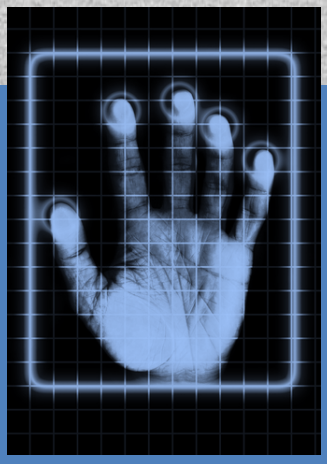
Adapted by J. Hengstler from © Cybrain, Dreamstime.com

A K-12 Primer for British Columbia Teachers Posting Students' Work Online

By Julia Hengstler, Educational Technologist & Instructor, Faculty of Education, Vancouver Island University, Nanaimo, British Columbia

An overview of key considerations that should be taken by British Columbia K-12 educators when using online sites or services to post student work or exemplars.



© Saniphoto, Dreamstime.com

5/19/2013

Contents

This primer is not a legal document and does not constitute legal advice.

Written 2013 by

Julia Hengstler

Educational Technologist & Instructor
Faculty of Education
Vancouver Island University
Nanaimo, British Columbia, Canada
Email: Julia.Hengstler@viu.ca
Twitter: @jhengstler

With special thanks to:

- **Liesel Knaack**, Director, Centre for Innovation and Excellence in Learning, Vancouver Island University, Nanaimo, British Columbia
- **Mark Hawkes**, e-Learning Coordinator, Learning Division, Ministry of Education, British Columbia
- **Dave Gregg**, e-Learning Officer, Learning Division, Ministry of Education, British Columbia
- **Larry Kuehn,** Director of Research and Technology, British Columbia Teachers' Federation
- **Rebecca Avery**, e-Safety Officer, Kent County Council, United Kingdom
- **John Phipps**, Field Experience Supervisor, Vancouver Island University, Nanaimo, British Columbia

Privacy-sensitivity to new technologies needs to occur at the beginning of the course development and delivery process, not in the middle when a privacy breach has occurred. If, after all cautions have been taken and a privacy breach still occurs and the individual harmed complains to the Information and Privacy Commissioner, then the instructor can show a history and record of due diligence…

From Privacy Guide for Faculty Using 3rd Party Web Technology (Social Media) in Public Post-Secondary Courses (Cooper, Southwell, & Portal, 2011, 14).

Source: Microsoft Clip Art

Introduction

Posting student content on the internet (whether in a 'secure' school district site or more open locations like Wordpress or Twitter) provides many learning opportunities for students. Educators may use these tools to connect students to others in a more global context. A kindergarten class may wish to share Tweets about today's weather with a class in China or Ecuador—working through a teacher's Twitter account. Students may develop their language and writing skills by sharing posts on a blog that asks for constructive feedback from other students or accomplished writers. A class might do a recorded webcam chat with a scientist in Antarctica studying global warming. Students may use Google documents to collaborate while writing a poetry anthology or collecting water quality data from streams across the community. A classroom teacher might want to use a website with a photo gallery of student artwork to connect with parents, guardians, and the local community. As educators, we have many reasons to use Web 2.0 and social media tools—but we must also be aware of the risks of their use and how to manage those risks. Risks can run from the commercial—such as exposure to advertising and spam—to the aggressive (e.g. cyberbullying) –to the sexual (e.g. pornographic)—to impersonation and identify theft. Many teachers and schools in British Columbia (BC) were well into using Web 2.0 and social media technologies before we knew much about the privacy risks and well before the current BC laws and regulations were being amended and discussed to protect our students and teachers.

While "BC's privacy laws are arguably the strongest in Canada" (Cooper, et al., 2011, 2), the inescapable reality is that many teachers and schools are using Web 2.0 and social media tools right now and may be in total ignorance of the new legislative requirements—especially those restricting the storage of personal information on servers external to Canada without explicit written consent, the need for teachers to be able to document evidence that parents/guardians and students were provided knowledge of and notice for the reasons the technologies are being used, and documenting the known risks. Some teachers may think that these rules are optional. They're not. If found in breach of the current privacy protection laws in BC, an individual teacher could be fined between $2,000.00 to $5,000.00 while a school could face fines as high as $50,000.00 In such a situation, educators, administrators, schools, and districts need to deal with the British Columbian policies and practices around K-12 use of these tools much like we deal with seismic upgrading: we look at the particular building, review the groups of people who will be using it, where it was built, when it was built, what codes were in place at that time, and if/how those codes have changed.

With the recent changes in BC laws and regulations, BC K-12 schools should be making reasonable and visible progress toward compliance with these new privacy requirements and should be working toward bringing their policies, procedures and practices into accordance with the BC privacy legislation. To extend this analogy, remember that just as any new construction would be expected to be in full compliance with earthquake standards for safety, this would mean any schools, districts and/or teachers starting out with Web 2.0 and social media tools should be expected to be in full

compliance with privacy legislation. Let's face it, teachers are excited when their lesson plans play out and their students do great things, but sometimes new teachers—and even seasoned veterans—can leap to posting student exemplars (created by minors) online without consideration of the laws and regulations that K-12 educators in British Columbia are required to follow.

This primer is a guide to some of the considerations that should be followed in the process of planning to post exemplars of minor students' work online from K-12 schools in British Columbia, Canada. The laws and regulations around privacy protection in British Columbia, especially with regard to use of third-party online sites and services have changed significantly in the past few years. Many schools are still trying to catch-up—to develop and implement the relevant policy and procedural changes. While the practice of posting and sharing minor students' work online has been around for a while, the rules and regulations haven't and we ALL need to do our 'upgrading' to comply.

Our ability to model these rules and regulations help form the social norms for technology use with parents, guardians, minor students and our communities and help lay the foundations for key components of digital citizenship.

