REDWOOD AREA SCHOOL DISTRICT #2897

Technology Policies and Procedures Handbook

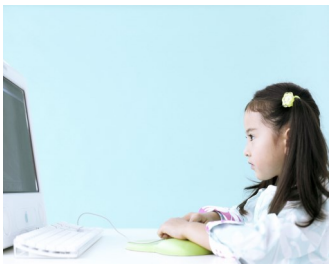
SUPPORT, CHALLENGE, LEARN, ACHIEVE

Updated August 1, 2021

Table of Contents

Policy #524- Technology and Internet Responsible Use and Safety Policy

I. PURPOSE



The purpose of this policy is to set forth policies and guidelines for access to the school district technology system and responsible and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district technology system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district technology system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district technology system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district's technology system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system

for classroom activities, educational research, professional or career development activities, and limited high-quality, self-discovery activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. RESPONSIBILITY OF USE

A. Users are prohibited from using school district system and Internet resources or accounts to access, review, upload, download, store, print, post, receive, transmit or distribute:

1. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
2. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;

3. materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process and will not post information or materials that could cause damage or danger of disruption to the educational process;

4. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination;

B. Users will not use the school district system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

C. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.

D. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware, or wiring or take any action to violate the school district system's security, and will not use the school district system in such a way as to disrupt the use of the system by other users.

E. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

F. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

1. This paragraph does not prohibit the posting of employee contact information on school district web pages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

2. Employees creating or posting school-related web pages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:

   a) Such information is classified by the school district as directory information, and verification is made that the school district has not received notice from a parent/guardian or eligible student that such information is not be designated as directory information in accordance with Policy 515; or

   b) Such information is not classified by the school district as directory information but

written consent for release of the information to be posted has been obtained from a parent/ guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

3. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about a user or another individual on networks such as "Facebook," "Twitter," "Instagram," "Snapchat," and "Reddit," and similar websites or applications.

G. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use school district accounts, access codes or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of appropriate school authorities.

H. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school technology device, and will not plagiarize works they find on the Internet.

I. Users will not use the school district system for the conduct of a business, for unauthorized commercial

purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the appropriate school district official.

J. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy (MSBA/MASA Model Policy 514). This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.

K. Student users are not allowed to use personal e-mail in the school district.

L. Users will not use the school district system for the purpose of personal message sending or internet chatting, nor may users post and build personal online websites.

M. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises school district system may also be in violation of this policy as well as other school district policies. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct including, not limited to, suspension or cancellation of the use or access to the school district technology system and the Internet and discipline under other appropriate

school district policies, including suspension, expulsion, exclusion, or termination of employment.

N. If a user inadvertently accesses unacceptable materials or unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

O. The school district reserves the right for each classroom advisor to establish additional expectations as it relates to use of technology in their classroom. Student users must follow these guidelines in addition to policies and procedures listed in the Technology Handbook.

VI. FILTER

A. With respect to any of its technology devices with Internet access, the School District will monitor the online activities of both minors and adults and employ technology protection measures during any use of such devices by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;
2. Child pornography; or
3. Harmful to minors

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

C. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

D. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

A. Use of the school district computer system and Internet uses shall be consistent with school district policies, including but not limited to those in the following areas:

1. The use of intellectual property.

2. Student Discipline. (Policy #506)

3. Curriculum Development. (Policy #603)

4. Instructional Curriculum. (Policy #604)

5. Textbooks and Instructional Materials. (Policy #606)
6. Technology access.
7. Protection and Privacy of Student Records. (Policy #515)
8. Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees. (Policy #505)
9. Interviews of Students by Outside Agencies. (Policy #519)
10. Student Disability Nondiscrimination. (Policy #521)
11. Student Sex Nondiscrimination. (Policy #522)
12. Bomb Threats. (Policy #804)
13. Distribution of Materials on School District Property by Nonschool Persons. (Policy #904)
14. Bring Your Own Device (BYOD) Policies and Procedures (Policy #524.1)

VIII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district technology system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the

search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of electronic files and e-mail files on any district sponsored network system such as local servers and cloud based systems. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act).

