**Risks that could arise with Cloud Computing**

The major risk associated with cloud computing is that data will not always be stored in Canada. Some data may be stored in the United States of America which enacts the trans-border data act. There is also the risk of the student posting something and the ‘digital footprint’ it leaves. We need to make sure the students are aware that once something is posted, it is online for good and they should be aware of what they are posting online. The personal information requirements (anything that can be used to identify you and where to find out) for creating an account will be limited to only what is necessary for the registration process. If you are concerned about someone figuring out your child’s name, you are able to sign up with your name instead. I want to remind you as well that I have suggested that you have your child sign up with their parent’s email address so that if any notices come, you will be able to see them and have access to them. Cloud computing is not 100% risk free but I have been doing everything I can to put rules, guidelines and options in place to keep your child as safe as I possibly can.

**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 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.” 1(Hengstler, 2013)

**How to stay safe with Cloud Computing**

Cloud Computing is designed to give you access to your data no matter where you go. Make sure that you have access to your child’s accounts so when you want, you can go online and see what they are posting. If I find something that is unsettling, I will contact you immediately.  There is also the option for your child to click on a button titled ‘report abuse’ within many web 2.0 tools if they come across anything unsettling. Before a student will be able to use cloud computing tools and contact others, I am requiring them to sign (as well as their parents) the consent form so that they are aware of the expectations when using the tool. If you do not feel comfortable signing the consent and having your child use cloud computing, even with all the adaptations suggested, additional options will be given, without any hindrance to their grade or learning.

**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 online and cloud based tools. Alternate activities will be provided to students, if parents/guardians 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.

[1] 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>