Consideration 1: Copyright & Ownership

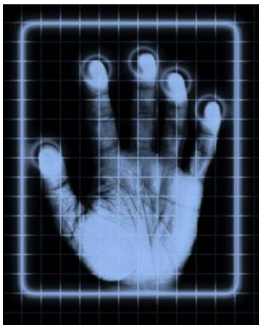
Key Question: Who does the content belong to?

For Canadians, there are no formalities required to copyright original work. The author is the immediate owner of the copyright in the original work, except in certain cases where he or she is under an employment contract.

Graduate Studies Office, University of Waterloo, 2013

Student work done by the student is the property of the student—full stop. The student maintains all rights to that intellectual property and by extension the rights for any minor British Columbian student (under 19 years of age) would be administered and overseen by a parent or guardian.

Recent changes in the Copyright Act have allowed for "Fair Dealing" of copyrighted content for Educational use. (See University of British Columbia, 2013, Copyright>>Copyright FAQ>>Basics 1.5 What is fair dealing and how does it relate to copyright? http://copyright.ubc.ca/faq/basics/#basics5). That said, when dealing with minors or when using more than 'excerpts' it is wise and prudent for a BC educator to request permission of the copyright holder through the parent or guardian.



© Saniphoto, Dreamstime.com

Consideration 2: Identifiability, Content & Risks

Key Question: What content will be posted and how will it be identified?

Personal information for minors should be considered to be any recorded information, including contact information that would uniquely identify the individual (e.g. name, age, gender, physical attributes, health/education/economic status) (Cooper, Southwell, & Portal, 2011). In the case of data posted on the internet, a student's first name, combined with class or teacher information can be sufficient to uniquely identify an individual. While all this data may not be on one page on a site or service, if it is distributed across a site or sites (service or services) that information can be easily brought together to identify the specific student.

Even if you remove identifiers such as a student's name from an assignment header (e.g. Reasons I Use Social Media by J. Hengstler→Reasons I Use Social Media by Student 4), or a photo, BC educators, administrators, schools and districts must make sure that the content posted does not provide any specific personal and identifiable information without express written consent of a minor student's parent or guardian. Moreover, educators must also be diligent and make sure that no indication of personal and identifiable information is 'hidden' in data like embedded code or in a file name, etc.

Adapted by J. Hengstler from © Cybrain, Dreamstime.com

Consideration 3: Storage Location & Risks

Key Question: Where will the content be posted & who will see it?

Work or exemplars of minor students can be posted in a variety of places. They could be placed on web sites that range across the spectrum from a password protected site run/moderated by a district to a Faculty of Education student's personal portfolio on a specific web site to a publicly accessible site like Flickr, Twitter, or Facebook. Each type of location carries its own risks—even the password protected district sites**. Remember that anything posted online is merely a cut-and-paste away from being public knowledge (e.g. a proud parent can take content from a password protected site—to which s/he might have rightful access—and paste it on a public Facebook account far beyond district control. In such cases, expectations of participation/access should be developed and communicated to all using and/or accessing the site/service.)**

Educators cannot assume because they are planning to post minor student content to a password protected server on a school district web site, that they are automatically 'covered'. Further, posting to cloud-based sites like Google, Facebook, and Weebly, have specific privacy law implications and due diligence requirements for BC educators under the Freedom of Information and Protection of Privacy Act, as well as the requirements for public bodies (including schools) as outlined by the BC Privacy Commissioner's Cloud Computing Guidelines for Public Bodies (February 2012).

For example, many cloud based services store data on servers outside of Canada. Google has "at least 12 significant" storage installations in the United States (Wikipedia, 2013). Apple recently built a large server farm for much of the iCloud data in Maiden, North Carolina, USA. All of these servers and their content would be subject to the 'foreign' regulations of the countries where they are physically located. This means that these Google and Apple servers would be subject to the US Patriot Act—and other US laws—which allow the US government to search through the data on those servers. (Similarly, data stored in other countries would be subject to the laws of those countries.) In order to think about posting minor student exemplars online, educators must be clear about *where* they would like to post the information. Educators need to consider the privacy of the web site or service along with its physical data storage location and the privacy risks, including any data that must be contributed if students are required to create accounts. When planning to post minor student work online in any venue, educators should evaluate the potential of using non-identifiable pseudonyms as a possible strategy to protect privacy. Educators should also provide an alternative assignment for those opting out of posting content online, especially if the activity or assignment is for a 'grade' or 'marks'.

Consideration 4: Explicit Informed Consent & Risks

Key Question: Has the parent/guardian received sufficient information and has *written* permission been obtained?

While some other Canadian provinces do recognize "emancipated minor status", in BC students under the age of 19 should be considered minors subject to parental oversight or guardianship. Since putting student content ANYWHERE on the internet exposes students to a certain level of privacy risk,

British Columbia educators wanting to post a minor student's content online (or have the minor student post his/her content online) have a legal, moral, and ethical responsibility to obtain written informed consent of the minor student's legal parent or guardian.

Cooper, Southwell, & Portal (2011) defined "informed consent" and the attendant "notice" and "knowledge" as follows:

Informed Consent

The principle of seeking the individual's permission for, and securing his or her agreement to, the collection, access, use, disclosure or storage of the individual's personal information by providing the individual with sufficient notice and knowledge of the reason for, and the circumstances and implications surrounding, the proposed collection, use or disclosure. Informed consent is typically requested and provided in written form.

