/or links, typically (but not always) on a daily basis.

The term is a shortened form of weblog. Authoring a blog, maintaining a blog or adding an article to an existing blog is called "blogging". Individual articles on a blog are called "blog posts," "posts," or "entries". The person who posts these entries is called a

"blogger." (Wikipedia) Here is an animated explanation and review of safety that students will review at school: <http://www.brainpop.com/english/writing/blogs/>

### **Why am I using Kidblog?**

Kidblog provides teachers with the tools to help students safely navigate the digital – and increasingly social – online landscape.

Kidblog allows students to exercise digital citizenship within a secure, private classroom blogging space. Kidblog's security features put safety first:

- Teachers have administrative control over all student blogs and student accounts
- Students' blogs are private by default, viewable only classmates and the teacher.
- Teachers can add password-protected parent and guest accounts to the community at their discretion.
- Comment privacy settings block unsolicited comments from outside sources.
- Kidblog is fully Children's Online Privacy and Protection Act ("COPPA") compliant and does not require any personal information from students.

### **Risks that could arise**

While no internet-based experience can ever be 100% risk-free, know that I will take every reasonable measure to manage expected risks.

Please refer to Kidblog's Privacy Policy for further information: Kidblog agrees to treat your personally identifiable information in accordance with the terms of their current privacy policy which is available for review at: <http://kidblog.org/home/privacy-policy/>

The Privacy Policy will be reviewed and discussed with students prior to using Kidblog.

### **What's 'personal information'?**

“People have different standards of what they consider ‘personal’ information. Sharing over social media has done a fair bit to reset our expectation. Regardless of personal definition, if the information, data, or content could be used to identify you, it’s ‘personal information’ – though professional or business contact information may be treated separately.”<sup>1</sup>(Henglstler, 2013). A student’s personal information could include: name, date of birth, address, telephone number, email address, educational information, and anything that identifies an individual, including photographs. If any information, data or content could be used to identify you it is then qualified as “personal information”.

### **Why is BC so sensitive to privacy laws regarding data?**

“Shortly after the 9/11 attacks on the US in 2001, the American government enacted the United States Patriot Act that allowed the United States government to search private and public data housed on servers on United States soil. At the time, The British Columbia Medical Services Plan was hosting our provincial medical records in the United States. Unions in British Columbia expressed concern over the ability of the American government to search through British Columbian’s personal medical records and histories. Ultimately, the rule is: if you transfer or authorize the transfer of your personal information outside of Canada, that data is subject to the laws and practices of the country where it sits – be it the United States, China, or India. (Remember that minors, under the legal care of an adult, cannot authorize such a transfer.) Not all locations have similar notions about your right to privacy. Since cloud computing is a relatively new technology, the laws and best practices governing it are still changing and there is a need to stay current.”<sup>1</sup>(Hengstler, 2013)

### **Why is a consent form necessary?**

Various provinces in Canada – and other jurisdictions across the world – have enacted laws to protect personal privacy. In BC, the Personal Information Protection Act (PIPA) covers all independent schools. It is one of the most defined privacy protection frameworks in Canada. PIPA states that ‘private bodies’ such as independent schools have defined legal requirements for handling your personal information when it is within their ‘custody’ and ‘control’. Generally, private bodies must make sure that your personal information cannot be stored or accessed outside of Canada without your expressed permission – ‘consent’ (Note: there are certain expectations in the law like data covered by treaties, etc.). PIPA states that your consent must be in writing, state to whom your personal information may be disclosed, and how your information will be used. Also, if you post personal information about others, their permission must also be secured.

### **What if I don’t want to consent?**

You have the right as a parent/guardian to withhold consent to your child using Kidblog. Alternate activities will be provided to students in the event that parents/caregivers choose to withhold consent and that selection of an alternate activity will not affect a student’s grade.

While no internet-based experience can ever be 100% risk-free, know that I will take every reasonable measure to manage expected risks.