F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

IX. TECHNOLOGY USE AGREEMENT

A. The proper use of the Internet, the school district's technology resources, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and employees of the school district.

B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. <u>The Technology Use Agreement</u>

The Technology and Internet Responsible Use and Safety Policy, in its entirety, is provided for review to all users and parents or guardians through paper copy, school newsletter, the Technology Policies and Procedures Handbook, or the school district website.

The Technology Use Agreement from must be read and signed by the user, the parent or guardian, and the supervising teacher (High School – homeroom teacher, Middle School – first block teacher, or Elementary- homeroom teacher). The form must then be filed at the school office. In lieu of signing each individual student agreement, the supervising teacher will print a list of classroom students and sign the list to be filed at the school office.

Employee technology use agreements will be filed in the district office.

X. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on school district diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet.

XI. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Internet use.

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with school district policies.
2. Disclaimers limiting the school district's liability relative to:
    a. Information stored on school district diskettes, hard drives or servers.
    b. Information retrieved through school district computers, networks or online resources.
    c. Personal property used to access school district computers, networks or online resources.
    d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student or the student's parents.
6. Notification that the collections, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communica-

tions, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the school district's acceptable use policy, the student's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XII. PARENT/GUARDIAN RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents/Guardians are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents/Guardians will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.

2. A description of parent/guardian responsibilities.

3. A notification that the parents have the option to request alternative educational activities not re-

quiring Internet access and the material to exercise this option.

4. A statement that the Internet Use Agreement must be signed by the user the parent or guardian, and the supervising teacher prior to use by the student.

5. A statement that the school district's acceptable use policy is available for parental review.

XIII. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district's Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References:

15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)

Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969)
United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Kowalski v. Berkeley County Sch., 652 F.3d 565 (4th Cir. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References:

Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
Policy 406 (Public and Private Personnel Data)
Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
Policy 506 (Student Discipline)
Policy 514 (Bullying Prohibition Policy)
Policy 515 (Protection and Privacy of Pupil Records)
Policy 519 (Interviews of Students by Outside Agencies)
Policy 521 (Student Disability Nondiscrimination)
Policy 522 (Student Sex Nondiscrimination)
Policy 603 (Curriculum Development)
Policy 604 (Instructional Curriculum)
Policy 606 (Textbooks and Instructional Materials)
Policy 806 (Crisis Management Policy)
Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

Loss of User Privileges

Violations of the Technology and Internet Responsible Use and Safety Policy (#524), including any inappropriate or intentional damage caused to technology equipment at Redwood Area Schools, will result in the following Loss of User Privileges:

First Offense: Technology access is revoked for one week

Second Offense: Technology access is revoked for the remainder of the quarter

Third Offense: Technology access is revoked for the remainder of the semester/year

The listing of actions does not imply or require that all be used before a more severe consequence is imposed, nor does it imply that each action listed under disciplinary actions be imposed in each case.

In the case that a student needs to use a computer for class work, the teacher may allow use of a non-networked machine. In the case of research, he/she will have access to print materials available in the media center.

Enforcement of Consequences:

- The classroom advisor will notify the Technology Coordinator of the offense and consequence.
- The Technology Coordinator will remove user privileges and set up a non-networked machine if requested

by any of the student's classroom advisors. The Technology Coordinator will notify the student's principal and site level teachers of the offense and consequence.

- The student's principal will send a letter notifying parents/guardians of the revocation.

Policy 524.1 - Bring Your Own Device (BYOD) Policies and Procedures

I. PURPOSE

Area School District (RASD) provides wireless network access in each of its school buildings in order to provide students with 21st century learning opportunities. The purpose of this procedure is to establish clear guidelines and procedures to ensure the integrity of RASD's network. This BYOD policy applies, but is not limited to all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

A. Smartphones
B. Other mobile/cellular phones
C. Tablets
D. Portable media devices
E. PDAs
F. Netbooks
G. Laptop/notebook computers, including home desktops
H. Any personally-owned device capable of storing data and connecting to a network

The policy applies to any hardware and related software that is not organizationally owned or supplied, but could be used to access organizational resources or the internet. That is, devices users have acquired for personal use but also wish to use in the school environment.