Notice

Verbal or written advisory provided to an individual stating that his or her personal information is required for a particular purpose and may or will be collected, accessed, used, disclosed or stored in a particular way, by a particular entity, in a particular place, at or for a particular time. *The written form is most preferred and defensible.*

Knowledge

> Verbal or written advisory provided to an individual that, in addition to basic notification, provides the individual with additional important and relevant details about the purpose, circumstances, consequences and implications surrounding the stated collection, access, use, disclosure or storage of the individual's personal information. *The written form is most preferred and defensible*. (Portal et al., 2011, Appendix A, ii)

To obtain written and informed consent, the parent/guardian must be aware of the purpose for sharing the data, where it will be shared and with whom, types of data that will need to be shared, including whether students are required to have their own accounts requiring specified personal information (e.g., will students be expected to set up an account on the public Prezi site to post their presentations or will the content be posted through a teacher's account?). The parent/guardian must also be adequately informed of the risks involved. For example, if students need to create an individual account for a service or website, what is the personal information that will be collected when creating that account, who will be able to access that personal information, and what will it mean to the students' privacy. This presupposes that the educator understands these items him/herself and can explain them in understandable terms. In cases where English (or French in the case of French Immersion schools/programs) is not the first language of parents/guardians being contacted, care must be taken to ensure that these people can truly understand in order to give true informed consent for student participation. Where necessary, educators should try to explain jargon or technical terms in 'plain English' and/or provide some type of graphic organizer to support text.

The educator in BC would be expected to

> *Carefully review the user agreement and privacy policy of the technology with particular respect to how personal information may be collected, used, disclosed and stored by the host. Then insert a synopsis of the privacy concerns or risks as stated in the agreement or policy, how you perceive or project them to be and if there are privacy protection tools on the site that students can use.*
>
> Cooper, S., Southwell, J., & Portal, P. (2011).

Furthermore, in ALL cases, the parent/guardian and student have the right to deny such permission at their discretion. There are a variety of rational reasons that parents/guardians might deny permission: custody issues, safety issues (e.g. a student may have been previously threatened or harmed and is trying to avoid any future encounters), concern over cultural or religious discrimination, etc. In such a case, especially if posting the content is a requirement of the class or a specific assignment for a grade, ***the educator MUST provide alternatives to the assignment in the notice sent home and/or the attendant permission form.***

Once the educator has settled on a location for posting student exemplars, the educator must provide written notice to the parent/guardian that would outline:

- Reason for posting content or using the site/service
- Specific site/service to be used for posting content
- Types of content to be posted
- Whether students would be required to establish an account on the site/service
- Identifiable privacy risks for establishing an account and/or posting data to the site/service
- The educator's risk management strategies for using the site/service
- The educator's alternative activity if permission is denied

Putting student content online always involves some level of risk—whether it is on a 'secure' school district server with password protection or open for the world to easily find. As educators, we rarely think much about risk considerations, unless we are going on a field trip. This permission for posting student content should be as essential to your practice as your school requirement for field trip permission forms. For a field trip form, educators are expected to outline some of the expected risks associated with student participation. Virtually every parent or guardian has been on a field trip to a museum, park, or other common location. For these places, the risks are "regularized" because the parent or guardian has some context and expectations of what could go wrong. Risks associated with online participation are not regularized and many parents and guardians are not well aware of the potential risks, how they can be managed, and what steps the educator and school can take if there is an e-safety incident. The United Kingdom's Byron Review (2008), "Safer Children in a Digital World (Section 1.3)", sets out a useful matrix for educators to classify and evaluate risks to students using Web 2.0 and social media. It looks at the dimensions of content, contact, and conduct against the type of risks such as commercial, aggressive, sexual, and value-based as below:

	COMMERCIAL	AGGRESSIVE	SEXUAL	VALUES
CONTENT (child as recipient)	• Advertisements • Spam • Sponsorship • Personal information	• Violent or hateful content	• Pornographic or unwelcome sexual content	• Bias • Racist • Misleading information or advice
CONTACT (child as participant)	• Tracking • Harvesting personal information	• Being bullied, harassed or stalked	• Meeting strangers • Being groomed	• Self-harm • Unwelcome persuasions
CONDUCT (child as actor)	• Illegal downloading • Hacking • Gambling • Financial scams • Terrorism	• Bullying or harassing another	• Creating & uploading inappropriate material	• Providing misleading information or advice

Online Risks from Section 1.3 of "Safer Children in a Digital World: The Byron Review (2008)

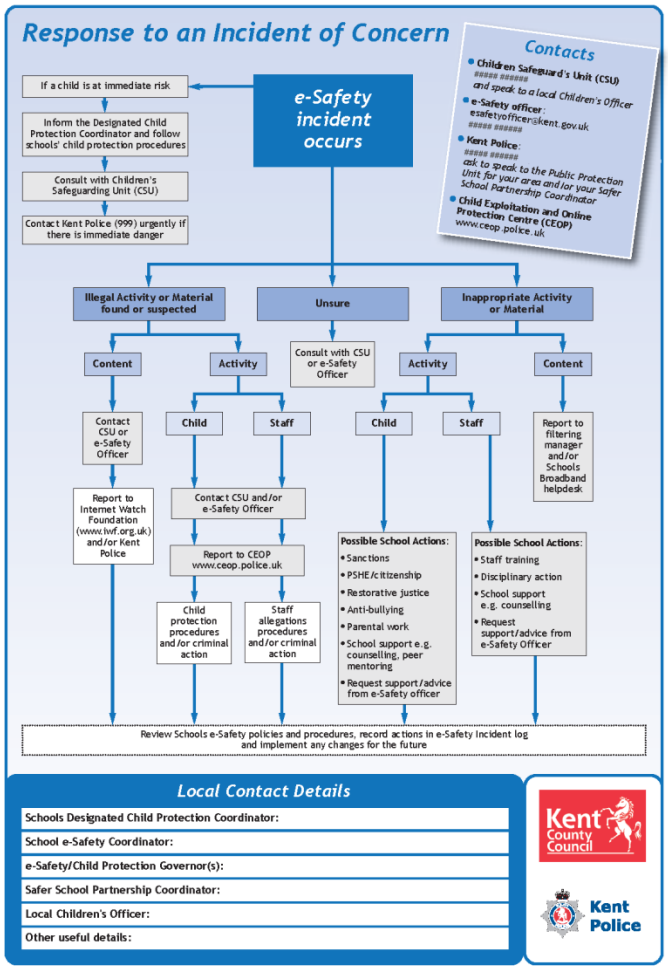
Missing from this matrix, however, are the critical risks of impersonation and identify theft that stem from the ability of others to track and harvest both publicly and privately available information.

