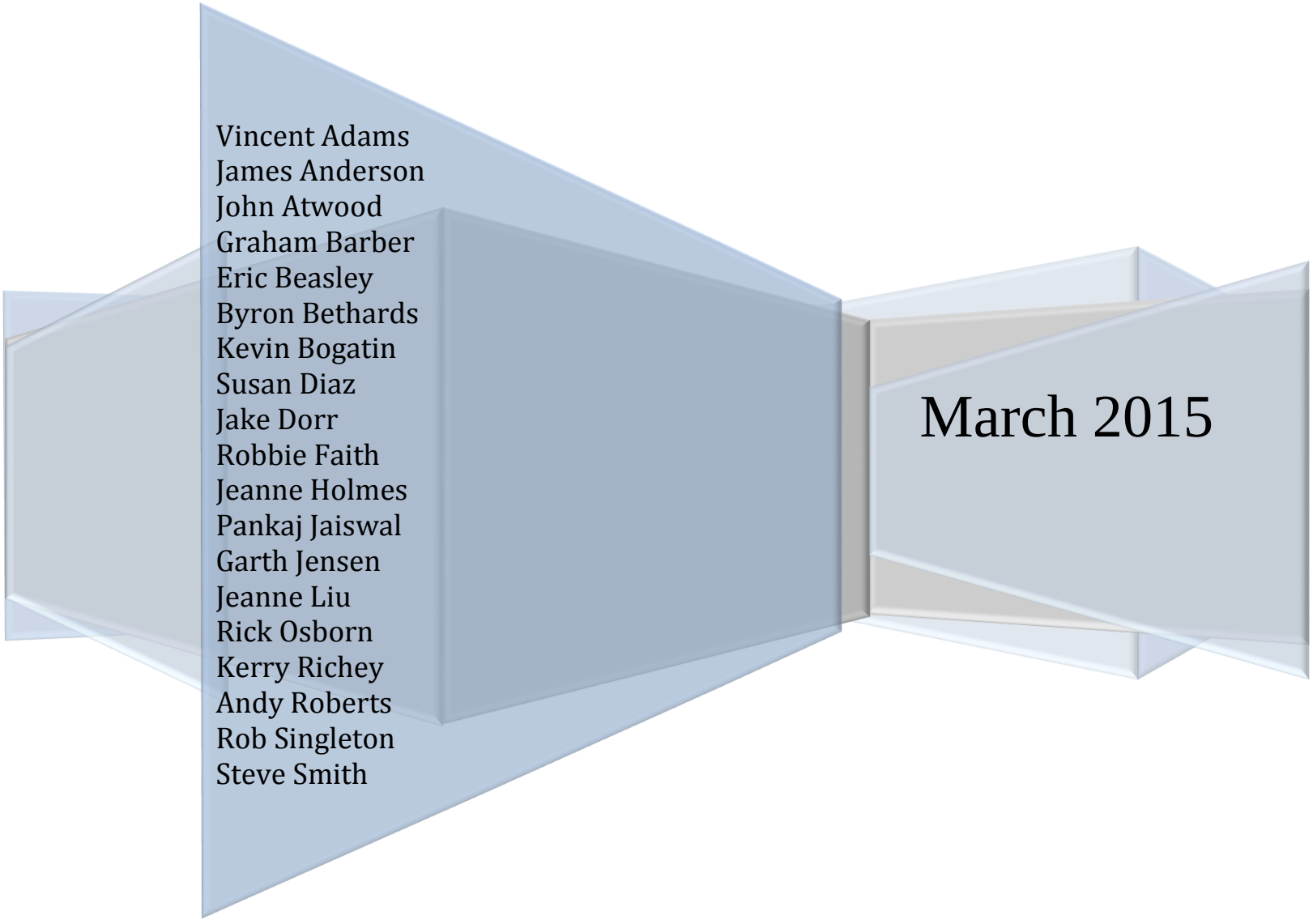
Superintendent's Technology Advisory Committee (TAC)



Vincent Adams
James Anderson
John Atwood
Graham Barber
Eric Beasley
Byron Bethards
Kevin Bogatin
Susan Diaz
Jake Dorr
Robbie Faith
Jeanne Holmes
Pankaj Jaiswal
Garth Jensen
Jeanne Liu
Rick Osborn
Kerry Richey
Andy Roberts
Rob Singleton
Steve Smith

March 2015

Background

The Technology Advisory Committee (TAC) was formed in fall 2014 with the charge of advising the superintendent on technology-related issues that impact students, teachers, support staff, and families. The group began meeting in early October, and completed this first round of recommendations on February 18, 2015.

After immersing in background information regarding 509J's technology initiative and current areas of concern, TAC formed three subcommittees to address issues in the following areas:

- Health/Communication
- Parental Controls/Internet Filter
- Language and Vocabulary/Policy

Each subcommittee met and developed recommendations that were brought to the larger group for discussion and approval. The recommendations were based on current research, authoritative best practices, and the expertise of members of TAC. This document represents the first phase of TAC's work.

As requested by the Superintendent, TAC also developed recommendations for Phase IV 1:World implementation. In the future, TAC will bring additional recommendations, including a plan for 1:World program evaluation.

Phase IV 1: World Implementation Recommendations

High School—Full implementation as quickly as infrastructure will allow.
Increase technology support proportionately to the number of devices. Create a staffed help desk with inclusion of student support as part of the technology support plan. The high schools should decide which devices are appropriate at their level, with input from TAC. Engage high school principals in planning and providing strong leadership and support during the implementation process.

Rationale:

- Implementation should occur as quickly as possible to:
    - Provide continuity for incoming 9th graders who have used one-to-one devices through their middle school years;
    - Address the pressing equity issue for students without access to personal devices;
    - Provide more effective instruction to students with special learning needs;
    - Provide all teachers access to technology as a teaching tool;
    - Ensure that students have the technology skills they need for college; and
    - Make technology tools and technology-based learning available to all students in all classrooms at the high school level.
- For full implementation to be effective, adequate infrastructure needs to be in place. Infrastructure includes building wiring, technology support (technical and instructional) and professional development.
- As demonstrated at the middle school level, building leadership is essential for effective implementation.

Elementary—Full implementation grades K-5 at Lincoln and Garfield Schools and at other schools, grades 3-5, as quickly as infrastructure will allow. Consider mid-year implementation where possible.
Generally, at the elementary level use should be cart-based, with some home use as deemed appropriate by building administrators, teachers, and families. The Committee recognizes the budget restraints and it may only be possible to implement at 5th grade, but recommends going as deep as possible toward third grade.

Rationale:

- Implementation in grades 3-5 should occur as quickly as possible to
    - Promote digital literacy at an earlier age;
    - Address the pressing equity issue that we have students without access to personal devices;
    - Provide more effective instruction to students with special learning needs; and
    - Prepare students for device use at the middle school level.
- In grades 3-5 the use of devices changes and learning includes an increasing amount of content production by students.
- Device use in grades 3-5 allows for more collaboration among teachers.
- Full accessibility to devices at Lincoln and Garfield will support the implementation of the new dual immersion curriculum.

TAC will make a recommendation in the future regarding implementation in the remaining K-2 classrooms in the district. More discussion needs to occur at the school and district levels regarding how the devices are most appropriately used at this level, and how to address parent concerns about health and safety for young children.

Summary of Additional Recommendations

The implementation of a one-to-one device changes the scope of traditional technology implementation in schools. Historically, computer devices have been limited to lab time or checked out for limited durations of time. However, in the new paradigm of one-to-one implementation, students have access to the device throughout the day, and in many cases at home as well. While this can serve to give new and greater learning opportunities, there are potential areas of concern that need to be addressed. The following recommendations are designed to help address issues that have been identified in initial phases of 1:World implementation.

Health
The Health Subcommittee focused on six potential areas of concern:

- Wireless (Wi-Fi) Radiation
- Screen Time (socialization, behavioral, and general health)
- Vision (prolonged reading on illuminated devices)
- Ergonomics
- Sleep

Recommendation 1: Develop a training curriculum for students and staff that addresses the health concerns outlined above. The training curriculum should incorporate current research and best practices, and be made available to staff, students and parents. While staff and students should be

the primary audience, parents should have access to the same information through fliers, website, and other means. (See appendix, page 6 for more details regarding curriculum and supporting research.)

Recommendation 2: Make tools available to encourage healthy use of electronic devices. A suite of tools should be made available to staff, students, and parents that includes:

- Device usage reporting application: delivering usage information to parents
- Eye-break application
- Deactivation of Wi-Fi when screen is unlit
- Access to ergonomic accessories

These tools have been selected as low-cost, high impact means to foster the appropriate and safe use of electronic devices, to establish good technology habits, and to educate students in these areas, all key 21st Century skills.

Communication/Language

The goal of the communication recommendations is to increase the frequency and enhance the communication of the 1:World initiative by:

- Distributing clear and consistent messages articulating district mission, vision, and goals of 1:World;
- Fostering a culture of transparent communications as viewed by internal and external audiences;
- Providing the resources that the 1:World program and services offer and making them accessible to all students, staff members, and parents;
- Simplifying student, staff, and parent access to FAQs.

The audience for these recommendations includes students, staff, parents, community members, and school colleagues.

Recommendation 1: Make a 1:World link prominent and understandable on the district homepage.