II. DEFINITION OF USERS

The term user in the proceeding information is considered any student, employee or guest of Redwood Area School District who

brings a personal device to use on RASD campuses or in RASD buildings.

III. TECHNICAL REQUIREMENTS

A. Where applicable, each electronic device must have unexpired and functioning antivirus protection installed.

B. Each device must have wireless capability to access the Internet. Connecting to the network with Ethernet cables is not permitted by the school district.

IV. GUIDELINES FOR USE OF PERSONAL DEVICES

A. Student users must understand that the use of a personal device in the classroom is for instructional use only and at the advisor's discretion. Users must have permission from the classroom advisor to use a personal device in the classroom.

B. Use of personal devices in the classroom must support instructional activities.

C. Users must power off and put away personal devices if directed to do so by RASD staff.

D. Users must ensure that their personal device does not disrupt the learning of others. For example, audio should be muted unless directed otherwise by instructional staff.

E. Users may use their personal device in supervised public areas only, such as in the media center under a staff member's supervision.

F. Users must abide by the Redwood Area School District's Technology and Internet Responsible Use and Safety Policy when using personal devices. (Policy # 524)

G. Users are not allowed to access any network resources other than the Internet.

H. Users are responsible for the use of their personal device at all times.

I. Users should practice caution when allowing others to access their personal device.

V. STUDENT USERS FAILING TO COMPLY WITH THE ABOVE GUIDELINES WILL RECEIVE THE FOLLOWING CONSEQUENCES:

A. 1st Offense: Personal device will be confiscated and placed in the office where the student may retrieve it at the end of the day.

B. 2nd Offense: Personal device will be confiscated for 1 to 5 school days, based on the nature of the offense and principal's discretion. The student will be required to turn in the personal device to the office at the beginning of each school day and the student may retrieve it at the end of each school day. The parent will be notified by the site level principal.

C. 3rd Offense: Personal device will be confiscated for 5 school days. The student will be required to turn in the personal device to the office at the beginning of each school day and the student may retrieve it at the end of each school day. A parent conference will be held with the site level principal.

D. Violations that will result in the immediate and permanent loss of access or suspension:

1. Accessing websites of a pornographic, sexual, illegal nature or other websites considered inappropriate under Redwood Area School District policies.

2. Activity involving cyber-bullying or harassment of another user or group of users.

3. Activity of a malicious and/or illegal intent.

4. Failure to surrender a device to a staff member upon request may result in suspension.

Any other violations and misuses of a personal device on school grounds will be subject to established discipline policies and procedures.

VI. DISCLAIMERS

A. Wireless access is available for the Internet only. Users of personal devices will not be granted access to other network resources such as school-system owned software and hardware devices including printers.

In addition, Redwood Area School District's technology department personnel are not permitted under Minnesota State law to provide technical support for personal devices.

B. No work orders may be submitted to the technology department for personal devices, nor does the school system provide any technical support for these devices. Support and technical assistance is the sole responsibility of the user.

C. No charging stations for personal devices will be available.

Redwood Area School District assumes no responsibility for malfunction, damage, theft, or loss of personal devices used on any of school campuses or in any of its school buildings, including confiscated devices.

Chromebooks

Redwood Area Schools provides all students in grades 2-12 a Chromebook for educational use in school. These devices are provided for students to carry with them throughout the school day. Students in grades 5-12 may also take them home. This document provides students and their parents/guardians with information about the general use of technology, ownership of the devices, rights and responsibilities for possession of the device, educational use, care of the Chromebook and being a good digital citizen.

Ownership

The Redwood Area School District retains sole right of possession of the Chromebook. The Redwood Area School District lends the Chromebook to the students for educational purposes only for the academic year. Additionally, the Redwood Area School District administrative staff and faculty retain the right to collect and/or inspect Chromebooks at any time, including via electronic remote access and to alter, add or delete installed software or hardware.