**Further information:**

**Kidblog Home:** <http://kidblog.org/home/>

**Kidblog Terms of Service:** <http://kidblog.org/home/terms-of-service/>

<sup>[1]</sup> Julia Hengstler is the Educational Technologist with the Faculty of Education at Vancouver Island University & an Instructor in Educational Technology. Please visit this site for more background information about her: [http://www.viu.ca/education/faculty/profiles/hengstler\\_j.asp](http://www.viu.ca/education/faculty/profiles/hengstler_j.asp)

**Informed Consent**

Kidblog is an Internet based blog site that houses its servers on United States soil. It is a “Fenced” blog site with a limited, bounded set of users. The only users that can participate are the teacher and the students. Kidblog is designed for K-12 teachers who want to provide each student with an individual blog. Students publish posts and participate in academic discussions within a secure classroom blogging community. Teachers maintain complete control over student blogs and user accounts. Students will be assigned a username and password to log into Kidblog.

What is blogging? A blog is a website for which an individual or a group frequently generates text, photographs, video or audio files, and/or links, typically (but not always) on a daily basis. The term is a shortened form of weblog. Authoring a blog, maintaining a blog or adding an article to an existing blog is called "blogging". Individual articles on a blog are called "blog posts," "posts," or "entries". The person who posts these entries is called a "blogger." (Wikipedia) Here is an animated explanation and review of safety that students will review at school (<http://www.brainpop.com/english/writing/blogs/>)

Blogging has become a great way to get students reading and writing. Our blog is going to be used for group discussions and the sharing of learning, ideas, information and resources that focus on school related topics. It is an opportunity for students and teachers to collaborate on assignments. Each child will have a blog page to design and add entries. This page will only be visible to the teacher and students in our class. Students will be shown log on procedures and discuss acceptable use in our computer classes. When writing blog posts students will be responding to questions posed by the teacher and peers. When responding to student blogs it is expected that students respond to blog posts with positive and supportive comments. Blogging provides us with a way to extend our thinking and connect our ideas with each other and students. Students that post inappropriate or negative comments will not be allowed to participate. This will help students learn to be good digital citizens.

Kidblog Terms of Service (<http://kidblog.org/home/terms-of-service/>)

### **ACCEPTABLE USE**

The purpose of the use of Kidblog is to facilitate communications for education by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user the use of your account must be in support of and consistent with the educational objectives. Transmission of any material in violation of any Canadian or International regulation is prohibited. This includes, but is not limited to, copyright material, threatening or obscene material, illegal material or material protected by trade secret. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is prohibited.

The School reserves the right to review any material on user accounts and to monitor file server space in order to make determinations on whether specific uses of the network are inappropriate.

### **SECURITY**

- Security on any computer system is a high priority, especially when the system involves many users. A user must never allow others to use his/her password. Users should also protect their passwords to ensure system security and their own privileges and ability to continue use of the system.
- If you feel you can identify a security problem on Kidblog you must notify a system administrator. Do not demonstrate the problem to other users.
- Attempts to log on to Kidblog as a teacher/administrator will result in cancellation of user privileges.
- The teacher/site administrator will deny any user identified as a security risk for having a history of problems with other computer systems to Kidblog.
- ***Kidblog's Privacy Policy:*** <http://kidblog.org/home/privacy-policy/>

### **ENCOUNTER OF CONTROVERSIAL MATERIAL**

Users may encounter material, which is controversial, and which users, parents, teachers or administrators may consider inappropriate or offensive. However, on the Internet it is impossible to control the content of data and a user may discover controversial materials. It is the user's responsibility not to initiate access to such material. The School shall not be held liable for any decision to restrict or regulate access to Internet materials.

## **ETIQUETTE**

All communications and information posted on Kidblog via the Internet should be assumed to be the private property of those who posted it. All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

A. All users are expected to behave as they would in any other environment where they represent their school. It is important that users conduct themselves in a responsible, ethical, and polite manner in accordance with the standards of propriety in the District.

