

Wendell School District No. 232 recognizes the importance of providing positive, productive educational experiences through the district's Internet, computer, and network services. To promote this objective and protect its staff and students the board authorizes the superintendent or designee to:

1. Prohibit and prevent school computers and other school owned technology-related services from sending, receiving, viewing or downloading materials that are deemed to be harmful to minors, as defined by Idaho Code Section 18-1514.
2. Prohibit and prevent unauthorized online disclosure, use, or dissemination of personally identifiable information of students.
3. Select and employ technology protection measures on the district's computers to filter or block Internet access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of a minor, or other information that is determined to be in violation of district policies.
4. Establish and enforce appropriate disciplinary measures to be taken against persons violating this policy.
5. Handle complaints regarding the enforcement of the district's Internet use policies and procedures.

The district will limit Internet access to materials that enrich and support the curriculum and educational needs of users, contribute to the delivery of efficient and effective business or educational functions, and expedite professional district communications.

PRIVACY

Use of the district's technology resources is a privilege and not a right. Access has not been established as a public access service or a public forum. The district reserves the right to monitor, inspect, copy, review, delete, and/or store at any time and without prior notice any and all results of usage of the Internet, computers, mobile computing devices, network resources, and any and all information transmitted or received in connection with such usage. All such information will be and remains the property of the district and users have no expectation of privacy regarding such materials. The district has the right to place restrictions on the use of the district's Internet, computers, mobile computing devices, and network resources and may also deny access to staff and students who violate related policies and procedures.

INTERNET SAFETY FOR STUDENTS

The district's instructional program will include a component of Internet safety for students, including interaction on social networking sites and cyberbullying awareness and response.

The district will take appropriate steps to protect all students from access, through the district's computers, including mobile computing devices, to visual depictions that are obscene, contain child pornography, are harmful to minors, or depicting the sexual exploitation of a minor, as defined in Idaho Code §18-1507, by installing and utilizing specific technology that blocks or filters Internet access to such visual depictions.

The building principal or designee may authorize the disabling the Internet filter system only for the purpose of enabling access for bona fide research or other lawful purpose. Disabling of the Internet filter system by any other staff member or student will result in disciplinary action.

As required by the Children's Internet Protection Act, this district will hold annual public meetings to receive input from parents and other patrons regarding the district's Internet safety plan, including the use of an Internet filtering service.

Any staff member, student, parent, or patron may file a complaint regarding enforcement of this policy or request that the district either block, or disable a block of, a particular website. The individual must file a written complaint with the superintendent. The District Technology Committee will review the request and a committee's recommendation will be submitted to the superintendent. The superintendent will render a written decision and notify the individual who made the request. The superintendent's decision will be final.

PROHIBITED USES

The district's Internet, computers, mobile computing devices, and network resources may only be used for approved district activities and educational purposes. All users must fully comply with this policy and immediately report any violations or suspicious activities to the classroom teacher or building principal. Prohibited uses of district technology include, but are not limited to:

- 1. Causing Harm to Individuals or to Property**
 - a. Use of obscene, profane, vulgar, inflammatory, abusive, threatening, disrespectful language or images.
 - b. Making offensive, damaging, or false statements about others.
 - c. Posting or printing information that could cause danger or disruption.

- d. Bullying, hazing or harassing another person.
- e. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data.
- f. Disguising one's identity, impersonating other users, or sending an anonymous email.
- g. Posting personal information (e.g. phone number, address) about oneself or any other person, except to responsible agencies.

2. Engaging in Illegal Activities

- a. Participating in the sale, purchase or promotion of illegal items or substances.
- b. Accessing or transmitting:
 - i. Pornography of any kind
 - ii. Obscene depictions.
 - iii. Harmful materials.
 - iv. Materials that encourage others to violate the law.
 - v. Confidential information.
 - vi. Copyrighted materials without authorization or as provided by fair use regulations.
- c. Attempting to disrupt the computer system or destroy data by any means.

3. Breaching System Security

- a. Sharing one's or another person's password with others.
- b. Entering another person's account or accessing another person's files without authorization.

- c. Allowing others to gain access to one's individual account
- d. Interfering with other users' ability to access their accounts.
- e. Allowing student access to sensitive data.
- f. Attempting to gain unauthorized access to another computer.
- g. Using software or hardware tools designed to interfere with or bypass security mechanisms.
- h. Utilizing software or hardware applications that are not approved for business use.
- i. Attempting to evade the district's computer filtering software.

4. Improper Use or Care of Technology

- a. Accessing, transmitting or downloading large files, including posting chain letters or engaging in spamming.
- b. Attempting to harm or damage district technology, files or data in any way.
- c. Alteration of configured equipment, including the addition of unauthorized passwords and users accounts.
- d. Leaving an account open or unattended.
- e. Attempting to remedy a security problem and not informing a school official.
- f. Failing to report the abuse of district technology.
- g. Installing, uploading or downloading unauthorized programs.