Consideration 5: Safety & Protection Plan

Key Question: Is there a plan to respond to an e-safety incident?

Since use of the internet always involves some risk for students, educators must have a plan for responding to e-safety incidents that arise. It helps if the school and district have developed a response framework as well. For some ideas on what should be considered when developing a risk management plan see Appendix A: Teacher/Student Privacy Protection Plan. A risk management plan might include how the nature of content posted will be controlled, whether content will be posted through a single account after it has been "passed" by the educator, whether students' first and last names will be removed from posted items. It should include a copy of (or at least an explicit reference to) the school's acceptable use policy, as well as any class policies/procedures, and instruction on how to protect your own and other people's privacy.

It is prudent to plan the response a school or district might make to a privacy breach or other incident of concern that might occur while K-12 students are using Web 2.0 and social media tools for educational purposes. Kent County Council's "Response to an Incident of Concern (2012)" (thumbnail at right) is a world class model outlining roles and responsibilities for a school when e-safety incidents arise. The Kent County Council's model is based on an integrated response including schools, child welfare, health, and police. A key element of the model is an e-Safety Officer in each school—distinct from technology faculty/staff (those who deal with networking, hardware, and software issues). This e-Safety Officer role is an important one. Additionally, this model collects data about e-safety incidents reported in an e-safety incident log kept at each school that helps inform changes in practice and policies for the future.



Response to an e-Safety Incident ©Kent County Council, 2012

Appendix B: Potential BC Response to an Incident of Concern provides a possible British Columbian adaptation of the Kent County Council model. It outlines possible roles and responsibilities for BC schools in the event that there is an e-safety issue reported. In this vision, the role of e-Safety Officer is maintained as a role separate and distinct from the school or district technology managers. Such a model should not be difficult to implement as a similar type of role and responsibility structure is already firmly in place in the BC educational system with regard to reporting child abuse and neglect.

If an incident should occur, the school and educator should be prepared to communicate the incident to the parent/guardian in an effective way that complies with regulatory expectations. While legislation and practice are still evolving in this area, "Privacy Breaches: Tools and Resources" (2012) from the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC)provides some direction regarding what may constitute acceptable notification. In the case below, "e-safety incident" replaces "privacy breach":

> Notifications should include the following pieces of information:
>
> - Date of the e-safety incident;
> - Description of the incident;
> - Description of any information inappropriately accessed, collected, used or disclosed or received;
> - Risk(s) to the individual caused by the incident;
> - The steps taken so far to control or reduce the harm from the incident;
> - Future steps planned to prevent further incidents of a similar nature;
> - Steps the individual and parent/guardian can take to further mitigate the risk of harm;
> - Name and contact information of an individual at the school or district who can answer questions or provide further information;
> - Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. (If the school or district has already contacted the Privacy Commissioner, include this detail in the notification letter.) (OIPC BC, March 2012, 8)

Following BC's OIPC's suggested privacy breach protocols, in response to an e-safety incident, an educator, administrator, school or district, should prepare a list of frequently asked questions and answers to assist staff responsible for responding to further inquiries (OIPC BC, March 2012, 8).

Appendix C: 2 Response Letters Home after an Incident of Concern: Facebook with Users 13 Years or Older & Users under 13 Years (2012) has been shared by Kent County Council as examples of notification letters to send out in response to an e-safety incident in a school. Kent County Council's e-Safety web site has a wealth of additional information to support the use of technology with children in educational contexts: http://www.kenttrustweb.org.uk//Children/safeguards_esafety.cfm. For some useful and extensive resources closer to home for BC educators, parents/guardians, and students, see Mediasmarts.ca from Canada's Centre for Digital and Media Literacy. Mediasmarts.ca has a list of resources called "Cyber Security Consumer Tip Sheets" on topics like: "Safe Surfing" and "Socializing and Interacting Online" as well as resources like:

- A Word About (N)ethics
- Cyberbullying Rights and Responsibilities: Teacher Backgrounder
- Introduction to Cyberbullying: Avatars and Identity
- Cyberullying and Civic Participation
- Cyberbullying and the Law Fact Sheet
- Classroom Resources to Counter Cyerbullying

Consideration 6: Media Waiver Non-Coverage

Adapted by J. Hengstler from
© Alphaspirit, Dreamstime.com

Key Question: What if there's an existing school media waiver?

If there is a school media waiver, it likely will not be sufficient to cover you and your students' work for a variety of reasons:

- The waiver may not specify the type of content you are intending to post, where you're intending to post it and/or your purposes in posting it.
- If information written by one student contains information about another person(s), you may not have a waiver to release information on that 2nd party.
- The waiver may be specific only to the school or district's promotional needs (e.g. sports or team photos for publication).
- The waiver may be specific to certain media types (e.g. print or specific website/service).
- Not all parents/guardians will have signed and returned a media waiver.

In such a case it is prudent for the educator to consult with the school principal, or any other responsible individual to whom the educator is referred to by the principal, to determine whether the pre-existing media waiver would cover the intended activities and uses proposed—ensuring that the waiver supplies sufficient knowledge and notice for the informed consent required by law. It would be best to get a statement in writing (print or electronic) from a school administrator or official if the waiver is considered applicable in the educator's specific case. Note that a waiver alone would not meet the requirements of "notice" and "knowledge" for the informed consent required by BC regulations.