Recommendation 2: Redesign and reorganize the 1:World website. Include:

- Page for tips and tricks for technology use at home
- Clearly defined and easy to read 1:World objectives
- Prominent display of video/slideshow of technology in use at school
- Links to policy with brief explanations
- Forms page—all forms accessible, with detailed description and downloadable
- Vocabulary page of frequently used terms—with a searchable glossary
- Page for staff members with resources
- Lesson ideas
- Technology tips
- Classroom management tips
- Sample lesson videos
- Student project examples
- Updated and clearly organized frequently-asked questions (FAQ) section that is searchable
- Page of links to curriculum, standards, and integration of 21st century skills
- Page for “in process” what’s going on now? Where are we?

- Page of newsletters and presentations
- Contact information—communication flowchart and staff listing (who does what)
- Page of links to research, including student and staff video "testimonials"
- Page for training information and professional development schedule for staff
- Page for help—fix-it-yourself help tips
- Use the Vancouver Public Schools website as a template and for ideas: http://portalsso.vansd.org/portal/page/portal/VSD_Home_Public/VPS_Parent_and_Families/VPS%20weLearn%2011

Recommendation 3: Provide training information for staff members on policy and health considerations.

Recommendation 4: Add technology-related policy to annual review.

Recommendation 5: Include policy in parent, staff, and student handbooks.

Recommendation 6: Create a technology listserv—monthly newsletter (Tech Bytes); include this in the district office Communiqué.

Recommendation 7: Regularly present goals, vision, and status of 1:World at staff meetings.

Recommendation 8: Send quarterly blurbs to schools for publications in newsletters with a link to join technology listerv.

Recommendation 9: Continue parent information nights and include updates, progress, teacher demonstrations, and survey data.

Recommendation 10: Use the Vancouver School District website as an example for what information to use and share.

Parental Controls/Internet Filter

Recommendation 1: Adopt the following set of principles on which to base future decisions regarding parental controls and internet safety:

- Responsibility for keeping students secure is a partnership between parents and the school district.
- Security should be evaluated based on grade level appropriateness, and should reflect the philosophy that privilege comes with responsibility. At the high school level, security should be set at the Child Internet Protection Act (CIPA) or other applicable regulation minimum. At the middle school level, technology access should consider this unique developmental stage by balancing opportunities to pursue digital resources while providing guidance and restrictions as appropriate. Middle school should be between elementary school and high school in terms of restrictions. The school principal, in collaboration with site input, should recommend the default level of restrictions per school. This allows the school to differentiate access as appropriate. At the K-5 level, access should be more limited.
- Decisions on security level should be a balance between safety, access, and cost (money and staff time).
- Security decisions should consider the impact on access for families that have only school devices.

- When devices are at home, give parents control over content and time to the limits that are logistically and administratively possible.
- The district should provide training and resources to parents on how to limit screen time and access (e.g., pamphlets, curriculum nights, web-based newsletters).
- The district should provide a way for parents to easily share security strategies. Security is a combination of technology solutions and parental decisions.
- Teachers should have knowledge of policies, decisions, and what internet filters are doing at different levels of grades and how and what can be controlled by teachers on individual devices.

Recommendation 2: The school district should develop an opt-out policy/procedure that allows parents to request an opt-out of location services. This should include education for parents and students regarding how the school district is using location services.

Recommendation 3: The school district should perform periodic privacy audits that evaluate the ability of vendors to collect personal data of students. This is especially important with new apps. The Consortium of School Networking (CoSN), a national association of school district chief technology officers, recently developed a set of security questions to help schools evaluate companies' security practices. CoSN recommends that schools ask these security questions before they sign purchase agreements with technology vendors.
http://www.cosn.org/sites/default/files/03_SecurityQuestions.pdf (See appendix, page 24 for CoSN security questions.)

Policy
Recent state legislation created new provisions and amending statutes to encourage school boards and districts to have thoughtful conversations about how technology is utilized in schools, and how to make better educational use of all computers, tablets, and other electronic devices. Also, districts implementing curriculum that integrates technology are now required to grant access to these materials free of charge.

TAC reviewed district policies and administrative regulations related to technology use in the district, and is recommending revisions. These recommended changes also were reviewed by human resources, technology, and instructional staff, and were sent to the School Board Policy Review Committee on January16 with the goal of moving them forward for Board approval in March. (See appendix, page 27 to view recommended revisions.)

Recommendation 1: Significant revisions are recommended for Board Policy GCAB-Personal Communication Devices and Social Media-Staff to bring the policy in compliance with House Bill 2426.

Recommendation 2: Minor revisions are recommended in these policies to streamline language, update terminology, and clarify content:
- Board Policy II/IIA-Instructional Resources/Instructional Materials
- Administrative Regulation IIBGA-AR-Electronic Communications System
- Administrative Regulation IIBGB-AR-Web-Page Guidelines
- Board Policy JFCEB-Personal Electronic Devices and Social Media-Student
- Administrative Regulation JFCEB-AR-Personal Electronic Devices and Social Media

Appendix

Superintendent's Technology Advisory Committee

Health Subcommittee

Minimizing Health Impacts of One-to-One Device Implementation—*Executive Summary*

The implementation of a one-to-one device changes the scope of traditional technology implementation in schools. Historically computer devices have been limited to lab time or checked out for limited durations of time. However in the new paradigm of one-to-one implementations, students have access to the device throughout the day, and in many cases at home as well. While this can serve to give new and greater learning opportunities, there are potentially health considerations to consider and be aware of.

We focused on six potential areas of health concern of tablet and laptop devices for children, and reviewed current research and authoritative recommendations for these areas.

- Wireless (Wi-Fi) Radiation
- Screen Time (socialization, behavioral, and general health)
- Vision (prolonged reading on illuminated devices)
- Ergonomics
- Sleep

Based on existing research and authoritative best practice materials, our recommendations include two key means to address and mitigate health issues: development of a training curriculum, and making tools available to encourage healthy use of the devices.

A training curriculum should incorporate current research and best practices to address the health concerns outline above, and made available to teachers, students, and parents. Teachers and students should be the primary audience when developing the curriculum, but parents should similarly have access to information through flier, website, or other means.

Just as important, a suite of tools to encourage healthy use of the device should be made available to students, teachers, and parents. Such tools include:

- Device usage reporting application: delivering usage information to parents
- Eye-break application
- Deactivation of Wi-Fi when screen is unlit
- Access to ergonomic accessories

These tools have been selected as low-cost, high impact means to foster the appropriate and safe usage of the device, establish good technology habits, and educate students on these areas, a key aspect of 21st century skills.

Minimizing Health Impacts of One-to-One Device Implementation—*Full Document*

Introduction

The goal of this paper is to discuss and document the research that has been conducted surrounding health impacts of technology in education, especially in regards to a one-to-one implementation. Based on our findings, we will make recommendations on how to address and minimize the potential impacts of these concerns.

We've focused on reviewing six areas of concern of tablet and laptop devices for children:

- Wireless (Wi-Fi) Radiation
- Screen Time (socialization, behavioral, and general health)
- Vision (prolonged reading on illuminated devices)
- Ergonomics
- Sleep

With physical development and growth being a major factor in health, our research and recommendations have split these groups into the following segments. We feel it is important to differentiate the different age groups we are discussing.

- Kindergarten to 2nd Grade (5 to 9 years old)
- 3rd to 5th Grade (9 to 12 years old)
- 6th to 8th Grade (12 to 14 years old)
- 9th to 12th Grade (14 to 19 years old)

American Academy of Pediatrics (AAP) Internet Safety Recommendations
http://safetynet.aap.org/internet.pdf

Wireless (Wi-Fi) Radiation

Concern

The proliferation of wireless devices in schools will expose children to excessive amounts of radiation.

Research Summary

Wireless technology, such as that used in laptops and tablets, utilizes low frequency, non-ionized electromagnetic fields as the means to transfer data. There is currently no definitive research that correlates these wireless technologies to health issues, however the proximity and quantity of wireless transmitters in relation to their users has been called out as a potential risk. The World Health Organization currently classifies radiofrequency electromagnetic fields as "possibly carcinogenic to humans."

IARC Monographs—Classifications
http://monographs.iarc.fr/ENG/Classification/ClassificationsAlphaOrder.pdf

Public health implications of wireless technologies
Cindy Sage, David O. Carpenter
Pathophysiology , Volume 16 , Issue 2 , 233 - 246
http://dx.doi.org/10.1016/j.pathophys.2009.01.011
Mobile phone use and brain tumors in children and adolescents: a multicenter case-control study
http://www.ncbi.nlm.nih.gov/pubmed/21795665
Electromagnetic fields (EMF)
http://www.who.int/peh-emf/en/
The precautionary principle: protecting public health, the environment and the future of our children
http://www.euro.who.int/
data/assets/pdf_file/0003/91173/E83079.pdf

Screen Time

Issues / Concerns
Children issued their own 1-to-1 device will increase their overall screen time, leading to adverse social, behavioral, and cognitive issues. Giving students their own devices in class or out of school will make it difficult for parents to monitor screen time.