- h. Copying district software for personal use.

- i. Using district technology for:
 - i. Personal financial gain.
 - ii. Personal advertising or promotion.
 - iii. For-profit business activities.
 - iv. Unapproved fundraising.
 - v. Inappropriate public relations activities such as solicitation for religious purposes.
 - vi. Inappropriate political purposes.

CONSEQUENCES FOR INAPPROPRIATE USE

Failure to comply with this policy or inappropriate use of the district's Internet, computers, mobile computing devices, or network resources may result in usage restrictions, loss of access privileges, and/or disciplinary action up to and including expulsion. The superintendent or designee may also report the violation to law enforcement where appropriate.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

NOTICE

The district will inform staff, students, parent/guardians, and other users about this policy through posting on the district website and by publishing in the student handbook. A copy of this policy will be available for review at the district office and will be provided in writing to parents/guardians upon request. The district will also file this policy with the state superintendent of public instruction every five years.

By accessing the district's Internet, computers, mobile computing devices, and network resources, users acknowledge awareness of the provisions of this policy and awareness that the district uses monitoring systems to monitor and detect inappropriate use.

All students and staff are required to sign a technology user agreement (see Policy No. 519F1, Internet, Computer and Network Services User Agreement) that signifies their understanding and agreement to follow these regulations.

G SUITE FOR EDUCATION

At Wendell School District, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Classroom, and more used by tens of millions of students and teachers around the world. At Wendell School District, students will use their G Suite accounts to complete assignments, communicate with their teachers, and learn 21st century digital citizenship skills.

The notice below provides answers to common questions about what Google can and can't do with your child's personal information, including:

What personal information does Google collect?

How does Google use this information?

Will Google disclose my child's personal information?

Does Google use student personal information for users in K-12 schools to target advertising?
Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will not create a G Suite for Education account for your child.

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

- Gmail (including Inbox by Gmail)
- Calendar
- Classroom
- Contacts
- Drive
- Docs

- Forms
- Groups
- Keep
- Sheets
- Sites
- Slides
- Talk/Hangouts
- Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Specifically, your child may have access to the following “**Additional Services**”: YouTube, GoogleMaps, Google Docs, Google Classroom, among others.

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, Wendell School District may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
- log information, including details of how a user used Google services, device event information, and the user’s Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education **Core Services**, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent.** Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With Wendell School District.** G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
- For external processing.** Google may provide personal information to affiliates or other trusted businesses or personal to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons.** Google will share personal information with companies, organizations or individuals outside of Google if it has 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, Google users or the public as required or permitted by law.
 - Google also shares non-personal information – such as trends about the use of its services – publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child’s information by Google. If you don’t provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child’s information as described in this notice. If you consent to your child’s use of G Suite for Education, you can access or request deletion of your child’s G Suite for Education account by contacting Wendell school District Technology Department. If you wish to stop any further collection or use of your child’s information, you can request that we use the service controls available to limit your child’s access to features or services, or delete your child’s account entirely. You and your child can also visit <https://myaccount.google.com> while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google’s G Suite for Education accounts or the choices available to you, please contact the Technology Department at Wendell School District. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the [G Suite for Education Privacy Center](https://www.google.com/edu/trust/) at <https://www.google.com/edu/trust/>), the [G Suite for Education Privacy Notice](https://gsuite.google.com/terms/education_privacy.html) at https://gsuite.google.com/terms/education_privacy.html) and the [Google Privacy Policy](https://www.google.com/intl/en/policies/privacy/) (at <https://www.google.com/intl/en/policies/privacy/>).

The Core G Suite for Education services are provided to us under [Google’s Apps for Education agreement](https://www.google.com/apps/intl/en/terms/education_terms.html) at (https://www.google.com/apps/intl/en/terms/education_terms.html) (see <https://support.google.com/a/answer/2888485?hl=en>), insert: and the [Data Processing Amendment](https://www.google.com/intl/en/work/apps/terms/dpa_terms.html) (at https://www.google.com/intl/en/work/apps/terms/dpa_terms.html)]



LEGAL REFERENCE:

Idaho Code Sections

- 6-210 – Recovery of Damages for Economic Loss Willfully Caused by a Minor
- 18-917A – Student Harassment – Intimidation – Bullying
- 18-1507 – Definitions – Sexual Exploitation of a Child – Penalties
- 18-1514 – Obscene Materials – Definitions
- 18-2201 – Computer Crime – Definitions
- 18-2202 – Computer Crime
- 33-132 – Local School Boards – Internet Use Policy Required

Children’s Internet Protection Act, Sections 1703 to 1721, USC Section 254(h)(1)

Cowles Publishing Co. v Kootenai County Board of Commissioners, 144 Idaho 259 (2007)

ADOPTED: July 2008

AMENDED: December 2020