**Google Apps for Education – Terms of Use Protocol for Staff and Students**

Google Apps for Education (GAFE) is a globally used collection of secure, online, “cloud computing” tools that provide staff and students with a set of tools for digital productivity, file storage, collaboration and communication.

We provide access to and manages Google Apps for Education accounts for staff and students in the district. These applications are different from public Google applications (such as gMail or Google Docs) in that they are managed by the district, do not present users with advertising or scan student or staff information for advertising, and allow for more strict filtering and application control by system administrators.

The personal information required for creating Google Apps for Education accounts, and any digital files created or uploaded into the platform are located on Google servers that reside outside of Canada, and are therefore subject to the British Columbia Freedom of Information and Protection of Privacy Act (FIPPA). The Google Privacy Policy and GAFE Terms of Service state that Google will not share any GAFE information with any 3rd party, except under legal obligation as mentioned in this document below. Therefore, we cannot guarantee protection of secret disclosures of information to a foreign authority as a consequence of foreign laws.

**Consent**
Before a student can be provisioned a GAFE account, a consent letter must be signed. No personal account information is shared with Google for any students where consent has not been obtained. A copy of the GAFE consent letter can be found at: <URL>.

**Personal Information for Account Creation**The GAFE platform allows to set up, manage and delete all our own staff and student accounts. To create an SD43 GAFE account, the following pieces of information are stored on Google’s servers: First and last name; School; password.

**Acceptable Use of GAFE**The use of GAFE by staff and students is bound by the Digital Responsibility for Staff and Students Administrative Procedure. As an overview, this document states that users will conduct themselves in a courteous, ethical and responsible manner while using all district technology resources, including the GAFE platform.

As all account and content information is hosted by Google on servers outside of Canada, there are important limitations to the type of information that can be shared within the GAFE system. Both staff and students must remember that the purpose of the GAFE tools are for “educational use’ only - meaning content related to classroom assignments, projects and curriculum related work. Therefore steps must be taken by all users to ensure that sensitive, confidential and/or personally identifiable information is not shared in any emails, attachments, files and documents created or uploaded into the GAFE system.

Staff and Students who are accessing the district GAFE platform need 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 (avoiding 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
* Formative assessment material (e.g., teacher comments, peer feedback)
* Calendars for assignment dates and project deadlines
* 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 (e.g., home addresses, phone numbers, email address)
* Confidential, sensitive personal information
* Any personally identifiable information (i.e, full names, addresses, emails, contact information) about other persons (e.g., any other student, teacher, parent, family member)
* Student records (e.g., student attendance, schedule, grades, report cards, etc)
* Classroom assignments involving sensitive or confidential personal information, (e.g., a family history assignment with full names, birthdates, birth locations, etc of family members)
* Health information (e.g. specialist assessments, psychology reports, IEPs)
* Any files in violation of copyright (e.g., illegally obtained music, videos, copyrighted images)
* Any form of harassment or bullying behaviour

If a student is unsure whether a specific type of information or use of Google Apps is appropriate or inappropriate, they should ask their teacher before creating the document or email. Inappropriate or prohibited use of GAFE may lead to suspension or termination of user privileges, legal prosecution or disciplinary action appropriate under any applicable laws, policies, regulations, collective agreements or contracts.

**Access to GAFE by System Administrators**As per the Digital Responsibility for Staff and Students Administrative Procedure (140.1 and 140.2), all activities conducted on the GAFE platform are not private, and may be monitored or reviewed at any time, and without prior notice.

**Access to GAFE by Google**As per the Google Apps for Education Terms of Service and Privacy documents, all the personal account information and any content created or uploaded into the GAFE platform is owned by and will not be shared or sold to third party organizations.

However, as outlined in their privacy policy, Google does maintain the ability to access and share personal or content data on the GAFE platform under the following circumstances:

* Google has obtained additional consent from the user to share personal information
* We grant Google explicit permission for troubleshooting purposes
* For legal reasons, Google will share personal information with companies, organizations or individuals outside of Google if they have a good faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
	+ meet any applicable law, regulation, legal process or enforceable governmental request.
	+ enforce applicable Terms of Service, including investigation of potential violations.
	+ detect, prevent, or otherwise address fraud, security or technical issues.
	+ protect against harm to the rights, property or safety of Google, their users or the public as required or permitted by law.