Research
Screen time has been linked to a number of health maladies, including cardiovascular disease, obesity, and asthma. The American Association of Pediatrics recommends limiting screen time and offering educational media and non-electronic formats such as books, newspapers and board games. They also advocate that parents establish "screen free" zones at home by making sure there are no televisions, computers or video games in children's bedrooms.

http://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Pages/Media-and-Childre n.aspx
http://psycnet.apa.org/journals/edu/94/1/145.html
Kids' 'screen time' linked to early markers for cardiovascular disease.
http://www.sciencenewsline.com/articles/2011042113000023.html
Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues
http://www.sciencedirect.com/science/article/pii/S0747563214003227
High Screen Time Is Associated with Asthma in Overweight Manitoba Youth.
http://www.ncbi.nlm.nih.gov/pubmed/23033847
Association between TV viewing, computer use and overweight, determinants and competing activities of screen time in 4- to 13-year-old children.
http://www.ncbi.nlm.nih.gov/pubmed/22158265

Eyesight

Concern
If tablets or laptops are used to replace hard copy textbooks, prolonged use could result in short-term and long-term eye problems for students.

Research

Computer Vision Syndrome is a set of eye and vision related problems experienced among frequent computer users. Symptoms may include:

- Dry eyes
- Blurred Vision
- Fatigue
- Headaches
- Neck, back and shoulder pain

Because of the way children use computers, these symptoms can make children particularly susceptible. Children have a lower degree of self-awareness and often do not notice discomfort and other symptoms associated with prolonged computer use.

The most effective means to prevent these problems is to limit the use of devices. Several articles recommend taking frequent breaks, such as the 20/20/20 rule, which is for every 20 minutes a user must look away at 20 feet for at least 20 seconds.

Of the articles and research reviewed, we found no conclusive information regarding eye problems and long-term effects of prolonged use of reading from illuminated devices. However, computer use can exacerbate existing conditions, making identification of eye problems more important for children using a computer frequently.

Tips for computer vision syndrome relief and prevention
http://iospress.metapress.com/content/r734u1l877233722/fulltext.pdf
Impact of computer use on children's vision
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2776336/
Factors leading to the Computer Vision Syndrome: an issue at the contemporary workplace.
http://www.ncbi.nlm.nih.gov/pubmed/15580914
Blink patterns: reading from a computer screen versus hard copy.
http://www.ncbi.nlm.nih.gov/pubmed/24413278
Reading from electronic devices versus hardcopy text.
http://www.ncbi.nlm.nih.gov/pubmed/24284668
A comparison of symptoms after viewing text on a computer screen and hardcopy.
http://www.ncbi.nlm.nih.gov/pubmed/21197801
Study of preferred background luminance in watching computer screen in children
http://www.ncbi.nlm.nih.gov/pubmed/24890155
Visual problems in young adults due to computer use.
http://www.ncbi.nlm.nih.gov/pubmed/22496007

Ergonomics

Concern

Poor ergonomics when reading or utilizing a tablet or laptop device could result in chronic pain over time.

Research
Research does support that prolonged use of a tablet, in combination with poor ergonomics can cause chronic pain.
http://www.hsph.harvard.edu/news/features/ipad-ergonomics-dennerlein/
Touch-screen tablet user configurations and case-supported tilt affect head and neck flexion angles
http://iospress.metapress.com/content/x668002xv6211041/fulltext.pdf
https://www.ucl.ac.uk/uclic/studying/taught-courses/distinction-projects/2011_theses/Stawarz_2011

Sleep Impacts

Concern
Use of computer devices, particularly at night, could impact the amount and quality of sleep students are getting.

Research
We have identified two different reasons why student sleep patterns might be affected by tablet or laptop use at home.

- Reduced melatonin levels
- Increased anxiety and stress levels

Research suggests that exposure to self-luminous displays for a duration of two hours or more can have a measurable effect on melatonin levels. Less time was not found to have a statistically significant impact. The other potential impact on sleep is that the tasks that students are conducting on the device before going to bed may be alerting or stressful stimuli. This can lead to sleep disruption. Academic performance has been directly related to sleep time and inversely related to overall sedentary screen media usage in some studies.

Research indicates that reading on devices that emit blue light can cause increased time to fall asleep, are less sleepy in the evening, and spend less time in REM sleep. Similarly, users have been found to be sleepier and less alert the following morning than those using traditional media. Research has also linked chronic suppression of melatonin secretion by nocturnal light exposure with an increased risk of breast cancer, colorectal cancer and prostate cancer.

http://www.sciencedirect.com/science/article/pii/S0003687012001159
http://www.brighamandwomens.org/about_bwh/publicaffairs/news/pressreleases/PressReleas e.aspx?sub=0&PageID=1962

Recommendations
Our recommendations include two parts that look to address and mitigate health issues in these six areas:

- Development of technology training curriculum that includes health impacts
- Providing tools to encourage healthy device usage habits

Technology Curriculum
Getting teachers, students, and parents the information on ways that technology can affect health is an important piece of a holistic 1-to-1 technology implementation. Many people are not aware of health impacts, and education is a key means of informing and mitigating potential issues. Training should be targeted to the following groups:

- Teachers
- Students
- Parents

Student curriculum should be adjusted to fit the student's grade level and the expected interactions with the devices. For example, if the device will be brought home, sleep impacts and screen time should be addressed. Older students, who are likely to be reading for long periods of time, should be aware of the impacts to reading for long periods.

It is recommended that this training be conducted before, or upon the issuing of one-to-one devices. A curriculum might look at the following, but not limited to:

- Internet safety
  - Personal information
  - Cyber bullying
  - Impacts of social media
  - Online searching
- Screen time
- Sleep impacts
- Ergonomics

Based on the American Pediatrics Association recommendations:
http://pediatrics.aappublications.org/content/126/5/1012.full

Parent Engagement and Training
Classes or information sheets informing parents of:

- What pieces of the curriculum are being done on tablets and computers
- How to watch for cyber bullying
- Social media education and training
- Health risks associated with technology use, and how they are being mitigated

Healthy Usage Tools
In addition to training, we recommend that a suite of tools be made available to students, teachers, and parents to encourage and foster healthy utilization of technology. We believe these are low-cost, high impact steps that address many of the concerns we've outlined above.

Device Usage Reporting
The introduction of 1-to-1 devices can make it difficult for parents to monitor their children's screen time, application usage, and time of day usage. We recommend that an application be installed to monitor screen time, applications used, and time of day usage. Parents would be able to opt into an automated monitoring report which would be made available to them on via email on a daily, weekly, or monthly basis. The report would allow parents to make

adjustments in at-home screen time based on the report, identify high usage, and be a way to help discussion of appropriate usage of the device.
Addresses: Screen time, sleep impacts

Turn off Wi-Fi when Screen Becomes Unlit
Impacts of Wi-Fi radiation upon health are controversial. Even without any definitive proof of a connection between Wi-Fi exposure and cancer, a significant public perception exists, and has yet to be satisfied. To address this concern, we recommend reducing unnecessary Wi-Fi exposure.
Addresses: Wi-Fi radiation

Eye Break Application
By default an unobtrusive 'eye break' application should be utilized to indicate when a break should be taken, as determined by extended periods of time with the display illuminated. This can serve as a reminder to take frequent breaks, particularly for those reading textbooks. Older students should have the option to disable this app.
Addresses: Vision impacts, ergonomics

External Keyboards and Tablet Stands
Addresses: Ergonomics

Conclusion

Educating students, staff, and parents about the healthy use of technology will help bring awareness not only to the importance of their school-issued device, but also to their own personal devices and technology habits. This should allow students and parents to make informed decisions to improve student health, and therefore improve student achievement. It is important that the proper tools are provided to help students.

This is by no means an exhaustive list, but is a reasonable starting point for the Corvallis School District to address health concerns that have been raised by parents and community members. We believe that implementation of these recommendations will show a good-faith effort to address concerns.

Superintendent's Technology Advisory Committee
Communication Subcommittee

Goal: Increase the frequency and enhance the communication of the 1:World initiative by:

- Distributing clear and consistent messages articulating district mission, vision, and goals of 1:World;
- Fostering a culture of transparent communications as viewed by internal and external audiences;
- Providing the resources that the 1:World program and services offer and making them accessible to all students, staff member, and parents;
- Simplifying student, staff, and parent access to FAQs

Audience: Students, Staff, Parents, Community Members, School Colleagues

Recommendations:

1. Make 1:World link prominent and understandable on District homepage
2. Redesign and reorganization of the 1:World website to include:
    - Page for tips and tricks for tech use at home
    - Clearly defined and easy to read 1:World Objectives
    - Prominent display of Video/Slideshow of technology in use at school
    - Links for policy with brief explanations
    - Forms page – all forms accessible, with detailed description and downloadable
    - Vocabulary page of frequently used terms – with a searchable glossary
    - Page for staff members with resources
        - Lesson ideas
        - Tech tips
        - Classroom management tips
        - Sample lesson videos
        - Student project examples
    - Updated, clearly formatted, and organized FAQ section that is searchable
    - Page of links to curriculum, standards, and integration of 21st century skills
    - Page for "in process" what's going on now? Where are we?
    - Page of newsletters and presentations
    - Contact information – communication flowchart and staff listing (who does what)
    - Page of links to research, including student and staff video "testimonial"
    - Page for training information and professional development schedule for staff
    - Page for help – fix it yourself help tips

Use this as a template and for ideas for the website:
http://portalsso.vansd.org/portal/page/portal/VSD_Home_Public/VPS_Parent_and_Families/VPS%20weLearn%2011

3. Training information for staff members on policy and health considerations
4. Policy added to annual review
5. Policy added in parent handbook, staff handbook, student handbook
6. Creation of a tech listserv – Monthly newsletter (Tech Bytes, etc.) Include this with the DO communique
7. Presentations of goals, vision and status of 1:World at all staff meetings
8. Quarterly blurbs sent to schools for newsletters with link to join tech listerv
9. Continuation of parent info nights – updates, progress, teacher demonstrations, survey data
10. Use the Vancouver SD site as an example on what information to use and share: http://portalsso.vansd.org/portal/page/portal/VSD_Home_Public/VPS_Parent_and_Families/VPS%20weLearn%2011

CORVALLIS EDUCATION TECHNOLOGY VOCABULARY/GLOSSARY
—DRAFT—

(This document will continue to be revised as needed.)

