



Security and Privacy Using Google Apps for Education (“G-Suite”) Newfoundland and Labrador English School District (“District”)

The District has established its own [Google for Education](#) domain - nlesd.ca - which is available to authorized users only. This means that the District has control over the domain and manages who can login. This provides the District with its own, online collaboration and communication system. Access to G-Suite is provided through a District supplied *nlesd.ca domain username and password*. **All District G-Suite access is only permitted through an nlesd.ca account.** One common domain (nlesd.ca) facilitates security, system administration, etc. which allows both staff and students of the District to use the online applications in a secure and safe environment.

Logging in to G-Suite, using your nlesd.ca account, grants access to applications and tools that are managed by the District. This online environment does not include advertising, and comes with strict controls over content and filtering. As such, these applications are different from available public Google applications.

The District is obligated to protect the personal information, in its custody, from unauthorized access. It must also manage the collection, use, disclosure and disposal of this information. The District will take all reasonable means to protect personal information. In keeping with our commitment, the District has extensively reviewed all policy and security measures regarding G-Suite. Based on this research, we are satisfied that G-Suite protects the privacy of all staff and students - [Privacy and Security Information](#).

Even though District data resides on Google servers it is still owned by the District and we are still responsible for this data. See the following article - [Introduction to Cloud Computing - Office of the Privacy Commissioner of Canada](#).

The following information outlines the information collected during the review of G-Suite security and privacy measures.

Types of Data and Rights to Data on G-Suite

Currently, Google Data centers are located all over the world. Any District data added, uploaded or created in G-Suite (such as this document) is stored on servers located in Google Data Centers. Even though data is stored on Google servers, the District still retains ownership of its data. Other District data, such as financial information, student information (e.g. PowerSchool), is stored on servers in District Data Centers which are protected behind security appliances and firewalls managed and deployed by the District.

The District is using G-Suite for teacher-student collaboration, teacher-parent collaboration, staff and student email, documents, presentations, websites, etc. Such data, which will be stored on Google's servers, also includes user login information (First Name, Last Name, User name), and their login password. All passwords are **encrypted** which means that the District and Google cannot read them.

Details regarding Google security and privacy are as follows:

1. G-Suite is governed and managed by the following security policies which ensures that Google will not inappropriately share or use personal information stored in our systems:
 - [Google Privacy Policy](#)
 - [Privacy and Security Information](#)
2. The [Google Apps for Education \(Online\) Agreement](#) confirms that District students, faculty, and staff are the *exclusive owners* of their data.
3. Google adheres to applicable U.S. privacy laws, and the [Google Apps for Education \(Online\) Agreement](#) details their obligations and compliance with FERPA regulations - [Family Educational Rights and Privacy Act](#).
4. [Google Cloud Platform Security](#) which ensures that their data protection compliance meets *international standards*.
5. All of a user's data is owned by the user and the District and [Google doesn't assume ownership of any customer data](#).
6. Google's position on reliability, privacy, and security – [security and privacy for administrators](#).

7. *There are no ads in Google Apps for Education (G-Suite) core services.*
8. Through implemented controls, security measures and policies protect user data, Google systems have obtained a *SAS 70 Type II verification* and Google will continue to seek similar verification.

Although the above mentioned laws and agreements may have no legal standing in Newfoundland and Labrador or Canada, the District is of the opinion that they do confirm and demonstrate Google's commitment to the protection of personal information of our users and is reflective of the high standards for security and privacy that is present in G-Suite.

Based on *Google's Privacy Policy* regarding the protection of personal information, the District is confident that G-Suite, which is different from public Google or generic Gmail, meets our expectations and requirements for security and privacy.

However, even though similar laws exist in Canada, under U.S. law the District cannot guarantee against the possible secret disclosure of information to a foreign authority (e.g. US Government, National Security Agency, etc.) as a consequence of foreign laws, criminal investigation, etc. The District is aware of the potential risk associated with a "secret disclosure" but considers the probability of such an event extremely low.