B. Users may not:

- use abusive, vulgar, profane, obscene, harassing, or other inappropriate language;”
- criticize the spelling, writing or keyboarding of others;
- re-post personal electronic mail received to public forums without the permission of the author.
- share password(s) with others;
- distribute or use anyone else’s account name and password;
- reveal your personal address or phone numbers of students or colleagues.
- transmit or post threatening, abusive, obscene or harassing material

Please keep page 1-3 for your records and complete page 4 to be sent back to me for my records.  
Thank you.

**Teacher Name**

**Contact Information**

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

I, \_\_\_\_\_, agree that my child, \_\_\_\_\_, will adhere to the expectations, terms and conditions attached as **“Specific Expectations, Terms and Conditions of Students Using Technology”** when using the above-named technology for a class assignment. I realize that if my child does not abide by these terms and conditions they may expose theirs or other people’s personal information to unauthorized third parties, leading to an invasion of their or other people’s privacy.

I, \_\_\_\_\_, agree to the collection, use, disclosure and storage of my child, \_\_\_\_\_’s, personal information inside or outside of Canada while using the technology described above for the purposes of engaging in classroom activities. I am aware of, and understand the identifiable privacy risks as described above.

I, \_\_\_\_\_, **do not give consent for my child,** \_\_\_\_\_, to participate in any activities using Kidblog. I understand that my child will be given alternate assignments similar to those that use Kidblog.

We understand the privacy risks and management strategies as they have been shared with us.

\_\_\_\_\_  
Parent / Guardian Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Student Signature

\_\_\_\_\_  
Date

Received by teacher on: \_\_\_\_\_

Running footer on this document: Adapted from original document created by T. Cameron. Changes may occur; this document is current as of terms of service on Sept. 8, 2014. Check with your own school to make sure it meets your school’s privacy policy. Review completed by Breanne Quist.

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

### Metadata

**Tool / Resource Name:** KidBlog

**URL:** [www.kidblog.org](http://www.kidblog.org)

**LMS or Web 2.0 Tool:** Tool

**Location of Reviewer:**

British Columbia, Canada

**Reviewer affiliation:**

Public School	
Independent School	X
Public Organization	
Private Organization	
Other	

**Enrollment Requirements:**

First name	X
Last name	
User name	X
Email address	X
Country	
Street address	
Postal code	
Phone number	
School / Organization	X
Age	
Birth date	
Password	X
Gender	

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Required user information that is displayed

User name	
Email	
Name	X
Avatar	
Location	

Tool Category:

Instructional	X
Informational	X
Presentation	X
Storage	
Game	
Other	

Grade level:

Primary (K-3)	X
Intermediate (4-6)	X
Middle School (7-9)	X
High School (10-12)	X

Subjects / Courses:

Math	
English	X
Science	
Social Studies	X
PE	

## A Tool to Support Web 2.0 & LMS Integration with Respect to Privacy

Health and Careers	X
Fine Arts	
Applied Skills	X

### General information

Open / Closed	Closed
Server location	US.
Tool privacy policy URL	<a href="http://kidblog.org/home/privacy-policy/">http://kidblog.org/home/privacy-policy/</a> Last updated May 16, 2012
Tool terms of service URL	<a href="http://kidblog.org/home/terms-of-service/">http://kidblog.org/home/terms-of-service/</a> Last updated May 16, 2012
Minimum age requirement	N/A
iOS app	X
Android app	X