Adaptive Learning
An educational process where the teaching methods and materials adapt to each student's pace and level. Technology is often the vehicle for delivering this process, since software can change exercises, questions, and content fluidly based on a student's previous answers and actions.

Application (APP)
Computer software that performs a task or set of tasks, such as word processing or drawing. Applications also are referred to as programs.

Assistive Technology
Any piece of technology, hardware or software, that helps a person with disabilities perform everyday tasks that might otherwise be difficult or impossible. This can include everything from wheelchairs to screen readers to text telephones.

Augmentative and Alternative Communication (AAC)
Any communication method that helps individuals with speech and language impairments to communicate. AAC technologies are a sub-category of assistive technologies and include text-to-speech communicators and picture communicators.

Bandwidth
The capacity of a networked connection. Bandwidth determines how much data can be sent along the networked wires. Bandwidth is particularly important for internet connections, since greater bandwidth also means faster downloads.

Big Data
A collection of data sets so large that specialized technologies, techniques, and technicians are required to process, manage, and store them. An industry has arisen around the processing and analysis of large volumes of student data.

Blended Learning
A teaching practice that combines, or blends, classroom and online learning. The instruction of a lesson occurs with both teacher interaction and computing devices. Also known as Hybrid Learning

Bring Your Own Device (BYOD)
Also known as Bring Your Own Technology (BYOT), this is an initiative where students bring their own mobile devices into the classroom for class purposes, as opposed to using school-issued devices. This is often seen as an alternative to 1:1 programs due to lower maintenance costs, though students without devices cannot participate.

Clickers
A system where individual students respond via technology to teacher-posed questions. The teacher has immediate access to a summary of their responses.

Cloud
The Cloud is a metaphor referring to groups of remote services and software networks that allow centralized data storage and online access to computer services or resources.

Cloud Computing
A generic term that refers to the computer hardware and software that powers the cloud. This includes servers (a computer with specialized software on it), data storage, applications, and more.

Common Core State Standards (CCSS)
A U.S. initiative to provide a national set of learning standards for Mathematics and English Language Arts. Adopted in Oregon in 2012.

Digital Native
An individual born during or after the common use of digital technologies, such as the internet, mobile devices, and apps. It is assumed that such individuals have a strong grasp of digital technology because it was a regular part of their lives.

Education Technology (EdTech)
Any kind of technology that is used for educational purposes by an educator or educational institution. Most commonly used in reference to software utilized in primary, secondary, and higher education, though it can cover much more than that.

Engagement
Used in the context of education, it means the attentiveness and interest of a student to the lesson at hand. If a student is highly engaged, it means the student is focused, and maybe even enthusiastic about the topic. The best learning occurs when there is high engagement.

Flipped Classroom
A form of blended learning, this is the practice of students watching lecture material (usually in video form) at home, then practicing their learnings in an interactive environment in the classroom. Households without computers or an internet connection cannot participate in this practice, however.

Gamification
The practice of applying game mechanics to an activity. Examples of game mechanics are goals, badges, competition, immediate feedback, and advancing through game levels (leveling up).

Hacker
A person with technical expertise who experiments with computer systems to determine how to develop additional features. Hackers occasionally are requested by system administrators to try and "break into" systems via a network to test security.

Hybrid Learning
Synonymous with Blended Learning. See the Blended Learning definition above.

Instructional Technology
A subset of education technology, this practice focuses more on the use of technology for instructional purposes, though the terms are sometimes used interchangeably.

Learning Management System (LMS)
A piece of software that manages, analyzes, and runs educational courses and training programs. Also included are student registration, curriculum management, skill and competency management, and reporting features. Most modern LMS packages are web-based. Corvallis has not adopted a district-wide LMS.

Massive Open Online Course (MOOC)
A free online course that includes video lectures, reading materials, problem sets, and a student community. These are often created by universities, however there is little, if any, professor or student interaction or feedback.

Mobile Device Management (MDM)
An industry term for the administration of mobile devices, such as smartphones, tablets, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices. CSD currently uses a JAMF Software products called Casper.

One-to-One (1:1)
Most commonly refers to a program where a school provides one device (e.g. laptop, tablet) per student.

Open Educational Resource (OER)
Any online educational material that is freely accessible and openly licensed for public consumption. Such materials can be online courses, lectures, homework assignments, exercises, quizzes, interactive simulations, and games.

Pedagogy
The science and art of education and learning theory. Just as there are fields of study in other subjects, this is the study of teaching.

Personal Learning Network (PLN)
An informal network of people that is professional in nature and meant to aid an educator in furthering his/her pedagogical craft.

Project Based Learning (PBL)
A teaching method based on the idea of "learning by doing." Students work on a hands-on real-world activity that demonstrates the concepts they are learning. PBL learning tends to have high student engagement.

Professional Development (PD)
A generic term for the growth of one's career-oriented competencies. Teachers regularly attend workshops and conferences, expand their professional learning network, and undergo performance evaluations to further their craft.

STEM (Science Technology Engineering Mathematics)
An acronym that stands for the fields of science, technology, engineering, and mathematics. These fields are often grouped together because of a national movement to promote these subjects in the U.S. This includes initiatives to integrate their curriculums together with the goal that such an emphasis will lead to a stronger high-tech workforce.

STEAM (Science Technology Engineering Art Math)
An acronym that stands for the fields of science, technology, engineering, arts, and mathematics. This is a reaction to the STEM initiative and includes the arts as a priority as well. Though it is not yet as widely promoted as STEM, it is gaining in popularity.

Student Information System (SIS)
A piece of software that manages student data. This includes grades, attendance, background information, discipline records, and health records. Corvallis currently utilizes a Global Scholar software product called Pinnacle.

Student Response Systems
Synonymous with Clickers. Sometimes also called Classroom Response Systems or, more generically, Audience Response Systems.

Uncovering Security Flaws in Digital Education Products for Schoolchildren

By NATASHA SINGER

February8, 2015

The New York Times

When Tony Porterfield's two sons came home from elementary school with an assignment to use a reading assessment site called Raz-Kids.com, he was curious, as a parent, to see how it worked. As a software engineer, he was also curious about the site's data security practices.

And he was dismayed to discover that the site not only was unencrypted, but also stored passwords in plain text—security weaknesses that could potentially have allowed unauthorized users to gain access to details like students' names, voice recordings or skill levels. He alerted the site to his concerns. More than a year later, the vulnerabilities remain.

"A lot of education sites have glaring security problems," said Mr. Porterfield, the principal engineer at a software start-up in Los Altos, Calif. "A big part of the problem is that there's not even any consensus of what 'good security' means for an educational website or app."

Contacted last week by a reporter, John Campbell, the chief executive of the Cambium Learning Group, the company behind Raz-Kids.com, said that his company took privacy very seriously and that the site did not store sensitive personal details like student addresses or phone numbers.

"We are confident that we have taken the necessary steps to protect all student and teacher data at all times and comply with all federal and state laws," Mr. Campbell wrote in an emailed statement.

Mr. Porterfield, though, has gone on to examine nearly 20 digital education products, used collectively by millions of teachers and students, and found other potential security problems. He alerted makers of those products, too—among them school-districtwide social networks, classroom assessment programs and learning apps.

Some, including Pearson, a leading educational publisher, and ClassDojo, a popular classroom management app for teachers, addressed the issues he brought to their attention. Others did not.

While none of the security weaknesses appear to have been exploited by hackers, some technologists say they are symptomatic of widespread lapses in student data protection across the education technology sector. They warn that insecure learning sites, apps and messaging services could potentially expose students, many of them under 13, to hacking, identity theft, cyberbullying by their peers, or even unwanted contact from strangers.

At fault, these experts say, is a common practice among start-ups of concentrating primarily on increasing their market share.

"For many younger companies, the focus has been more on building the product out and less on guaranteeing a level of comprehensive privacy and security protection commensurate with the sensitive information associated with education," said Jonathan Mayer, a lawyer and computer science graduate student at Stanford University. "It seems to be a recurring theme."

The New York Times asked Mr. Mayer to review the vulnerabilities in education tech software discovered by Mr. Porterfield and described in this article.

To help schools evaluate companies' security practices, the Consortium for School Networking, a national association of school district chief technology officers, published a list of security questions last year for schools to ask before they sign purchase agreements with technology vendors.