Rights and Responsibilities

- The students are solely responsible for any apps or extensions on their Chromebooks that are not installed by a member of the Redwood Area School District technology staff or teaching staff. Students are responsible for backing up their data to protect from loss. Users of School Technology have no rights, ownership, or expectations of privacy to any data that is, or was, stored on the Chromebook, school network, or any school

-issued applications and are given no guarantees that data will be retained or destroyed.

- Students may not use or install any operating system on their Chromebook other than the current version of ChromeOS that is supported and managed by the school.
- The Chromebook operating system, ChromeOS, updates itself automatically. Students do not need to manually update their Chromebooks.
- Chromebooks use the principle of "defense in depth" to provide multiple layers of protection against viruses and malware, including data encryption and verified boot. There is no need for additional virus protection.
- The school utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Chromebooks will have all Internet activity protected and monitored by the school while on campus. If an educationally valuable site is blocked, students should contact their teachers to request the site be unblocked. Parents/guardians are responsible for filtering and monitoring any internet connection students receive that is not provided by the school.
- Chromebooks seamlessly integrate with the Google Apps for Education suite of productivity and collaboration tools. This suite includes Google Docs, Sheets, Slides, Drawings, and Forms. All work is stored in the cloud.
- Students are restricted from installing Chrome web apps and extensions from the Chrome Web Store.
- The school will maintain a log of all Chromebooks that includes the Chromebook serial number, asset tag code, and name and ID number of the student assigned to the device.

- Each student will be assigned the same Chromebook for the duration of his/her time at Redwood Area Schools. Take good care of it!

Repairing/Replacing Your Chromebook

- Chromebooks include a one year hardware warranty from the vendor. The vendor warrants the Chromebook from defects in materials and workmanship. The limited warranty covers normal use, mechanical breakdown, and faulty construction. The vendor will provide normal replacement parts necessary to repair the Chromebook or, if required, a Chromebook replacement. The vendor warranty does not warrant against damage caused by misuse, abuse, or accidents.
- There are no fees associated with student use of the Chromebook. Each Chromebook will be replaced after 4 years. Redwood Area Schools will provide device support when necessary. A penalty could be assessed if purposeful damage is made to the device.

Chromebook Incident Procedure

- Students must pay a $20 fee for the first accidental case of damages, and full price for any subsequent damages. Students will not receive their repaired Chromebook back until this has been paid. Students may use Chromebooks available in each classroom until then. Site principals reserve the right to waive the $20 fee and assess full costs for damages if they determine it necessary.
- Student Discipline: If a student violates any part of this policy, the following disciplinary steps may be followed:
    a. Detention
    b. Loss of Privilege of Taking Device Home (Device will be checked out at the beginning of each day and returned at the end of school)
    c. In-School Suspension

d. Out-Of-School Suspension

e. Notification of Parents

- Estimated Costs (subject to change)
  - ◊ Replacement - $250 - $300
  - ◊ Screen - $20 for non-touchscreens, $80 for touchscreens
  - ◊ Keyboard - $25
  - ◊ Power cord - $20
  - ◊ Case - $20

No Expectation of Privacy

- Students have no expectation of confidentiality or privacy with respect to any usage of a Chromebook, regardless of whether that use is for school-related or personal purposes, other than as specifically provided by law. The school may, without prior notice or consent, log, supervise, access, view, monitor, and record use of student Chromebooks at any time for any reason related to the operation of the school. By using a Chromebook, students agree to such access, monitoring, and recording of their use.
- Teachers, school administrators, and the technology department staff may use monitoring software that allows them to view the screens and activity on student Chromebooks.

Student Google Apps Account

Redwood Area Schools is providing students the opportunity to obtain a school monitored and maintained Google Apps for Education account. These accounts are made available in order to collaborate with teachers and other students and are offered to students for curriculum use only. A Google Apps student account will be established at the request of the students' classroom teachers.

