

Crook County School District

Code: IIBGA
Adopted: 7/11/16
Revised/Readopted: 1/13/20
Orig. Code: IIBGA

Electronic Communications System-Acceptable use Policy

The Board is committed to the development and establishment of a quality, equitable and cost effective electronic communications system. The system's sole purpose shall be for the advancement and promotion of learning, teaching and communications through the district.

The district's system will be used to provide district-wide, state-wide, national and global communications opportunities for staff and students.

The superintendent and director of technology will establish administrative regulations for the use of the district's system including compliance with the following provisions of the Children's Internet Protection Act:

1. Technology protection measures, installed and in continuous operation, that protect against Internet access by both adults and students¹ to visual depictions that are obscene, child pornography or, with respect to the use of the computers by minors, harmful to students;
2. Educating minors about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other
3. Monitoring the on-line activities of students;
4. Denying access by students to inappropriate matter on the Internet and World Wide Web;
5. Ensuring the safety and security of students when using e-mail, social media, chat rooms and other forms of direct electronic communication.
6. Prohibiting unauthorized access, including so-called "hacking" and other unlawful activities by minors online;
7. Prohibiting unauthorized disclosure, use and dissemination of personal information regarding students;
8. Installing measures designed to restrict students' access to materials harmful to students.

The superintendent and director of technology will establish administrative regulations for use of the district's system by staff using their own personal electronic devices to download and store district proprietary information including personally recognizable information about the district students or staff. The regulations shall insure compliance with privacy rights under applicable federal and state laws and regulations, including but not limited to the Age Discrimination in Employment Act of 1967 (ADEA), the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act of 2008 (GINA) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA).

The administrative regulations will be consistent with sound guidelines as may be provided by the education service district, the Oregon Department of Education and/or the Oregon Government Ethics Commission and will include a complaint procedure for reporting violations.

The superintendent and director of technology will also establish administrative regulations for use of the district's electronic communications system to comply with copyright law.

Failure to abide by district policy and administrative regulations governing use of the district's system may result in the suspension and/or revocation of system access. Additionally, student violations may result in discipline up to and including expulsion. Staff violations will also result in discipline up to and including dismissal. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions. Fees, fines or other charges may also be imposed.

END OF POLICY

Legal Reference(s):

[ORS 30.765](#)
[ORS 133.739](#)
[ORS 163.435](#)
[ORS 164.345](#)
[ORS 164.365](#)

[ORS 167.060 to -167.100](#)
[ORS Chapter 192](#)
[ORS 332.107](#)
[ORS 339.250](#)
[ORS 339.270](#)

[OAR 581-021-0050](#)
[OAR 581-021-0055](#)
[OAR 584-020-0040](#)
[OAR 584-020-0041](#)

Crook County School District

Code: IIBGA-AR
Revised/Reviewed: 8/14/17; 1/13/20
Orig. Code: IIBGA-AR

Electronic Communications System

Definitions

1. “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:
 - a. “Obscene,” has the meaning given such term in Section 1460 of Title 18, United States Code;
 - b. “Child pornography,” has the meaning given such term in Section 2256 of Title 18, United States Code; or
 - c. Harmful to minors.
2. “Harmful to minors,” as defined by CIPA, means any picture, image, graphic image file or other visual depiction that:
 - a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
 - b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 - c. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.
3. “Sexual act; sexual contact,” as defined by CIPA, have the meanings given such terms in Section 2246 of Title 18, United States Code.
4. “Minor,” as defined by CIPA, means an individual who has not attained the age of 17. For the purposes of Board policy and this administrative regulation, minor will include all students enrolled in district schools.
5. “Inappropriate matter,” as defined by the district, means material that is inconsistent with general public education purposes, the district’s mission and goals.
6. “District proprietary information” is defined by the district as any information created, produced or collected by district staff for the business or education purposes of the district including but not limited to student information, staff information, parent or patron information, curriculum, forms and like items used to conduct the district’s business.

7. “District software” is defined by the district as any commercial or staff developed software acquired using district resources.

General District Responsibilities

The district will:

1. Designate staff as necessary to ensure coordination and maintenance of the district’s electronic communications system which includes all district computers, e-mail and Internet access;
2. 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;
3. Provide a system for authorizing staff use of personal electronic devices to download or access district proprietary information, that insures the protections of said information and insures its removal from the device when its use is no longer authorized;
4. Provide a system for obtaining prior written agreement from staff for the recovery of district proprietary information downloaded to staff personal electronic devices as necessary to accomplish district purposes, obligations or duties, and when the use on the personal electronic device is no longer authorized, to insure verification that information downloaded has been properly removed from the personal electronic device;
5. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district’s system;
6. 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;
7. Install and use desktop and/or server virus detection and removal software;
8. 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. A supervisor or other individual authorized by the principal may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;
9. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;
10. 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, social media, chat rooms and other forms of direct electronic communication;

11. Provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking and social media websites and in chat rooms;
12. 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;
13. Staff and students will be provided with access to email. Student email access will be provided by Google Apps for Education.
14. Program its computers to display a message reinforcing key elements of the district's Electronic Communications System policy and regulation when accessed for use;
15. Notify appropriate system users that:
 - a. 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 system are in compliance with Board policy, administrative regulations and law, the school administrators may routinely review user files and communications;
 - b. 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 system, 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;
 - c. The district may establish a retention schedule for the removal of e-mail;
 - d. 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;
 - e. 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;
 - f. 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 supervisor and system coordinator stating the need for the increase;
 - g. Passwords used on the district's system are the property of the district and must be provided to their supervisor or designated district personnel, as appropriate. Passwords that have not been provided to the district are prohibited;
 - h. Transmission of any materials regarding political campaigns is prohibited.