"It is a huge challenge because there hasn't been the time and attention and investment placed in security that school districts need," said Keith R. Krueger, the group's chief executive. His group has received financing from Dell, Google, Pearson, Microsoft and other companies involved in the education sector.

Security lapses are not limited to education software devised for prekindergarten through 12th-grade students, an annual market estimated at about $8 billion.

In the fall, as Mr. Mayer, the digital security expert, was preparing to teach a class at Stanford Law School for Coursera, a start-up that provides hundreds of free open online courses, he discovered a security weakness that could have allowed instructors to gain access to the names and email addresses of millions of Coursera students. Another flaw would have potentially allowed other websites, digital advertising networks or online analytics firms to compile lists of the students' courses.

Coursera, which has raised $85 million from investors, quickly ameliorated the situation. In an explanation posted on its site, the company acknowledged that it had been more focused on deflecting potential attacks from outsiders than on the possibility of misuse of student data by insiders.

"If we were too trusting, we learned our lesson on this," Richard C. Levin, the chief executive of Coursera, said in a recent interview.

Protection of student data is gaining attention as schools across the country are increasingly introducing learning sites and apps that may collect information about a student's every keystroke. The idea is to personalize lessons by amassing and analyzing reams of data about each student's actions, tailoring academic material to individual learning levels and preferences.

But some privacy law scholars, educators and technologists contend that federal protections for student data have not kept pace with the scope and sophistication of classroom data-mining. Although a federal privacy law places some limits on how schools, and the vendors to which they outsource school functions, handle students' official educational records, these experts say the protections do not extend to many of the free learning sites and apps that teachers download and use independently in their classrooms.

In an effort to bolster confidence in their products, more than 100 learning companies recently signed on to a voluntary industry pledge on student privacy. The signers agree, among other commitments, to "maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality and integrity of student personal information against risks—such as unauthorized access or use."

Although President Obama endorsed the industry pledge in a speech last month, it does not require ed tech vendors to comply with specific basic security measures—like encrypting students' names, screen names or other personal details. Nor does it prohibit companies from using weak security, like storing users' passwords in plain text, practices that could easily permit hackers to to hijack teacher or student accounts, potentially linking students' names to private details about their academic performance.

These kinds of security weaknesses are commonplace on consumer sites. But the law has long treated educational information as a category worthy of special protections, like credit or medical records. Considering the recent data breaches at even large, well-financed companies like Anthem and Sony, some privacy advocates want federal regulators to mandate that the education technology industry beef up student data protection.

"Bottom line, both the Federal Trade Commission and the Education Department could and should ramp up their student privacy enforcement," said Khaliah Barnes, director of the student privacy project at the Electronic Privacy Information Center, a nonprofit group. "Students have little recourse against current abuses."

Some learning companies were quite responsive to Mr. Porterfield's concerns. The Pearson product in which he found vulnerabilities last fall is an online student learning and assessment system, Pearson Realize. The weaknesses could have allowed unauthorized users to gain access to details about class rosters like student names.

The company's security experts corrected the issues in two days. Pearson was the only company to ask Mr. Porterfield to run his own tests afterward to make sure the fixes had worked.

"We should welcome the reporting of even a suspicion," said Rod Wallace, Pearson's chief information security officer. "We need to encourage the people who report them, engage them and let them know we are fixing them."

Last fall, Mr. Porterfield also contacted ClassDojo, a free classroom management program for teachers that, according to its developer, is used by at least one teacher in roughly one-third of American schools. The software engineer alerted company executives to security weaknesses that could potentially have allowed unauthorized users to gain access to students' names, behavior records and behavior scores.

Since then, ClassDojo has encrypted its mobile apps and instituted other security measures. Liam Don, the co-founder of ClassDojo, said its software was regularly subject to audits by security experts.

Security Questions to Ask of an Online Service Provider

It is important to understand your provider's security practices to ensure that data shared with and collected by the provider remain private and protected. You should work with your school district's security point of contact to determine whether the security practices of the provider comply both with school district policies and applicable laws. While neither the Family Educational Rights and Privacy Act (FERPA) nor Children's Online Privacy Protection Act (COPPA) prescribes specific security standards, school districts should look to industry suggested practice when assessing an online service provider.

The following is a non-exhaustive list of key security questions to discuss with your provider. A service level agreement (SLA) should include as many of these considerations as possible.

Data Collection

- What data does the provider collect?
- What, if any, data is collected by third parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

Network Operations Center Management and Security

- Does the provider perform regular penetration testing, vulnerability management, and intrusion prevention?
- Are all network devices located in secure facilities and under controlled circumstances (e.g. ID cards, entry logs)?
- Are backups performed and tested regularly and stored off-site?
- How are these backups secured? Disposed of?
- Are software vulnerabilities patched routinely or automatically on all servers?

Data Storage and Data Access

- Where will the information be stored and how is data "at rest" protected (i.e. data in the data center)?
    - Will any data be stored outside the United States?
    - Is all or some data at rest encrypted (e.g. just passwords, passwords and sensitive data, all data) and what encryption method is used?
- How will the information be stored? If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
    - FERPA requires that records for a school be maintained separately, and not be mingled with data from other school districts or users.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- How does the provider protect data in transit? e.g., SSL, hashing?
- Who has access to information stored or processed by the provider?
    - Under FERPA, individuals employed by the provider may only access school records when necessary to provide the service to the school district.
    - Does the provider perform background checks on personnel with administrative access to servers, applications and customer data?

    - Does the provider subcontract any functions, such as analytics?
    - What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
- If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTPPS?

Data and Metadata Retention

- How does the provider assure the proper management and disposal of data?
    - The provider should only keep data as long as necessary to perform the services to the school district.
- How will the provider delete data?
    - Is data deleted on a specific schedule or only on termination of contract? Can your school district request that information be deleted? What is the protocol for such a request?
- You should be able to request a copy of the information maintained by the provider at any time.
- All data disclosed to the provider or collected by the provider must be disposed of by reasonable means to protect against unauthorized access or use.
- Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession.

Development and Change Management Process

- Does the provider follow standardized and documented procedures for coding, configuration management, patch installation, and change management for all servers involved in delivery of contracted services?
- Are practices regularly audited?
- Does the provider notify the school district about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the school district?

Availability

- Does the provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the provider's protection against denial-of-service attack?

Audits and Standards

- Does the provider provide the school district the ability to audit the security and privacy of records?
- Have the provider's security operations been reviewed or audited by an outside group?
- Does the provider comply with a security standard such as the International Organization for Standardization (ISO), the Payment Card Industry Data Security Standards (PCI DSS)?

Test and Development Environments

- Will "live" student data be used in non-production (e.g. test or development, training) environment?
- Are these environments secure to the same standard as production data?

Data Breach, Incident Investigation and Response

- What happens if your online service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the school district for incident investigation?

CORVALLIS SCHOOL DISTRICT 509J

Code: GCAB
Adopted: 4/5/10

Personal Electronic ~~Communication~~ Devices and Social Media—Staff

Staff possession or use of personal electronic ~~communication~~ devices (PEDs) on district property, in district facilities during the work day, and while the staff is on duty in attendance at district-sponsored activities may be permitted subject to the limitations set forth in this policy and consistent with any additional school rules as may be established by the superintendent. At no time will a PED ~~personal communication device~~ be used in a manner that interferes with staff duty and responsibility for the supervision of students. A PED ~~"personal communication device"~~ is a device, not issued by the district, capable of electronically communicating, sending, receiving, storing, recording, reproducing, and/or displaying information and data.

~~that emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor of the device. These devices include, but are not limited to, walkie talkies, either long- or short-range portable radios, portable scanning devices, cellular telephones, pagers, personal digital assistants (PDAs), laptop computers, and similar devices with wireless capability. This also includes other digital audio and video devices such as, but not limited to, iPods, iPads, radios, and TV.~~

PEDs ~~Personal Cellular telephones/pagers and other digital audio and video devices~~ shall be silenced during instructional or class time, while on duty, or at any other time where such use of the device would cause a disruption of school activities or interfere with work assignment. ~~Cellular telephones~~ PEDs that have the capability to take photographs or record video or audio shall not be used for such purposes while on district property or while a staff member is on duty in district-sponsored activities, unless as expressly authorized by the principal or designee for a use directly related to and consistent with the employee's assigned duties. Computers, tablets, iPads, or similar devices brought to school will be restricted to academic activities during duty time.

~~Laptop computers and PDAs brought to school will be restricted to classroom or instructional-related activities only.~~ The district will not be liable for loss or damage to PEDs ~~personal communication devices~~ brought to district property and district-sponsored activities.

Personal Use

Staff members will utilize social media websites, public websites, and blogs judiciously by not posting confidential information about students, staff, or district business.[1] Staff may not post images of district facilities, staff, students, volunteers, or parents without written authorization from persons with authority to grant such a release. Staff members will treat fellow employees, students, and the public with respect while posting on social media websites, public websites, and blogs in order to prevent substantial disruption in school.

District Use

Communication with students beyond the school day will be appropriate, professional, and related to school assignments or activities. When communicating with students electronically, staff should use district-sponsored options including social media, iMessaging, grading programs, or district e-mail utilizing mailing lists to a group of students rather than individual students. Text messaging with students via short message service (SMS) ~~Texting students and using social network sites when~~

[1]Nothing in this policy is intended in any form to limit the right of employees to engage in protected labor activities via the use of social media.