# Appendix G: Comparison Chart for the Privacy Compass Website

Tool Comparison Chart		Canvas	Edmodo	Kidblog	Mathseeds	Office 365	Pinterest	Reading Eggs	Reading Eggspress	Twiducate	Twitter	
Enrollment Requirements	First name				P			P	P			
	Last name			T	P			P	P	T		
	Username			T								
	Email address		O	T								
	Street address											
	Postal code											
	Country											
	Phone number											
	School / Organization name											
	Age				S			S	S			
	Gender											
	Group Code											
	Password											
Displayed User Information	Username											
	Email address											
	Name											
	Avatar	O	O				O			O	O	
	Location										O	
	Age											
Grade Level	Primary (K-3)											
	Intermediate (4-6)											
	Middle (7-9)											
	High School (10-12)											
Tool Category	Instructional											
	Informational											
	Presentation											
	Storage											
	Game											
	Other											
Subject / Courses	Math											
	English											
	Science											
	Social Studies											
	Physical Education											
	Health and Careers											
	Fine Arts											
	Applied Skills											
Additional Information	Open or Closed Tool	C	C	C	C	C	Op	C	C	C	Op	
	Server Location	US	US	US	US	US	US	US	US	CAN	US	
	Minimum Age	13	13	PC		PC	13				13	
	iOS App											
	Android App											
	Stores IP address											

Code Legend:

PC	Under 13 with parental consent
P	Parent
T	Teacher
S	Student
O	Optional
C	Closed
Op	Open

