



Privacy Impact Assessment for Google Suite for Education (GSFE)

Part 1 - General

Name of District:	Nanaimo Ladysmith Public Schools		
PIA Drafter:	Dale Burgos/Andy Canty		
Email:	Dale.Burgos@sd68.bc.ca	Phone:	250.741.5273
Program Manager:	Andy Canty		
Email:	Andy.Canty@sd68.bc.ca	Phone:	250.741.5339

1. Description of Initiative

Introduction:

This Privacy Impact Assessment addresses the proposed use by the District of “Google Suite for Education” (“**GSFE**”) for educational programs offered by the District.

The advantages of the Initiative include:

- GSFE is offered to educational institutions at no additional cost;
- Reduction in paper use and efficiency in work flow;
- Enables workflow collaboration and sharing;
- Accounts can be accessible from any device via an internet connection;
- Fosters connections between students and educators to work collaboratively on projects;
- Unlimited storage capacity available in the Google Drive;
- Enables District to control sharing settings which enhances security of shared files and work.
- No software to install or maintain, and no manual maintenance (ie. security patching or time consuming support);
- Light weight computers that are easy to distribute;
- Able to administer machines through the school regardless of the number of devices.

Process

Once a school registers their web address with Google, the school is able to administer teacher and student accounts from an online administrative dashboard. The GSFE applications are unlike other public Google applications in that they enable greater filtering, advertisement blocking and application controls at the District level. The District can also control and place limits on information sharing, which can (for example) be limited to only school district issued account.

The attached User Guidelines for Staff and Students provides an overview of the Google Solution and its use within schools.

GSFE

The District will offer each of their schools, access to GSFE. The applications are:

- **Google Classroom:** Lets teachers create and organize assignments, provide feedback and easily communicate with their classes
- **Google Docs:** Personal Narratives, Fictional Stories, Paragraph Writing, Internet Safety Presentations, Word Definition Presentations for Word Studies, Student-led Conference Presentation, Forms for Quizzes for Language Arts, Reading, Science and Social Studies and online note-taking using custom made Google Forms
- **Google Sites:** Student ePortfolios, Local Research Projects, Collaborative Science Research
- **Google Maps:** Social Studies, Provincial First-nations Studies Projects, and Mapping Places in British Columbia and Recording Elevation Profiles on BC Destinations;
- **Google Picasa:** Classroom Picture Editing, Presentation Creation, Subject Topic Catalogues and Field Trip Documentation
- **Google Earth:** 3-D Exploration of the earth, Castles, Cathedrals and World Museum Trips, Geography Tours, Literature Trips
- **Gmail:** Communication with students, Book Club Communication, Reader Response Journals
- **Google Keep:** Create, share, and manage notes and to-dos.
- **Google Contacts:** Manage contacts
- **Google Calendars:** Organization of classroom projects, assignments and school events

- **Google Vault:** Archiving and eDiscovery for GSFE
- **Chrome extensions:**
 - *Read&Write for Google Chrome is a Chrome extension that provides accessibility and productivity tools in the GSFE environment. These include such functions as text-to-speech, dictation, word prediction, picture and talking dictionaries, voice notes, translation, vocabulary lists, and study skills in Google Docs, the Chrome web browser, and documents stored in Google Drive. It also may include Snapverter, which is an optional add-on for Read&Write for Google Chrome that converts printed documents and inaccessible digital files into readable PDF files within Google Drive.*

Based on this PIA, the School District can ensure that their use of the Google Solution meets the requirements set out in the *Freedom of Information and Protection of Privacy Act* (the “Act”). This PIA and accompanying checklist and descriptions serves as the School Districts’ PIA as required under s.69 (5.3) of the Act.

Security Measures and Consent

The Initiative necessarily entails use by students of the internet and storage of information in the Cloud, which may entail storage of information outside of Canada. The Initiative also involves the provision of third party hosting services by Google, which maintains servers outside of Canada.

In addition, to protect the security of each student’s personal information, the District intends to limit the information that students use and provide through GSFE. Students will be instructed on appropriate uses of the Google Solution that minimizes any personal information that may be subject to collection using these tools.

The Google Solution will also be based upon individual informed consent, so that students/parents who are uncomfortable with the potential for foreign access and storage or any third party access by Google can opt out of the Google Solution, and an alternate program will be provided to them.

Third Party Provider (Google)

GSFE is designed and hosted by Google, but will be administered by the District.

Google declares that while designs and maintains GSFE, it does not individually track or monitor student activity using this technology.

The terms and conditions upon which Google provides these services include the following:

- Google disclaims any property interest in any data generated by staff or students using GSFE: <https://support.google.com/a/answer/60762>
- Google represents that they will not share data with others except as noted in their Privacy Policy as of March 31, 2014 (<http://www.google.com/policies/privacy/>).