~~communicating with students~~ is discouraged. Communication with students using PEDs regarding non-school-related matters is prohibited during work hours and strongly discouraged at all other times.

~~Staff members who use social network sites (e.g., Facebook, MySpace, and Twitter) for personal use will not post confidential information about students, staff, or district business. Staff members will treat fellow employees, students, and the public with respect while posting.~~

Exceptions to the prohibitions set forth in this policy may be made for health, safety, or emergency reasons with superintendent or designee approval.

Staff are subject to disciplinary action up to and including dismissal for using a PED ~~personal communication device~~ in any manner that is illegal or violates the terms of this policy. Staff actions on social media websites, public websites, and blogs, while on or off duty, which disrupt the school environment, are subject to disciplinary action up to and including dismissal. A "disruption" for purposes of this policy includes, but is not limited to, one or more parents threatening to remove their children from a particular class or particular school, and/or a threatened or actual negative impact on the learning environment. The taking, disseminating, transferring, or sharing of obscene, pornographic, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (commonly called texting, sexting, e-mailing) may constitute a crime under state and/or federal law. Any person taking, disseminating, transferring, or sharing obscene, pornographic, or otherwise illegal images or photographs, will be reported to law enforcement and/or other appropriate state or federal agencies.

Licensed staff are subject at all times to the Standards of Competent and Ethical Performance for Teachers.

The superintendent shall ensure that this policy is available to all employees.

END OF POLICY

CORVALLIS SCHOOL DISTRICT 509J

Code: II/IIA
Adopted: 7/12/99
Revised/Readopted: 1/6/03, 2/7/11

Instructional Resources/Instructional Materials

The Board believes that proper care and judgment should be exercised in selecting instructional materials. While the Board retains the authority to approve district instructional materials adoptions, it authorizes the superintendent to develop and implement administrative procedures governing how selections are determined. Such procedures will provide for administrator, staff, parent, student and community involvement and employ suitable selection criteria to ensure that the recommended instructional materials will meet the needs of the program, students, teachers and community.

The superintendent in collaboration with building principals will recommend a schedule for review of instructional materials. Such timeline will consider the requirements of the State Board of Education adoption cycle, other state mandates, local district initiatives and fiscal practicalities.

All textbook and instructional materials recommended for adoption shall be approved for use by the Board. Prior to Board approval, students and interested district patrons will have the opportunity to review the recommended instructional materials and be encouraged to provide opinions about them and their use in the classrooms. If state adopted materials are not selected, an independent adoption will be ~~is~~ submitted for Board approval.

All supplementary materials and library/media resources will be selected cooperatively by teachers, principals, library/media teachers, and sometimes with the assistance of students and parents. Board approval is not needed for supplemental materials and resources.

Recommended textbook, supplementary materials, and library/media resources will be inclusive and value diversity in all forms when possible; contain appropriate readability and viewing levels; support the district's adopted curriculum contents; provide for ease of teacher use; be attractive and durable and be purchased at a reasonable cost.

The district will establish a process and timeline for regularly determining and considering whether the textbooks and other instructional materials are available through online resources that enable students with print disabilities to receive textbooks and instructional materials free of charge.

~~The Board recognizes that the appropriate use of some instructional materials shall include parental and administrative notification prior to its use. These materials have a legitimate purpose in a school's education program. However, since the content may include mature themes for students, parents and the appropriate building administrator will be notified prior to use. The Board supports the use of these materials as a resource to enhance and present the curriculum goals of the district and the content of specific adopted courses. Therefore, teachers are required to show evidence, through their lesson plans, of the intended use of the material(s) and the standard, benchmark, and/or curricular content area the resource supports. Administrative notification and/or concurrence and parental permission by the teacher are required specific to the materials and grade level in question. If a parent does not grant permission, an alternative assignment will be available for their student.~~

The Board recognizes that materials containing mature themes and content ~~may~~ have a legitimate purpose in a school's educational program. However, ~~T~~ the Board wishes to ensure that the use of such instructional and/or supplementary material enhances and supports the curriculum goals of the district and of specific adopted courses, and that the content of the material is appropriate for the developmental level of the student. Therefore, teachers are required to show evidence, through their lesson plans, of the intended use of the material and the standard/benchmark and related curriculum the resource supports. Administrative notification and/or concurrent and parental permission by the teacher are required specific to the materials containing mature themes and grade level in question. ~~Additionally, and prior to its use, parental permission and administrative concurrence may be required when the film contains mature themes that are rated beyond the age of the student.~~
If a parent does not grant permission, an alternative assignment will be available for the student.

The Board recognizes the right of individuals and/or groups to present complaints concerning instructional materials and programs in the schools. The superintendent will establish a review process for objections to instructional materials and programs. This process will provide for a timely and fair hearing, assuring that procedures are applied equitably to all expressions of concern.

The Board subscribes in principle and practice to statements of policy as expressed in the Copyright Fair Use Guidelines for Educational Multimedia, the American Library Bill of Rights and related interpretations thereof to include Statement on Intellectual Freedom, Confidentiality of Library Records and Access to Electronic Information, Services and Networks.

END OF POLICY

CORVALLIS SCHOOL DISTRICT 509J

Code: IIBGA-AR
Adopted: 7/12/99
Revised/Readopted: 12/10/01, 8/15/05, 11/6/06 6/21/10, 3/12/12

Electronic Communications System

Definitions

A. "Technology protection measure," as defined by the Children's Internet Protection Act (CIPA) means a specific technology that blocks or filters internet access to visual depictions that are:

1. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;

2. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or

3. Harmful to minors.

B. "Harmful to minors" as defined by CIPA 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;

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, an actual or simulated normal or perverted sexual acts, or a lewd exhibit of the genitals; and

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

C. "Sexual act; sexual contact" as defined by CIPA have the meanings given such terms in Section 2246 of Title 18, United States Code.

D. "Minor" as defined by CIPA means an individual who has not attained the age of 17. For the purpose of Board policy and this administrative regulation, minor will include all students enrolled in district schools.

E. "Inappropriate matter" as defined by the district means material that is inconsistent with general public education purpose, the district's mission, and goals.

F. "District system" includes those systems hosted by or accessed through the district (e.g., e-mail, network, and databases), as well as systems we contract through third party vendors (e.g., Linn Benton Lincoln Education Service District applications, Google).

General District Responsibilities

The district will:

A. Designate staff as necessary to ensure coordination and maintenance of the district's electronic communications system that includes all district computers, e-mail, and internet access.

B. Provide staff training in the appropriate use of the district's system including copies of district policy and administrative regulations. Staff will provide similar training to authorized system users.

C. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district's system;

D. Use only properly licensed software, audio, or video media purchased by the district or approved for use by the district. The district will comply with the requirements of law regarding the use, reproduction, and distribution of copyrighted works and with applicable provisions of use or license agreements.

E. Install and use desktop and/or server virus detection and removal software;

F. Provide technology protection measures that protect against internet access by both adults and minors to visual depictions that are obscene, child pornography; or with respect to the use of computers by minors, harmful to minors. An administrator, supervisor, or other individual authorized by the superintendent may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate.

G. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web.

H. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including "hacking" and other unlawful activities online, and ensure the safety and security of minors when authorized to use e-mail, chat rooms, and other forms of direct electronic communication.

I. Provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms.

J. Determine which users and sites accessible as part of the district's system are most applicable to the curricular needs of the district and may restrict user access, accordingly.

K. Determine which users will be provided access to the district's e-mail system.

L. Notify appropriate system users that:

1. The district retains ownership and control of its computers, hardware, software, and data at all times. All communications and stored information transmitted, received, or contained in the district's information system are the district's property and are to be used for authorized purposes only. Use of district equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette, and ensure that those authorized to use the district's systems are in compliance with Board policy, administrative regulations and law, school administrators may routinely review user files and communications. The district will inform system users that files and other information, including e-mail, generated or stored on district servers are not private and may be subject to such monitoring.

2. Files and other information, including e-mail, sent or received, generated, or stored on district servers are not private and may be subject to monitoring. By using the district's systems, individuals consent to have that use monitored by authorized district personnel. The district reserves the right to access and disclose, as appropriate, all information and data contained on district computers and district-owned e-mail system.

3. The district may establish a retention schedule for the removal of e-mail.

4. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction.

5. Information and data entered or stored on the district's computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the district. "Deleted" or "purged" data from district computers or e-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the district.

6. The district may set quotas for system disk usage. The district may allow system users to increase their quota by submitting a written request to the supervising teacher or system coordinator stating the need for the increase.

7. Transmission of any materials regarding political campaigns is prohibited. Providing general information is permitted, without advocacy for a position or candidate.

M. Ensure all staff and non-district system users complete and sign an agreement to abide by the district's electronic communications policy and administrative regulations. All such agreements will be maintained on file in the information services office. Internet and e-mail accounts are authorized and issued by virtue of a student's status as a currently enrolled student in the district. It is only by permission signed by parent or guardian that the student will be provided access to an internet or e-mail account. All such agreements will be maintained on file in the school office.