Created by: Breanne Quist

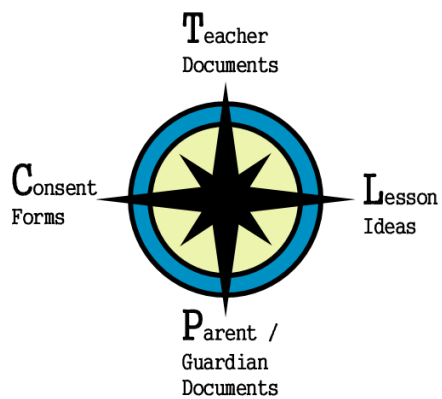


## Appendix H: Website Graphic Set

Mountain graphic that is embedded on the top of each page of the EPSS website



Compass Icon



All Documents Icon



Teacher Documents Icon



Parent Documents Icon



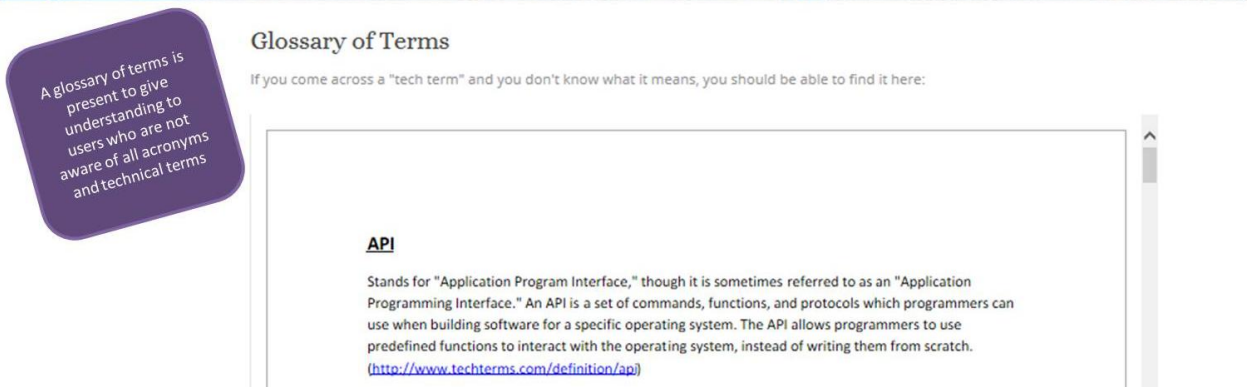
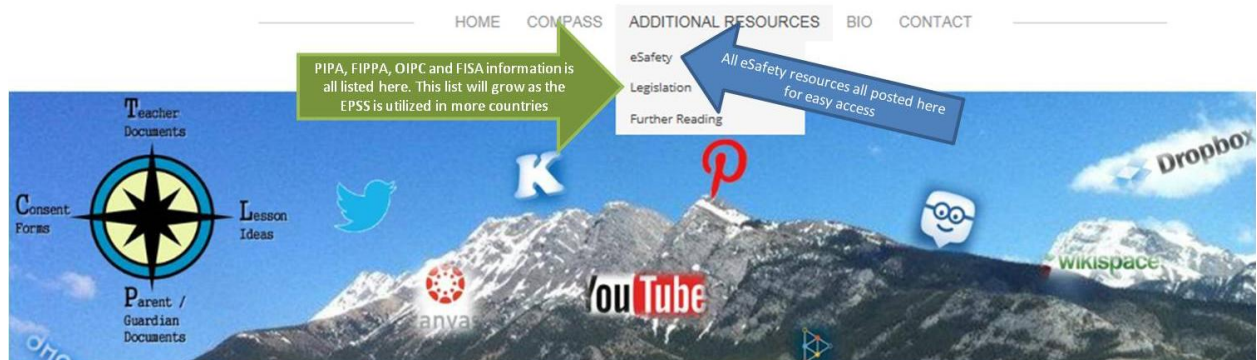
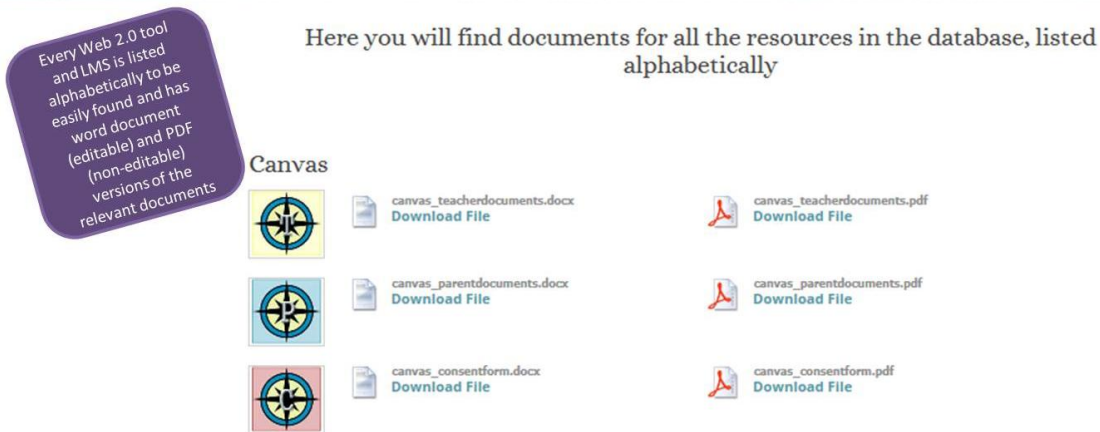
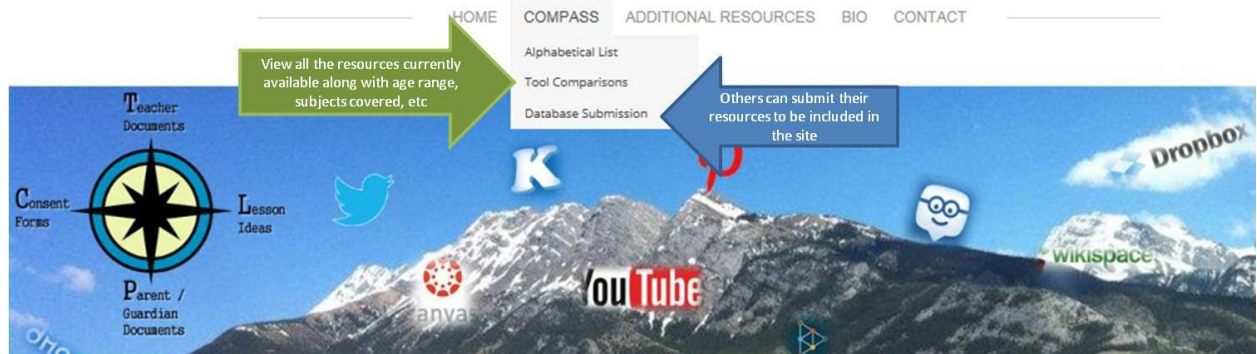
Consent Form Icon