Adapted by J. Hengstler from © Cybrain, Dreamstime.com

Conclusion

As stated at the outset, this is a primer. Rules and regulations around the use of technologies in educational contexts in British Columbia will continue to develop as our uses and the technology themselves evolve. In turn, our risks change and develop. An educator needs to stay current with these changes and be able to fully document the steps s/he has taken to ensure wise use of technology, especially when posting or sharing minor students' work online. It takes time, practice and experience. Many educators need to upgrade their practice in using online sites and services with minor students in British Columbia, Canada.

The attached appendices provide a few tools to help with that:

- Appendix A: Teacher/Student Privacy Protection Plan (adapted from Cooper, Southwell, & Portal, 2011) provides some considerations for creating a "risk management" strategy that you can document.
- Appendix B: Possible BC Response to an Incident of Concern (adapted from Kent County Council, Response to an Incident of Concern, 2012) outlines a flowchart of potential actions that could be taken in response to an e-safety incident of concern and is rooted in a school based model which includes an e-safety officer and interagency cooperation.
- Appendix C: Response Letters Home after an Incident of Concern: Facebook with Users 13 Years or Older & Users under 13 Years (Kent County Council, UK, 2012) supplies sample wording for a letter home in the event that a child has an e-safety incident such as exposure to inappropriate content on Facebook.
- Appendix D: Request to Use Minor Student Work—Teacher Posted (Example Letter) models a letter to parents/guardians with a 'tear-away' permission for a teacher to post student work online. It has been adapted and shared with permission of a previous Vancouver Island Faculty of Education student, Candace Hanes.
- Appendix E: Informed Consent Agreement Template (adapted from Cooper, Southwell, & Portal,2011) provides a framework for developing permission slips for Web 2.0 and social media based activities

Disclaimer: This was not written by a lawyer. Before you, your school, or your district use any documents, be sure to have them vetted by school or district administration.

References

Byron, T. (2008). Safer Children in a Digital World: The Report of the Byron Review. http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/27_03_08byronreview.pdf

Cooper, S., Southwell, J., & Portal, P. (2011). Privacy Guide for Faculty Using 3rd Party Web Technology (Social Media) in Public Post-Secondary Courses. Vancouver Island University & BC Campus Publication. https://www.viu.ca/foipop/documents/Privacy_Guide_SocialMedia_Cloud_PostSecondary_Classes_2011.pdf

Graduate Studies Office. (2013). Ownership of student's work. University of Waterloo. http://gradcalendar.uwaterloo.ca/page/GSO-Students-Work

Hanes, C. (2012). Permission slip. Personal communication.

Kent County Council. (2012). eSafety Incident Response Letter (Facebook 13+).

Kent County Council. (2012). eSafety Incident Response Letter (Facebook Underage).

Kent County Council. (2012). Response to an Incident of Concern Poster. http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/ResponsetoIncident_A4Poster.pdf

Mediasmarts. (2013). Mediasmarts.ca: Canada's Centre for Digital and Media Literacy.

Office of the Information & Privacy Commissioner for British Columbia (OIPC BC). (February 2012). Cloud Computing Guidelines for Public Bodies. http://www.oipc.bc.ca/guidance-documents/1427

Office of the Information & Privacy Commissioner for British Columbia. (March 2012). Privacy Breaches: Tools and Resources. http://www.oipc.bc.ca/guidance-documents/1428

University of British Columbia. (2013). Copyright>>Copyright FAQ>>Basics 1.5 What is fair dealing and how does it relate to copyright? http://copyright.ubc.ca/faq/basics/#basics5

Wikipedia. (2013). Google platform. http://en.wikipedia.org/wiki/Google_platform#Datacenters

Appendix A: Teacher/Student Privacy Protection Plan

Adapted by J. Hengstler, 2013 from the *Privacy Guide for Faculty Using 3rd Party Web Technology (Social Media) in Public Post-Secondary Courses* (Cooper, Southwell & Portal, 2011)

NB: Before using any documents be sure to have them vetted by school or district administration prior to use.

Here are some elements to consider when creating a Teacher and Student Privacy Protection Plan:

1. **Determine what control you will have over student activity for uploading:**
    - What will the assignment require?
    - What content will be uploaded or posted?
    - How will the content be used?
    - With whom will the content be shared?

2. **If you, the teacher, will have limited control over content uploaded by students or other users, or if your students will be required to create an account and/or profile, you will need to draft a student user agreement that states:**
    - The reasons for using the technology;
    - The acceptable use agreement for the school –or refers to it & where it may be found;
    - Any specific class etiquette you expect;
    - The terms and conditions for uploading content;
    - The terms and conditions for using and disclosing personal information and the risks involved.

3. **If personal information from the student is necessary to use the technology and complete the class assignment, the teacher must provide options for students and parents/guardians who do not want to consent to the use of their personal information for the assignment such as:**
    - Participation under a pseudonym or avatar;
    - Having the teacher upload the student content anonymously to a "class" area;
    - Supplying a different assignment that does not require uploading data and/or sharing of personal information.

4. **Prepare a session or mini-lesson on privacy as preparation for the activity. The session should:**
    - Review basic privacy principles, such as knowledge, notice and consent and the fundamental requirements of FIPPA in terms that are developmentally appropriate to the student;
    - Identify best practices for students in protecting their personal information when using the specific technology, such as the risks of uploading or disclosing their or other people's personally-identifying information and the importance of and techniques for mitigating these risks;
    - Note: Sessions such as this can be beneficial for parents and guardians as well.