<u>System Access</u>

A. Access to the district's systems is authorized to students with parent approval and when under the direct supervision of staff; as well as Board members, district employees, ~~students with parent approval, and when under the direct supervision of staff~~, district volunteers, district contractors, or other members of the public as authorized by the system coordinator or district administrators consistent with the district's policy governing use of district equipment and materials.

B. Students, staff, Board members, volunteers, district contractors, and other members of the public may be permitted to use the district's systems for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/ guidelines/etiquette, and other applicable provisions of this administration regulation. Personal use of district-owned computers, including internet and e-mail access by employees, is prohibited if it interferes with the employee's duties during the employee's work hours. Additionally, Board member and employee use of district-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.

General Use Prohibitions/Guidelines/Etiquette

Operation of the district's systems relies upon the proper conduct and appropriate use of system users. Students, staff, and others granted system access are responsible for adhering to the following prohibitions and guidelines which require legal, ethical, and efficient utilization of the district's system.

A. Prohibitions

The following conduct is strictly prohibited:

1. Attempts to use the district's systems for:
   a. Unauthorized solicitation of funds;
   b. Distribution of chain letters;
   c. Unauthorized sale or purchase of merchandise and services;
   d. Collection of signatures;
   e. Membership drives;
   f. Transmission of any materials regarding political campaigns.

2. Attempts to upload, download, use, reproduce, or distribute information, data, software, or file share music, videos, or other materials on the district's systems in violation of copyright law or applicable provisions of use or license agreements.

3. Attempts to degrade, disrupt, or vandalize the district's equipment, software, materials, or data or those of any other user of the district's systems or any of the agencies or other networks connected to the district's systems.

4. Attempts to evade, change, or exceed resource quotas or disk usage quotas.

5. Attempts to send, intentionally access, or download any text file or picture or engage in any communication that includes material that may be interpreted as:
   a. Harmful to minors;
   b. Obscene or child pornography as defined by law or indecent, vulgar, profane, or lewd as determined by the district;
   c. A product or service not permitted to minors by law;
   d. Harassment, intimidation, menacing, threatening, or constitutes insulting or fighting words, the very expression of which injures or harasses others;
   e. A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
   f. Defamatory, libelous, reckless, or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense, or otherwise violates any law, rule, regulation, Board policy, and/or administrative regulation.

6. Attempts to gain unauthorized access to any service via the district's systems which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs.

7. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student directory and personally identifiable information. Personal contact information includes photograph; age; home, school, work, or e-mail addresses; phone numbers; or other unauthorized disclosure, use, and dissemination of personal information regarding students.

8. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization.

9. Attempts to use another individuals account name or password, or access restricted information, resources, or networks to which the user has not been given permission.

B. Guidelines/Etiquette

Appropriate system use etiquette is expected of all users and is explained in district training sessions and as described in the Student Network Use Handbook.

Complaints

Complaints regarding use of the district's Electronic Communications System may be made to the teacher, principal, employee's supervisor, or system coordinator. The district's established complaint procedure will be used for complaints concerning violations of the district's Electronic Communications System policy and/or administrative regulation. See Board policy KL and accompanying administrative regulation.

Violations/Consequences

A. Students

1. Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of district system access up to and including permanent loss of privileges.

2. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.

3. Disciplinary action may be appealed by parents, students, and/or a representative in accordance with established district procedures.

B. Staff

1. Staff who violate general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements, and applicable provisions of law.

2. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.

3. Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for competent and ethical performance of Oregon Educators will be reported to TSPC as provided by OAR 584-020-0041.

4. Violations of ORS 244.040 will be reported to Government Standards and Practices Commission.

C. Others

1. Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.

2. Violations of law will be reported to law enforcement officials or other agencies, as appropriate and may result in criminal or civil sanctions.

Telephone/Membership/Other Charges

A. The district assumes no responsibility or liability for any membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by any home usage of the district's systems.

B. Any disputes or problems regarding phone services for home users of the district's systems are strictly between the system user and his/her local phone company and/or long distance service provider.

Information Content/Third Party Supplied Information

A. System users and parents of student system users are advised that use of the district's systems may provide unintentional access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's systems accordingly.

B. Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third party individuals are those of the providers and not the district.

C. System users may, with supervising teacher or system coordinator approval, order services or merchandise from other individuals and agencies that may be accessed through the district's system. These individuals and agencies are not affiliated with the district. All matters concerning merchandise and services ordered including, but not limited to, purchase terms, payment terms, warranties, guarantees and delivery are solely between the seller and the system user. The district makes no warranties or representation whatsoever with regard to any goods or services provided by the seller. District staff and administration shall not be a party to any such transaction or be liable for any costs or damages arising out of, either directly or indirectly, the actions or inactions of sellers.

D. The district does not warrant that the functions or services performed by or that the information or software contained on the systems will meet the system user's requirements or that the system will be uninterrupted or error-free or that defects will be corrected. The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the systems and any information or software contained therein.

Corvallis School District 509J

~~**Student Electronic Account**~~

Technology Responsible Use Agreement Form

Student Name _____ Grade _____

School _____

Parent or Guardian Section

I have read the District's Technology Responsible ~~Student Electronic~~ Use Handbook (part of the Student/Parent Handbook), online at: https://dnn.csd509j.net/Portals/1/Publications%20and%20Reports/S-P%20Handbooks/2011-12%20SP%20Handbook%20English.pdf

The Technology Responsible ~~Student Electronic~~ Use Handbook is summarized on the back of this form. I hereby release the district, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the district system, including, but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services. I understand that I can be held liable for damages caused by my child's intentional misuse of the system.

To maintain system integrity, monitor network etiquette, and ensure that those authorized to use the district's systems are in compliance with Board policy, administrative regulations and law, school administrators may routinely review user files and communications. I understand by using the district's systems, individuals consent to having that use monitored by authorized district personnel.

I understand that use of the district's systems students may be exposed or be able to navigate to materials that may be considered objectionable and inconsistent with the district's mission and goals. I will instruct my child regarding restrictions against accessing material that are in addition to the restrictions set forth in the Technology Responsible ~~Student Electronic~~ Use Handbook. I also will emphasize to my child the importance of following the rules for personal safety.

I give permission for my child to access only those portions of the local and wide area network ~~s (hereafter referred to as the "Network")~~ connections that are approved by the Corvallis School District, and to use PEDs ~~personal electronic devices~~ and services only as approved by the district.

Parent or Guardian Signature _____ Date _____

Parent or Guardian Name Printed _____ Phone _____

Home Address _____

E-Mail _____

Student Section

I have read the District's Technology Responsible ~~Student Electronic~~ Use Handbook (site address above) and summary on the back of this form. I agree to follow the rules contained in this handbook. I understand that if I violate the rules my account can be terminated and I may face other disciplinary measures.

Student Signature _____ Date _____

Please return this completed form with registration materials to your student's school.

STAFF AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT

I have read the district's Electronic Communications System policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions will result in suspension or revocation of system access and related privileges and/or referral to law enforcement officials.

I understand that I take responsibility for ensuring the confidentiality of information placed on the district system. This responsibility includes monitoring of shared rights and privileges, including but not limited to third party systems such as Google Apps for Education. If I do not understand how to protect confidential student information, I will notify my supervisor and seek training before proceeding.

In consideration for the privilege of using the district's Electronic Communications System and in consideration for having access to the public networks, I hereby release the district, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use or inability to use the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

I understand that my district electronic communications are subject to public records law.

Signature: _____

Home Address: _____

Date: _____ Home Phone Number: _____

Assigned Username: first name last name

Initial Password: password (to be changed by user)

AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT
(Non-District System User)

I have read the district's Electronic Communications System policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions result in suspension or revocation of system access and related privileges and/or referral to law enforcement officials.

I understand that I take responsibility for ensuring the confidentiality of information placed on the district system. This responsibility includes monitoring of shared rights and privileges, including but not limited to third party systems such as Google Apps for Education. If I do not understand how to protect confidential student information, I will notify my supervisor and seek training before proceeding.

In consideration for the privilege of using the district's Electronic Communications System and in consideration for having access to the public networks, I hereby release the district, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use or inability to use the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

I understand that my district electronic communications are subject to public records law.

Signature: _____

Home Address: _____

Date: _____ Home Phone Number: _____

Assigned Username: first name last name

Initial Password: password (to be changed by user)

CORVALLIS SCHOOL DISTRICT 509J

Code: IIBGB-AR
Adopted: 5/2/05

WEB-PAGE GUIDELINES

All web pages must follow district guidelines and be approved by the building principal and/or webmaster prior to publication.

Content

All web pages must:

1. Contain name, address and district e-mail address of the author. Student web pages shall cite ~~use~~ the sponsoring staff member;

2. Be grammatically correct with no spelling errors. Spell checking and proofreading are required;

3. Contain current and accurate information;

4. Include a copyright statement, if appropriate;

5. Use district approved templates;

6. Contain a created or modified date and the name or initials of the person responsible;

7. Identify district affiliation and contain a link to return to the district's home page.

Links to other than district sites are subject to approval by the webmaster. All links should be checked regularly and revised as necessary.

Use of web pages for personal financial gain is prohibited.