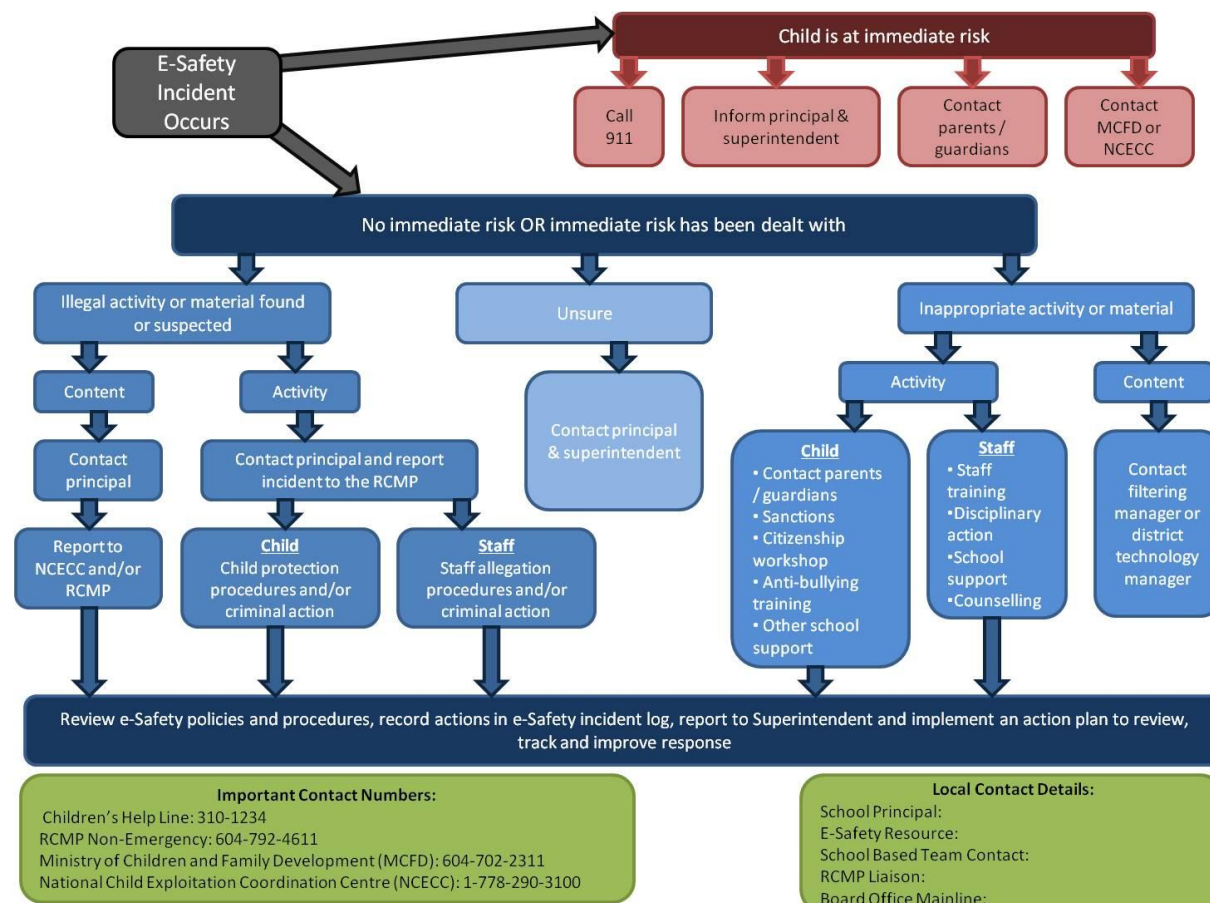
Lesson Plan Icons



## Appendix I: Screen Shots of Navigation for The Privacy Compass Website



## Appendix J: eSafety Incident Response Flow Chart



Adapted by J. Hengstler (2013) and modified by B. Quist (2014) with permission from Kent Country Council's Response to an incident of concern, 2012.

Modified by: Breanne Quist