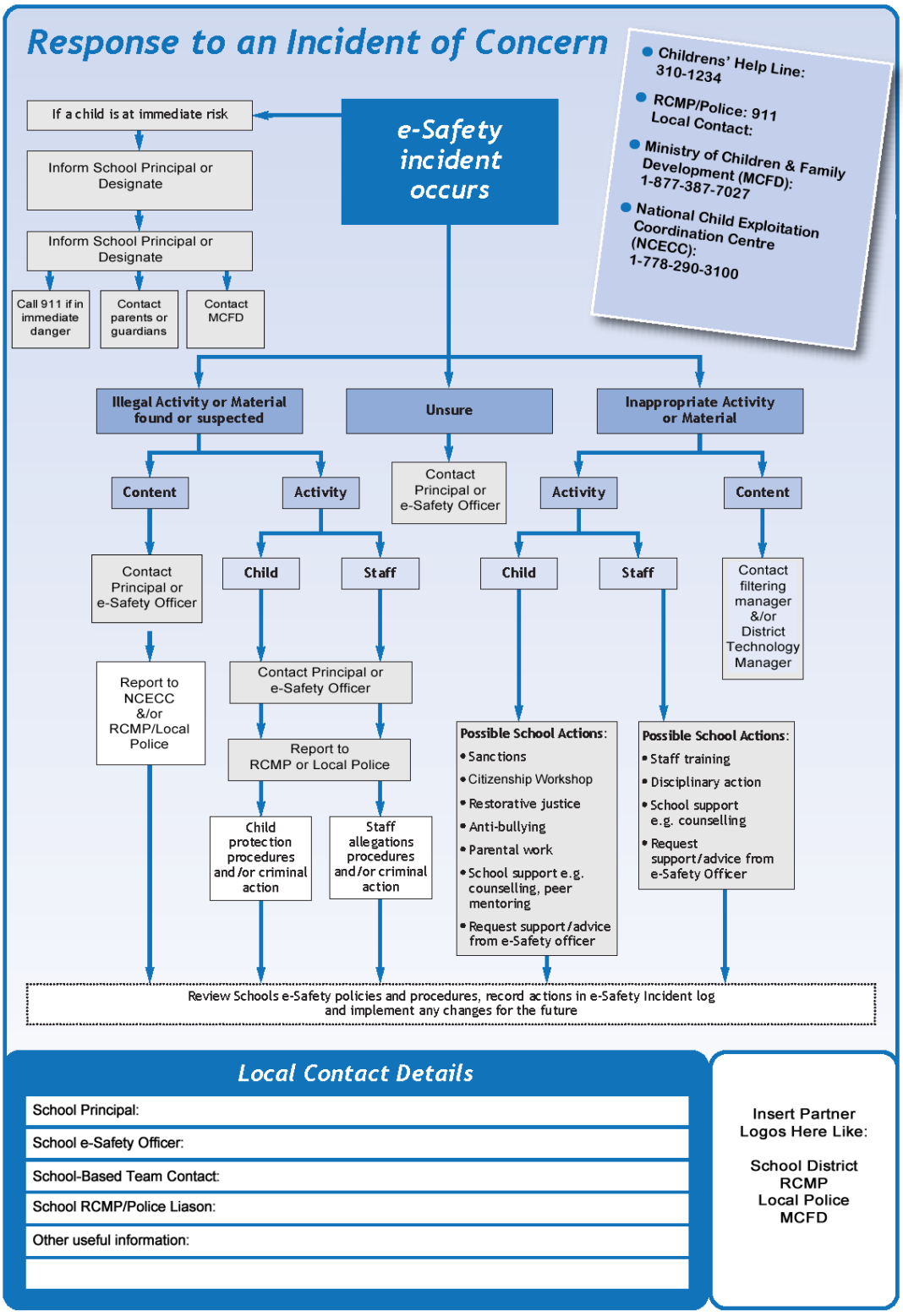
5. **Prepare and distribute a privacy and technology tips sheet to students that gives them easy to follow advice for using the site or service planned.**
    - Provide a similar information sheet for parents/guardians.

6. **Draft a written plan (that you can keep as a record) outlining the steps or process you will follow if there is a suspected privacy breach or an e-safety incident of concern (e.g., cyberbullying, contact by a stranger). You have a duty under FIPPA to both prevent and address breaches**.

7. **Discuss with your administrator and/or technology specialist (if so directed by your administrator) to review your proposed online activity so that they are aware and supportive of the privacy plan and protocols you've established.**

Appendix B: Possible BC Response to an Incident of Concern

(Adapted from Kent County Council's Response to an Incident of Concern, 2012)



Adapted J. Hengstler with permission from Kent County Council's "Response to an e-Safety Incident" (2012)

Adapted 2013 by J. Hengstler from Response to an Incident of Concern, Kent County Council (2012)

Appendix C: Response Letters Home after an Incident of Concern

Facebook Incident with Student 13 Years or Older (Kent County Council, 2012)

Note: References to UK & Kent specific resources have been highlighted for BC adaptation purposes

Dear Parents/Carers,

Following a serious incident where pupils in school may have been approached online by strangers, we would like to bring the importance of keeping children safe online to the whole school community.

<Our school> is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Websites such as Facebook offer amazing communication and social connections, however they can pose risks to children and young people such as cyberbullying, gaming, grooming and inappropriate content.

e-Safety is an important part of keeping children safe at (INSERT NAME) School. e-Safety is taught to all pupils which explains and demonstrates how to stay safe and behave appropriately online but we can only be successful in keeping children safe online if we work with you. Your help is needed to talk to your children about how they can keep themselves safe and behave appropriately online. It's important that we are all vigilant when children are using the internet and act to ensure they are protected from people who may pose a risk to them. Children can accidently or deliberately be exposed to illegal, unwanted or unpleasant content, comments or activity online and there are steps you can take at home to minimise this risk.