Standards

Web-page authors shall:

1. Comply with Board policies, administrative regulations, these guidelines and copyright laws;

2. Respect the rights of others;

3. Maintain the privacy of others;

4. Use websites for academic, educational and research purposes only;

5. Use conventions of standard English or other languages.

Web-age authors shall not:

1. Display abusive, harassing, libelous, obscene, offensive, profane, pornographic, threatening, sexually explicit or illegal material;

2. Use website for commercial, purchasing or illegal purposes.

Disclaimer

The district has made every reasonable attempt to ensure that the district's web pages are educationally sound and do not contain links to any questionable material or anything that can be deemed in violation of the district's electronic communications policy. However, system users and parents of student system users are advised that use of the district's systems may provide unintentional access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's systems accordingly.

Student Safeguards

1. Web-page documents may include only the first name and the initial of the student's last name; last names may be used with parent permission.

2. Documents may not include a student's phone number, address, names of other family members or names of friends.

3. Published e-mail addresses are restricted to staff members or to a general group e-mail address where mail is forwarded to a staff member.

4. Decisions on publishing student pictures will be made by the supervising teacher, after checking with the school office to determine if the student's parents have approved ~~objected to~~ such publication.

Maintenance

Maintenance of web pages, including the timely update of information and periodic checks of links, is the responsibility of the author. Web pages not up to date may be removed by the webmaster.

The district reserves the right to remove web pages, and if necessary, access to user accounts, without prior notice, if the content is unacceptable.

Privacy

There shall be no expectation of privacy for information stored on or transmitted with district equipment. The district webmaster may review web pages to maintain system integrity and to monitor appropriate use of district equipment. Illegal activities will be reported to the appropriate authorities.

Corvallis School District 509J

Student Permission to Publish Form

Parent or Guardian:

It is our practice when publishing your child's photo, work, or web pages electronically, such as on the Internet, to seek your written permission in accordance with the Family Educational Rights and Privacy Act (FERPA).

Staff Person_____ School Phone Number _____

PLEASE FILL OUT THE FOLLOWING INFORMATION AND RETURN TO SCHOOL

_____ has my permission to publish as indicated by checkmarks
(School or Staff Person
below.

- ❑ Photo of my child. (Full names will not be published with photos without specific parental permission).
- ❑ Full name of my child in association with photos and other published documents.
- ❑ Work done by my child.
- ❑ Web pages created by my child.

I understand that personally identifiable information, such as address and telephone numbers will not be published electronically regardless of permission granted by this form. (Refer to board policy in the School Board Policy Handbook, Section J: Students, Education Records Management, and Personally Identifiable Information).

Student Name _____ Date_____

Parent Signature _____ Date_____

Daytime Phone _____ Evening Phone _____

CORVALLIS SCHOOL DISTRICT 509J

Code: JFCEB
Adopted: 2/5/07
Revised/Readopted: 8/23/10

Personal Electronic Devices and Social Media—Student

~~Subject to the conditions of this policy and administrative regulation JFCEB-AR,~~

Student possession or use of personal electronic devices (PED) on district property, in district facilities during the school day, and while the student is in attendance at district-sponsored activities may be permitted subject to the limitations set forth in this policy and consistent with any additional school rules as may be established by the principal and approved by the superintendent. A PED ~~"personal electronic device"~~ is a device that is capable of electronically communicating, sending, receiving, storing, recording, reproducing, and/or displaying information and data. ~~emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor of the device. These devices include, but are not limited to walkie talkies, either long- or short-range portable radios, portable scanning devices, cellular telephones and pagers, other digital audio devices (e.g., iPODS), personal digital assistants (PDAs), laptop computers, and similar devices with wireless capability. At no time will any device be allowed which provides for a wireless, unfiltered connection to the Internet.~~
The district will not be liable for personal electronic devices brought to district property and district-sponsored activities.

Students may not access social media websites, public websites, and blogs using district equipment, while on district property, or at district-sponsored activities unless the posting is approved by a district representative. The district will not be liable for information or comments posted by students on social media websites when the student is not engaged in district activities.
~~Social media Web sites are Web sites such as, but not limited to, Facebook, MySpace, and Twitter.~~

Exceptions to the prohibitions set forth in this policy may be made for health, safety, or emergency reasons with prior principal or designee approval or when use is provided for in a student's individualized education program (IEP).

~~The district will not be liable for PEDs brought to district property and district-sponsored activities.~~

Students whose behavior is found to be in violation of this policy will be subject to loss of privileges and disciplinary action, up to and including expulsion for using a PED in any manner that is academically dishonest, illegal, or violates the terms of this policy.[2] A referral to law enforcement official also may be made. PEDs owned by students and brought to district property or used in violation of this policy are subject to confiscation and will be released to the student's parent or property owner, as appropriate.

The superintendent is directed to develop administrative regulations and/or approve school rules as necessary to ensure that student use of such devices is consistent with this policy. Administrative regulations may include grade- or age-level possession and/or use restrictions by students on district property and at district-sponsored activities; consequences for violations; a process for responding to a student's request to use a PED, including an appeal process if the request is denied; and such other provisions as the superintendent may deem necessary. The superintendent may provide for the confiscation of PEDs, and the delivery of such devices to law enforcement, if requested for evidence purposes. The superintendent is responsible for ensuring that pertinent provisions of Board policies, administrative regulation, and school rules governing PEDs are included in staff handbooks and student/parent handbooks ~~and other means~~, reviewed annually, and updated as necessary.

END OF POLICY

[2]The taking, disseminating, transferring, or sharing of obscene, pornographic, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, etc.) may constitute a crime under state and/or federal law. Any person taking, disseminating, transferring, or sharing obscene, pornographic, or otherwise illegal images or photographs will be reported to law enforcement and/or other appropriate state or federal agencies.

CORVALLIS SCHOOL DISTRICT 509J

Code: JFCEB-AR
Adopted: 1/8/07
Revised/Readopted: 6/21/10

PERSONAL ELECTRONIC DEVICES AND SOCIAL MEDIA

Students may use and possess personal electronic devices (PEDs) on district grounds subject to the following:

1. Support of PEDs ~~personal electronic devices~~ is subject to available district resources including, but not limited to, IP addresses and network bandwidth capacity. Laptop computers and PEDs ~~PDAs~~ brought to school and accessing district resources may be restricted to classroom or instructional-related activities only and these activities may not impede district network capacity.

2. PEDs ~~personal electronic devices~~ shall not be used in a manner that disrupts the educational process, school programs or activities, or in a manner that violates law, Board policies, administrative regulations, school rules, or classroom rules[3].

3. Unless authorized in advance by the building principal or designee for health or safety reasons, for use as a study aid, or in the event of an emergency situation that involves imminent physical danger:

    a. PEDs ~~personal electronic devices~~ are not permitted to be turned on or visible on campus during the regular school day by students attending elementary and middle schools;

    b. PEDs ~~personal electronic devices~~ may be used during the student's break time at high school. ~~They may not be used at any time in the proximity of any class, school activity, or event that may be in session or in progress during the regular school day.~~

    c. PEDs may be used as electronic study aids in the classroom if provided as a part of a student's individualized education program (IEP), or if permission is received from the student's teacher. Otherwise, they may not be used at any time in the proximity of any class, school activity, or event that may be in session or in progress during the regular school day.

~~4. At no time will any personal electronic device be allowed to be used for disruptive purposes while on district property or while the student is engaged in district-sponsored activities~~.

[3]The taking, disseminating, transferring, or sharing of obscene, pornographic, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, etc.) may constitute a crime under state and/or federal law. Any person taking, disseminating, transferring, or sharing obscene, pornographic, or otherwise illegal images or photographs will be reported to law enforcement and/or other appropriate state or federal agencies.

5. PEDs ~~personal electronic devices~~ that have the capability to take photographs or record video or audio ~~Digital devices which have the capability to take "photographs" or "moving pictures"~~ shall not be used for such purposes while on district property or at district-sponsored events unless as expressly authorized in advance by the principal or designee.

6. The district shall not be responsible for loss, theft, or damage to PEDs ~~personal electronic devices~~ brought to district property or district-sponsored events.

7. PEDs ~~Personal electronic devices~~ must not be displayed in plain view during prohibited times of use.

~~8. PEDs personal electronic devices may be used as electronic study aids in the classroom if provided as a part of a student's individualized education program (IEP), or if permission is received from the student's teacher.~~

8. The use of PEDs ~~personal electronic devices~~ in any way to send or receive messages, data, or information in any form (text, image, audio, or video) that would pose a threat to academic integrity, contribute to, or constitute academic dishonesty is strictly prohibited.

9. The use of PEDs ~~personal electronic devices~~ in any manner (text, image, audio, or video) that would violate the confidentiality or privacy rights of another individual is strictly prohibited.

10. Students shall comply with any additional school rules as established by the building principal and classroom rules as approved by the building principal concerning the appropriate use of PEDs ~~personal electronic devices~~.

11. PEDs ~~personal electronic devices~~ used in violation of law, Board policy, administrative regulation, or approved school rules will be confiscated, turned in to the school office, and/or transferred to law enforcement officials as appropriate. If law enforcement does not retain the device as evidence, the device will be returned to the student or parent following parent notification, conference, detention, suspension, and/or expulsion.

12. Students may not use PEDs ~~personal electronic devices~~ to access social media sites through a connection to district equipment or the district network unless the posting is approved by an authorized district representative.