Overview of Google apps for Education:

- **Google Apps** is a collection of free online applications. These applications do not reside on the computer, itself, but rather they are accessed through a web browser. This is considered working in the "cloud". The benefit of this structure allows flexibility in accessing documents and projects from ANY computer with Internet access. Staff and students can access their school documents from the lab, the classroom, the public library and even from home!
- **Google Apps for Education** is a special setup of the popular Google Apps, tailored specifically for educational institutions. For example, accounts are managed by the school district (and not by Google) and advertisements are all turned off. Google Apps for Education allows school districts to carve off a special Google domain/area for their staff and students to create, collaborate and share ideas online between each other, as well as provide the framework for sharing across districts.
- **Students need to know:** Students will follow school policies for appropriate use when using Internet based services like Web 2.0 applications & Google Apps. These services are considered an extension of the school's network. Students

have no expectation of privacy in their use as school and service administrators have the right and ability to monitor user accounts for policy and security enforcement.

- **Parents need to know:** The Technology and Internet Responsible Use and Safety Policy will be enforced. School staff will monitor student use of applications when students are at school. Parents are responsible for monitoring their child's use of applications when accessing programs from home. Students are responsible for their own behavior at all times.

Cyber Safety and FCC Ruling

Under FCC ruling, school districts are required to educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

Cyber safety and bullying videos are presented at least once per year to all students. During this time, teachers initiate discussion related to cyber safety and students are given the opportunity to learn and ask questions.

Cyber safety and bullying facts:

1. Nearly 43% of kids have been bullied online. 1 in 4 has had it happen more than once.
2. 70% of students report seeing frequent bullying online.
3. Over 80% of teens use a cell phone regularly, making it the most common medium for cyber bullying.
4. 68% of teens agree that cyber bullying is a serious problem.
5. 81% of young people think bullying online is easier to get away with than bullying in person.
6. 90% of teens who have seen social-media bullying say they have ignored it. 84% have seen others tell cyber bullies to stop.
7. Only 1 in 10 victims will inform a parent or trusted adult of their abuse.
8. Girls are about twice as likely as boys to be victims and perpetrators of cyber bullying.

9. About 58% of kids admit someone has said mean or hurtful things to them online. More than 4 out 10 say it has happened more than once.
10. About 75% have visited a website bashing another student.
11. Bullying victims are 2 to 9 times more likely to consider committing suicide.

Visit our school website to access information on common sense use of the internet and what you as a parent/guardian can do to keep your child safe online. The Cyber Safety link can be found on the District->Technology Home page.

Redwood Area Schools
Technology Use Agreement - Employee

SCHOOL DISTRICT EMPLOYEE

I have read and do understand the school district policies relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by them. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print):

_____

User's Signature:

_____

Date:

_____

Redwood Area Schools
Technology Use Agreement—Student

STUDENT

I have read and do understand the school district technology policies and agree to comply with all the rules. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print)_____

User's Signature:_____

Date:_____

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the school district technology policies and understand that this access is designed for educational purposes. I understand that accounts for my child are established for school network access and Google Apps for Education. I certify that the information contained on this form is correct. The school district has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the school district or its employees or agents to be responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting.

Parent or Guardian's Name (please print):_____

Parent or Guardian's Signature:_____

Date:_____

Your child may have his/her classroom work, projects, photos, classes and name posted on the internet or in school publications during the course of the school year. If you wish to limit this for your child, please request and complete the designated form from the school office.

SUPERVISING TEACHER
(High School – homeroom teacher, Middle School – first block teacher, or Elementary – homeroom teacher)

I have read the school district policies relating to technology and Internet safety use and agree to promote these policies with the student. Because the student may use the Internet on the school district technology system for individual work or in the context of another class, I cannot be held responsible for the student's use of the Internet or network. As the supervising teacher, I do agree to instruct the student on responsible use of the Internet and network and proper network etiquette.

Teacher's Name (please print):_____

Teacher's Signature:_____

Date:_____