- Check that your child's profile is set to private and that only approved and known friends can see any information that is posted
- Closely monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information, clicking on unknown links, installing applications and not posting offensive messages or photos
- Ask them to like Click CEOP (Child Exploitation and Online Protection Centre) www.facebook.com/clickceop.
- Set up your own profile so you understand how the site works and ask them to have you as a friend on their profile so you know what they are posting online. Have a look at the advice for parents/carers from Facebook www.facebook.com/safety
- Read the Information for parents about safer social networking from CEOP at www.thinkuknow.co.uk/parents

- Make sure your child understands the following rules:
  - Always keep your profile private
  - It's not a good idea to accept friends you don't know in real life as they could be anyone, even if they are friend of a friend, they are still a stranger
  - Never post anything online which could reveal your identity or anything you wouldn't want an adult to see
  - Only click on links that you trust and always ask an adult if first if you are not sure
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell an adult you trust if you feel threatened, see something that makes you feel worried or someone upsets you online
  - Visit www.thinkuknow.co.uk for advice and information about keeping safe online

Websites to visit for more information:

www.thinkuknow.co.uk – Parents should visit the "Parent/Carer" Section and use the "Click CEOP" button to seek advice and report online abuse. Children and Young people can also access the site for advice and information and to report any concerns they have about online activity.

www.childnet.com – Visit the 'Know It All' Section for an interactive guide about online safety

ww.getsafeonline.org – Free up-to-date Security advice including using complex passwords and managing hacked accounts

www.kent.police.uk/internetsafety - Guidance from Kent Police

www.kent.gov.uk/esafety - Guidance from Kent County Council

The School e-Safety Coordinator (NAME) or Designated Child Protection Coordinator (NAME) are available to discuss any help you may need or concerns that you may have.

If you are worried that your child is at risk of harm or criminal offence has been committed then you can report your concerns using one of the following contacts. Please do not notify suspicious profiles of your actions, as this could enable them to delete material which might be required for any Police investigations

Kent Children's Social Care: 08458 247247

Kent Police: 101 or 999 if there is immediate risk

CEOP: Visit www.ceop.police.uk and use the "Click CEOP" reporting button

Yours Sincerely

Head Teacher

Facebook Incident with Student Under 13 Years (Kent County Council, 2012)

Note: References to UK & Kent specific resources have been highlighted for BC adaptation purposes

Dear Parents/Carers,

Following a serious incident where pupils in school may have been approached online by strangers, we would like to bring the importance of keeping children safe online to the whole school community.

<Our school> is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and it is not possible to control or verify the content. Facebook's terms and conditions state that all users must be 13 years or older and as such we strongly recommend that parents do not allow their children to have their own personal profiles online if they are below this age. We are however aware that many children do use such sites and it is possible that by banning access and removing children's' technology it may mean that children do not feel able to raise any concerns or problems encountered with parents/carers or adults in school. For more advice and information about under age use of Facebook please visit https://www.thinkuknow.co.uk/parents/Secondary/What-are-they-doing/Socialising/Under-13s-and-Face/

e-Safety is an important part of keeping children safe at (INSERT NAME) School. e-Safety is taught to all pupils which explains and demonstrates how to stay safe and behave appropriately online but we can only be successful in keeping children safe online if we work with you. Your help is needed to talk to your children about how they can keep themselves safe and behave appropriately online. It's important that we are all vigilant when children are using the internet and act to ensure they are protected from people who may pose a risk to them. Children can accidently or deliberately be exposed to illegal, unwanted or unpleasant content, comments or activity online and there are steps you can take at home to minimise this risk.

- Check that your child's profile is set to private and that only approved and known friends can see any information that is posted
- Closely monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information, clicking on unknown links, installing applications and not posting offensive messages or photos
- Ask them to like Click CEOP (Child Exploitation and Online Protection Centre) www.facebook.com/clickceop.
- Set up your own profile so you understand how the site works and ask them to have you as a friend on their profile so you know what they are posting online. Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents

- Make sure your child understands the following rules:
  - Always keep your profile private and never accept friends you don't know in real life
  - Never post anything online which could reveal your identity or anything you wouldn't want your parents to see
  - Only click on links that you trust and always ask an adult if first if you are not sure
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell an adult you trust if you feel threatened, see something that makes you feel worried or someone upsets you online

Websites to visit for more information:

www.thinkuknow.co.uk – Visit the "Parent/Carer" Section and use the "Click CEOP" button to seek advice and report online abuse

www.childnet.com – Visit the 'Know It All' Section for an interactive guide about online safety

ww.getsafeonline.org – Free up-to-date Security advice including using complex passwords and managing hacked accounts

www.kent.police.uk/internetsafety - Guidance from Kent Police

www.kent.gov.uk/esafety - Guidance from Kent County Council

The School e-Safety Coordinator (NAME) or Designated Child Protection Coordinator (NAME) are available to discuss any help you may need or concerns that you may have.

If you are worried that your child is at risk of harm or criminal offence has been committed then you can report your concerns using one of the following contacts. Please do not notify suspicious profiles of your actions, as this could enable them to delete material which might be required for any Police investigations

Kent Children's Social Care: 08458 247247

Kent Police: 101 or 999 if there is immediate risk

CEOP: Visit www.ceop.police.uk and use the "Click CEOP" reporting button

Yours Sincerely

Head Teacher

Additional information for schools to share - Further advice for parents/carers

<Our school> is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and it is not possible to control or verify the content.

Facebook's terms and conditions state that all users must be 13 years or older and as such we strongly recommend that parents do not allow their children to have their own personal profiles online.

Possible risks for children under 13 using Facebook may include:

- Facebook use "age targeted" advertising and your child could be exposed to adverts of a sexual or other inappropriate nature
- Children may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour
- Language, games, applications, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own
- Underage users can be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and inappropriate behaviour
- Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else!

We feel it important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting under aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children. We are however aware that many children do use such sites and it is possible that by banning access and removing children's' technology may mean that children do not feel able to raise any concerns or problems encountered with parents/carers or adults in school. It is also important that parents/carers are aware that whilst filtering tools or parental controls are very useful in keeping children safe online, they are not always effective and children may still access unsuitable content.