- Google enables the School District to add a digital “signature” to the header of our mail messages and thus recipients can check the domain signature to verify that messages are from our domain.
- The Google Apps’ digital signature conforms to the DomainKeys Identified Mail (DKIM) standard (<http://www.dkim.org/>). This feature facilitates our ability to mitigate spammers from forging the “From” on email messages so they appear to come from a user in our domain.
- Google acknowledges that it tracks some browsing activity in connection with GSFE apps, but it does not attempt to identify individual users. Rather, it uses activity and access history to improve and maintain these products.

We note that some concerns have been expressed in the United States about the collection, anonymization, aggregation and use by Google of student browsing history for internal research and product improvement purposes. Google makes clear in its Privacy Policy that it does collect information collected from its various services in order to maintain, protect and develop products and applications. However, this issue is subject to ongoing complaint proceedings in the US. Pending resolution of that complaint, the School District has provided a link to Google’s terms of service and privacy policies as part of the consent, so that any concerned individuals can make an informed choice.

Consent Process

Before using any Google products, students will have submitted a signed informed consent that acknowledges that their personal information will be disclosed, stored and accessed outside of Canada. The District will facilitate the consent-gathering process by sending home to each and every student a Kindergarten to Grade 8 [Consent Form](#) and a Grades 9-12 [self-consent form](#).

The School District will retain all consent forms in their local secure file storage areas for a period of one school year.

Once Google has received confirmation that an individual is verified as a student in a designated School in BC, an assigned educator will activate an email address for that student, which will also provide the student access to the other Google services as outlined in the consent form.

It should be noted that, the use of Google services is not an educational requirement for students. Students will not be obliged to use the assigned Google email, and that all school activities that rely on the use of student email must allow for and accept, an alternate email addresses or an equivalent means of student participation. Students will not be denied participation in a District/School-sponsored event or activity because they have not registered for a Google email address.

2. Scope of this PIA

This PIA covers the use of GSFE by schools within the School District and addresses the storage of data in non Canadian databases.

3. Related Privacy Impact Assessments

N/A

4. Elements of Information or Data

The personal information that will be disclosed to or accessible by or through the Initiative will be limited to:

- the student's Google-issued email address;
- student name and school
- student's browsing history while using the GSFE tools
- student work product.

The use of GSFE by School District staff and students is subject to the School District's Appropriate Use of School District Information Technology Administrative Procedure (AP 210). As a condition of use, users must agree to conduct themselves in a courteous, ethical and responsible manner while using all District technology resources, including the School District GSFE platform.

As all account and content information is hosted by Google on servers outside of Canada, to protect against any risk of foreign access and storage the School District will impose limitations to the type of information that can be shared within the School District GSFE system.

Both staff and students will be instructed by the School District on safe and acceptable use of the GSFE system and that the purpose of the GSFE tools are for "educational use" only. All stored content is to relate to classroom assignments, projects and curriculum work. Therefore, all users are to ensure that sensitive, confidential and/or personally identifiable information is not shared in any emails, attachments, files and documents and are not to be created or uploaded into the GSFE system. Staff and Students who access the district GSFE platform will be instructed to familiarize themselves with the uses and types of information that are both acceptable and unacceptable:

Acceptable Uses/Types of Information

- Classroom assignments, research notes, presentations, school-based projects (but must avoid posting assignments that involve personally identifiable, sensitive or confidential information);
- Curriculum-based multimedia objects created by students (videos, pictures, audio files, animations, etc.);
- Curriculum-based quizzes, tests, surveys;
- Calendars for assignment dates, project deadlines; and,
- Communication with teachers and other students related to these acceptable educational purposes (avoiding personally identifiable, sensitive or confidential information).

Unacceptable Uses/Types of Information

- Personal contact information (i.e. home address, phone number, email address and gender);
- Confidential, sensitive personal information (i.e. health, race or religious affiliation);

- Personal identifiable information about other persons i.e. other students, parents, teachers or family members (i.e. full names, addresses, emails, contact information);
- Student records (e.g. student attendance, schedule, grades, report cards, educator notes);
- Classroom assignments involving sensitive or confidential personal information, (e.g. a family history assignment with full names, birthdates, birth locations and other family members);
- Health information (e.g. specialist assessments, psychology reports, IEPs);
- Files in violation of copyright laws (e.g. illegally obtained music, videos, copyrighted images); and,
- All forms of harassment or bullying.

Note: If a student or teacher is unsure whether a specific type of information or content is appropriate when using Google Apps, they will be instructed to check with their teacher or senior administrator in their educational setting before creating the document or email. Staff and students will also be notified that **inappropriate or prohibited use of GSFE may lead to suspension or termination of user privileges**, legal prosecution or disciplinary action.