Based on all information researched and information collected the District is satisfied to accept this "extremely low risk" in order to benefit from the educational and collaborative features of G-Suite for our users. Furthermore, thousands of teachers and students from across the country are already benefitting from using G-Suite and by leading the way, other Districts have laid the groundwork regarding security and privacy in G-Suite so that District students and staff can also benefit from its rich offering of educational applications and features. To date, approximately 70 million teachers and students are using G-Suite.

Username Within G-Suite

To further protect users, we have implemented the following naming convention:

Adults

Display name: Firstname Lastname opt
Username: firstnamelastname(opt)@nlesd.ca

Where (opt) is an optional string (sometimes in the middle not the end) to differentiate between individuals with similar (same) name. Opt is a mixture of letters and numbers.

Students

Display name: Firstname Lastname # (STUDENTS)
Username: flastname#_s@nlesd.ca

First initial used instead of firstname in the username as students may choose to use these usernames outside the system. Using initials reduces false familiarity and reduces problems with identifiably feminine names.

(STUDENTS) and _s used to identify and distinguish students in Display Name and username. It was a common request that staff wanted to know when they were corresponding with students or staff, some were reluctant to use the system otherwise. Due to the high number of family names in NL we added this marker. Where # is a random number to differentiate between individuals with same username.

No Advertising in G-Suite

G-Suite is free for educational purposes. G-Suite is also offered “**completely ad-free**” -- this means District data is not processed or scanned by Google's advertising systems.

See [Google Privacy FAQ](#) : Does Google use my organization’s data in G-Suite for advertising purposes?

*Completely ad-free covers the **core** Google Apps for Education (G-Suite) suite.* These core apps include, but are not limited to, Mail, Contacts, Drive, Docs, Sheets, Slides, Sites, Hangouts, Calendar, etc.

Note: It does not cover other non core Google Apps that a user may access through their G-Suite account such as YouTube or any other 3rd party app that a user authorizes through their own G-Suite account.

As well, there are no ads in Google Search when you are logged in with your District nlesd.ca account.

Access to NLESD.ca Online Information

The following persons, positions or employee categories have access to user logins, and through this, to their G-Suite accounts and information:

Senior District Technology Staff (designates) will be District's G-Suite domain administrators. G-Suite Domain administrators' access and rights include:

- Global access to all G-Suite (staff and student), account settings (usernames, alias'), user-created sites;
- Monitoring the entire nlesd.ca system (with cause – see District's Acceptable Use of Technology regulations);
- Viewing statistics regarding your account, such as information concerning your last login or data storage usage;
- Resetting your account password, suspend or terminate your account access and your ability to modify your account;
- Accessing or retaining information stored as part of your account, including your email, contacts and other information; and,
- Receiving account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request; and,
- Deleting your account and all data associated with that account;

⇒ School administration or assigned school staff are able to reset teacher/staff and student passwords.

Google tech support will be granted your account data only when District domain administrators grants Google employees **explicit permission** to do so for troubleshooting purposes. During the course of troubleshooting an issue or other investigation, the Google Support team may ask for the creation of a test administrator account, solely to be used to resolve the particular issue at hand and in conjunction with a designated G-Suite Administrator.

Notes:

- Students/staff can export their files from G-Suite when they leave the District.
- The District will determine when data will be removed/deleted from G-Suite. Under normal circumstances student accounts will be deleted in October after the user leaves the District to allow for any required transition to postsecondary institution.
-

Google and Confidential Information

As a company, Google has established one of the most secure, robust and resilient communication networks of ***distributed data centers in the world***. From Google: “securing and protecting information on these servers is critically important to us -- in fact, Google, Inc. relies upon the ***same network and server infrastructure used by our education customers on Google Apps for Education***”. For further information see ***How Google protects your data***.