However, if you should decide to allow your child to have a Facebook profile we strongly advise you to be aware of the potential risks posed to your child. You may want to consider the following points.

- Check their profile is set to private and that only approved friends can see information that is posted
- Closely monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information, clicking on unknown links, installing applications and not posting offensive messages or photos
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application on www.facebook.com/clickceop on their profile.
- Set up your own profile so you understand how the site works and ask them to have you as a friend on their profile so you know what they are posting online. Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Read the Information for parents from CEOP at www.thinkuknow.co.uk/parents

- Make sure your child understands the following rules:
  - Always keep your profile private and never accept friends you don't know in real life
  - Never post anything online which could reveal your identity or anything you wouldn't want your parents to see
  - Only click on links that you trust and always ask an adult if first if you are not sure
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell an adult you trust if you feel threatened, see something that makes you feel worried or someone upsets you online

Appendix D: Request to Use Minor Student Work—Teacher Posted (Example Letter)

(Adapted by J. Hengstler, 2013, from eportfolio permission slip developed with Candace Hanes, 2012)

NB: Before using any documents be sure to have them vetted by school or district administration prior to use.

[Insert date here]

Dear Parents/Guardians,

As part of our class, your child will be completing [name the activity here]. During this activity your child will be creating [insert type of student work to be created]. Once this activity is completed, we would like students in our class to share their work online. I feel that sharing this content will support our educational goals because [give educationally sound reasons here].

As a BC teacher, I am subject to the BC Freedom of Information and Protection of Privacy Act. In accordance with this Act, I must at all times protect the privacy of students under my care. Under this Act, I cannot use personal and identifiable information of a student (e.g., first name, last name, school, grade, teacher, class etc.), including student work, without the written consent of the student's parent or guardian. I am aware that some parents/guardians may not be comfortable publishing their child's content online.

This letter of informed consent is to ask your permission to use (your child) _____'s work namely _____to be uploaded to a specific teacher-created [site/account] located at [URL here]. The content will be accessible to [describe who can see it/audiences] by [describe how people will be able to get to it—password protected, email link, etc.?].

Your child's work will be uploaded by me to an account or site created for the class. Your child will not be asked to create an individual account or create a profile. The content uploaded **will NOT include your child's name and will NOT include any personal and identifiable information**. I have attached the privacy terms of [the site/service] to this letter. [You must attach the privacy terms].

You may withdraw your consent at any time. Please fill out and return the tear away section below if you give permission to have your child's work shared and posted as described. If you have further questions or concerns, please feel free to contact me [insert your email address & school phone number here]. Thank you for your consideration.

Sincerely,

[Insert your name here]

---------- Cut or tear here----------

☐ I **GRANT** permission for my **child's work** to be used or included with the class content uploaded to [describe place/site of upload] by the classroom teacher.

Child's Full Name (please print) _____

Parent/Guardian: (please print) _____

Parent/Guardian Signature: _____

Date: _____

Appendix E: Informed Consent Agreement Template

Adapted by J. Hengstler from Cooper, Southwell, & Portal, 2011

NB: Before using any documents be sure to have them vetted by school or district administration prior to use.

Student Name: _____ **Date:** _____

Class: _____ **Teacher:** _____

Name and Description of the Activity, the Site/Service Used, and the Reason for Use in Class:
[Teacher: Insert the name of the class, activity, project or assignment and identify the site/service to be used, including how and why it will be used. Explain any "jargon" or technical terms in plain English for all parents/guardians to understand.]

Example: "As part of the research paper requirements for History 12, students will be asked to participate in, and help develop, a class "history wiki" by uploading their research findings on a weekly basis to the class wiki on [wikisitenameherecom]. A wiki is an online site where participants can collaboratively create, share, and edit content on a specific subject or subjects through a web browser like Internet Explorer, Firefox, or Safari. The class wiki will be password-protected and restricted for use by class members only.
NOTE: If your child is unable to participate in this online activity, an alternative activity will be provided by the teacher."]

Identifiable Privacy Risks:
[Teacher: Carefully review the user agreement, terms of service, and privacy policy of the site/service with particular respect to what personal information will be collected, how personal information may be collected, used, disclosed and stored by the host. If the physical data storage location is unclear, assume it is external to Canada. Insert a summary of the privacy concerns or risks as stated in the agreement, terms of use or policy, the risk exposure as you interpret it from those documents, and identify the privacy protection tools available to students.]

Example: "Wikis created on the [wikisitenameherecom] web site require users to register by uploading their username and valid email address. According to [wikisitenameherecom]'s user agreement and privacy policy, all personal information uploaded will be collected and stored by [wikisitenameherecom] in [location] and may be shared with [wikisitenameherecom]'s clients. This means that students may receive 3rd party solicitation emails such as advertisements or spam. Further, any information students upload to the wiki will be displayed with students' usernames and emails. To protect their privacy, students must select opt-out options in the privacy controls section of the web site or use a pseudonym and alternate (non-personal) email address when registering to use the site. While in class, students will receive training on proper privacy settings and the importance of protecting their privacy as well as that of fellow classmates. A handout reviewing the site's privacy settings and expectations for behaviour & content is attached [Be sure to attach those documents.]."]

Consent Statement:

I, _____, parent or guardian of

_____ 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 the class activity described above. I am aware of and understand the identifiable privacy risks as described above and will support the classroom teacher in minimizing the exposure of my child's and other people's personal information while my child is using the technology and review the materials the teacher provides.

Please check the box below if you request that your child use a pseudonym or remain anonymous online for the purposes of this class to minimize exposure of his/her or other people's personal information to 3rd parties that are not part of this class or project or who are otherwise not entitled to this information:

	By checking the box on the left, I request that my child use a pseudonym or remain anonymous online.

This consent is valid for the duration of the course (or end of the school year) unless revoked by me in writing and delivered to the teacher.

Parent/Guardian Signature: _____ Date: _____