Part 2 - Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

1. Storage or Access outside Canada

Any personal information collected by Google through the GSFE system will be stored on servers located in the United States, and will therefore be subject to the laws of that jurisdiction (ie. the *USA Patriot Act*). Parents and students will be advised of this risk in writing, and asked to sign a consent to the foreign storage of this information.

2. Data-linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

3. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

** **Please note:** If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body’s privacy office(r) to determine how to proceed with this notification and consultation.*

4. Personal Information Flow Diagram and/or Personal Information Flow Table

1.	Student Consent and Parental Authorization is Sought to Start Using the Program and Collect Personal Information
2.	Student uses Program for course work
3.	Teacher access course work for purposes of evaluation and/or monitoring and progress assessment
4.	Information Technology technicians from the District will access the Program for the purposes of maintenance and upkeep
5.	<p>Google independently obtains additional consent from the user to collect, use and disclose the user's personal information for specifically defined purposes. Specifically, Google's Terms of Service provide that it may share personal information with companies, organizations and/or individuals outside of Google if the preservation or disclosure of the information is reasonably necessary to:</p> <ul style="list-style-type: none">(a) meet an applicable law, regulation, legal process or enforceable governmental request;(b) enforce applicable <i>Terms of Service</i>, including investigation of potential violations;(c) detect, prevent, or otherwise address fraud, security or technical issues;(d) protect against harm to the rights, property or safety of Google and our users or the public as required or permitted by law;(e) access account data only when the District System Administrators' grants Google employees explicit permission to do so for troubleshooting purposes; and,(f) remove any content that violates the Terms of Service by users.

5. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Student accounts could be compromised or misused.	Acceptable Use of Technology Policy, contractual terms of agreement in regard to security and password protection protocols etc. Limitation on information contained within accounts to exclude highly sensitive information	Medium	Low
2.	Parent or student withdraws consent or refuses to consent	School will produce alternative activity.	Low	Medium
3.	Unauthorized access to the student's personal information	Person student information is not stored in GSFE. Access to GSFE is password protected. Students instructed on minimizing personal information available through Initiative.	Low	Low
4.	Accidental or deliberate disclosure of personal information in Program	Contractual terms in regard to security; ongoing educational efforts with users; periodic auditing to detect unauthorized disclosures. Limitations on sensitivity of information utilized in connection with Initiative.	Low	Medium
5.	Unauthorized Use of Personal Information by Google (re: recent complaints about Google anonymizing and using information collected from student browsing history)	Provide notification to students and parents that Google collects and uses personal information for its own internal purposes, and seek consent.	Low	Medium

6. Collection Notice

Where the Initiative is collecting personal information directly from individuals we ensure that all individuals involved are told the following:

- (a) The purpose for which the information is being collected is for educational purposes including the grading of the students work.
- (b) The personal information that is being collected is directly related to, and necessary for, operating the student's program in the classroom.
- (c) School District #68 the business address is 395 Wakesiah Ave Nanaimo BC V9R 3K6 and our business telephone number of a District officer or employee who can answer questions about the collection is listed under Part's 1 – General

The School District will ensure that the collection of the personal information informs individuals using GSFE of the collection of personal information, the legality of authority for collection, the disposal of data for a pre-determined term of retention and the contact information of the person who can answer questions regarding the collection and correction of data and the effective date of consent as noted on the consent form. The signed consent forms will be sent, stored, retained and secured in the same directory location as the District's Student Information System (BCeSIS/MyEducationBC) which also has an approved PIA.

Part 3 - Security of Personal Information

NOTE: Consult with your privacy office(r) and security personnel when filling out this section.

1. Please describe the physical security measures related to the initiative (if applicable).

- N/A GSFE is a cloud based application

2. Please describe the technical security measures related to the initiative (if applicable).

GSFE is password protected

Firewalls exist at the schools

3. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Personal Information such as student name, email address and school will be controlled by Microsoft Active Directory and can only be changed within that structure by IS and teaching staff.

Students and teachers will also be instructed on what information is acceptable and what is unacceptable per Section 4 – Elements of Information or Data. This will limit the personal data.

4. Please describe how you track who has access to the personal information.

The GSFE system is protected by username and password.

Part 4 - Accuracy/Correction/Retention of Personal Information

1. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Student's name, grade and school to create the GSFE login. If any personal information requires an update, it can be completed by the school administrator.

2. Does your initiative use personal information to make decisions that directly affect an individual(s)?

No

3. If you answered "yes" to question 2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

4. If you answered "yes" to question 2, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 - Further Information

1. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No.

2. Does the program involve access to personally identifiable information for research or statistical purposes?

No. Student progress is only to provide assistance to the student.

3. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No

Part 6 - Privacy Officer(s) Comments

None