The following statements summarizes some of Google’s best industry practices for network security and user privacy:

- ⇒ It's your content, not ours. Your content belongs to your school, or individual users at your school - **Not Google**;
- ⇒ We don't look at your content. Google employees will only access content that you store on Apps when an administrator from your domain grants Google employees *explicit permission* to do so for troubleshooting – *this is done with an identifying unique PIN which is held by the District administrators*;
- ⇒ We don't share your content. Google does not share personal information with advertisers or other 3rd parties without your consent;
- ⇒ We sometimes scan content, but only under circumstances like spam filtering, anti-virus protection, or malware detection;
- ⇒ Our systems scan content to make our Apps work better for users, enabling unique functionality like powerful search in Gmail and Google Docs. This is completely automated and does not involve humans;

For more information, see our detailed:

- [Google Privacy Policy](#);
- [Technologies and Principles](#);

The following is from Section 7 of the [Google Apps for Education \(Online\) Agreement](#) under **Confidential Information**:

- **7.1 Obligations.** *Each party (i.e. the District and Google) will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to stakeholders, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any stakeholders, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its stakeholders, employees and agents in violation of this Section.*
- **7.2 Exceptions.** *Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.*
- **7.3 Required Disclosure.** *Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.*

Safety Online

[Google Safety Center](#) provides many resources are made available by Google to students, teachers and parents.

Core Services and Chromebooks [\(from Google\)](#)

Core Services

Gmail, Classroom, Drive and Docs, Contacts, Calendar, Keeps, Sites and Hangouts all represent the core services offered through G-Suite. There is no advertising in these core educational services and District data is not used for advertising purposes in any way. Student data created, collected and stored in these services is strictly used solely for purposes that these services are provided for, such as emailing and collaborating.

Chrome Sync

By logging in to *any* Chromebook or *any* Chrome browser, using nlesd.ca credentials, users will have access to their apps, data, bookmarks, etc. This is achieved with a built-in feature called Chrome Sync. It's automatic. This means by using Chrome Sync, users can get the same, personal experience no matter where they login or what device they use.

Google aggregates data from millions of users of Chrome Sync, only after completely removing personally-identifying information regarding individual users (e.g. name). This process is used to holistically improve core educational services. For example, if a particular web site visited appears to be broken, this web site would be moved lower in any Google search results. This process does not analyse any individuals behaviors and is not connected to any specific person. Furthermore, G-Suite users' Chrome Sync data is not used to target ads to individual users.

Note: *As desired, Chrome Sync can be disabled altogether, or you can choose to only sync certain data.*

Awareness of Terms of Use and Privacy

The District will take all reasonable steps to inform all District users of G-Suite (teachers, students and staff) about regulations regarding acceptable, responsible use of technology related security and privacy. Some of this information will be developed within the District or be referenced via online resources (e.g. Google Security Center).

Under the ATIPP Act the District has the responsibility to ensure that reasonable security measures are enforced to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. In addition, the District needs to inform users as to what information is being collected and what information Google may use and have access to, and that their data including e-mail will be stored outside of Canada and subject to foreign laws.

Staff and students should be aware of who has access to their accounts and information stored on Google. This information should outline what the domain administrators (nlesd.ca) can do with their account - see section **Access to NLESD.ca Online Information**.

Google's Privacy Policy clearly establishes who owns the data, and who has access to the data. Basically, Google will only access aggregate information, across millions of users, to improve service. **Google Cloud Platform** meets rigorous privacy and compliance

standards that test for data safety, privacy, and security. Even though these laws and governing regulations may have no legal standing in Newfoundland and Labrador or Canada, the District is confident that they do establish Google's commitment to the protection of personal information of our students, teachers and staff.

Data Stored on US Servers - Patriot Act

In order to reduce the impact should a server be compromised and to ensure a high degree of availability of data, Google has many servers located in data centers across the world. This is to protect against the risk of failure in one of their data centers. Currently, Google does have Data Centers located in Canada, however District data will primarily be stored in the U.S.

The impact of foreign legislation on security and privacy is a concern whenever data storage is outsourced outside of Canada or to a non-Canadian company. The ATIPP Act recognizes this, and while it does not restrict or prohibit this kind of outsourcing, it does require public bodies, such as the District, to ensure that reasonable measures are taken to mitigate privacy risks.

The U.S. Patriot Act is an example of such foreign legislation. The Patriot Act does allow American courts to order U.S. companies to provide them with limited information under such circumstances such as a counter-terrorism investigation. The possibility would also exist for such access under Canadian legislation if the data were stored on servers in Canada. However, such orders are very rare. Even under such legislation, the ownership of District data stored on Google servers still remains with the District. As per Google's security policies and procedures, the District will be notified if access to the data is requested, except when specifically prohibited by law.