16. Ensure all student, staff and non-school 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 school or district office;
17. Notify users of known copyright infringing activities and deny access to or remove the material.

System Access

Access to the district's system is authorized to:

1. Board members, district employees, students in grades K-12, with parent approval and when under the direct supervision of staff, and 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.
2. Students, staff, Board members, volunteers, district contractors and other members of the public may be permitted to use the district's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/guidelines/etiquette and other applicable provisions of this administrative regulation. Personal use of district-owned computers including Internet and e-mail access by employees is prohibited 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 same terms and 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 system 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.

1. Prohibitions

The following conduct is strictly prohibited:

- a. Attempts to use the district's system for:
 - (1) Unauthorized solicitation of funds;
 - (2) Distribution of chain letters;
 - (3) Unauthorized sale or purchase of merchandise and services;
 - (4) Collection of signatures;
 - (5) Membership drives;
 - (6) Transmission of any materials regarding political campaigns.

- b. Attempts to upload, download, use, reproduce or distribute information, data, software, or file share music, videos or other materials on the district's system in violation of copyright law or applicable provisions of use or license agreements;
- c. Attempts to degrade, disrupt or vandalize the district's equipment, software, materials or data or those of any other user of the district's system or any of the agencies or other networks connected to the district's system;
- d. Attempts to evade, change or exceed resource quotas or disk usage quotas;
- e. Attempts to send, intentionally access or download any text file or picture or engage in any communication that includes material which may be interpreted as:
 - (1) Harmful to minors;
 - (2) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
 - (3) A product or service not permitted to minors by law;
 - (4) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
 - (5) 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;
 - (6) 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.
- f. Attempts to gain unauthorized access to any service via the district's system 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;
- g. 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 information and personally identifiable information. Personal contact information includes photograph, age, home, school, work or e-mail addresses or phone numbers or other unauthorized disclosure, use and dissemination of personal information regarding students;
- h. Attempts to arrange student meetings with anyone on the district's system, unless authorized by the system coordinator or teacher and with prior parent approval;
- i. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
- j. Attempts to use another individual's account name or password, failure to provide the district with individual passwords or to access restricted information, resources or networks to which the user has not been given access.

2. Guidelines/Etiquette

System users will:

- a. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and administrative regulations;

- b. Respect other people’s time and cyberspace. Use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher or system coordinator. Avoid downloading excessively large files. Remain on the system long enough to get needed information then exit the system. Act as though every byte sent costs somebody time and money, because it does;
- c. Take pride in communications. Check spelling and grammar;
- d. Respect the privacy of others. Do not read the mail or files of others without their permission;
- e. Cite all quotes, references and sources;
- f. Adhere to guidelines for managing and composing effective e-mail messages:
 - (1) One subject per message - avoid covering various issues in a single e-mail message;
 - (2) Use a descriptive heading;
 - (3) Be concise - keep message short and to the point;
 - (4) Write short sentences;
 - (5) Use bulleted lists to break up complicated text;
 - (6) Conclude message with actions required and target dates;
 - (7) Remove e-mail in accordance with established guidelines;
 - (8) Remember, there is no expected right to privacy when using e-mail. Others may read or access mail;
 - (9) Always sign messages;
 - (10) Always acknowledge receipt of a document or file.
- g. Protect password confidentiality. Passwords are the property of the district and are not to be shared with others. Using another user’s account or password or allowing such access by another may be permitted with supervising teacher or system coordinator approval only. No system user may use a password on the district’s computers, e-mail system or Internet access which is unknown to the district;
- h. Communicate only with such users and/or sites as may be authorized by the district;
- i. Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques;
- j. Report violations of the district’s policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate.

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 - Public Complaints and accompanying administrative regulation.

Violations/Consequences

1. Students

- a. 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.
- b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
- c. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established district procedures.

2. Staff

- a. 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.
- b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
- c. 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 Oregon Administrative Rule (OAR) 584-020-0041.
- d. Violations of ORS 244.040 will be reported to Oregon Government Ethics Commission (OGEC).

3. Others

- a. 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.
- b. 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

1. The district assumes no responsibility or liability for any membership, phone charges or internet provider charges including, but not limited to, long distance charges, per minute (unit) surcharges, overage charges and/or equipment or line costs incurred by any home usage of the district's system.
2. Any disputes or problems regarding phone services or internet provider for home users of the district's system are strictly between the system user and their local phone company and/or long distance service provider.

Information Content/Third Party Supplied Information

1. System users and parents of student system users are advised that use of the district's system may provide 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 system accordingly.
2. 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.
3. 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.
4. The district does not warrant that the functions or services performed by or that the information or software contained on the system 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 system and any information or software contained therein.

Pages 7-10 apply to student / parent and non-staff use.



Dear Students & Parents/Guardians,

Crook County School District is committed to the use of technology and the Internet for educational purposes. Technology allows teachers to enhance and extend our curriculum in ways that were previously inconceivable. Along with the advantages of using technology also comes the need to educate students about responsibility and safety when using computers, tablets, smartphones and the Internet. The Crook County School District team is committed to providing our students with opportunities to learn and communicate with others, in a safe environment, through a wide range of technology.

In order to comply with the federal Children's Internet Protection Act, the district uses robust web filters and device management tools. We also provide digital citizenship toolkits and opportunities for our teachers and students to set, model, and follow responsible use guidelines in their classrooms. The district believes in access to the Internet and its wealth of information. While providing access to these resources, the district makes a concerted effort to only allow access to age appropriate content. The following Responsible Use Policy is meant to act as a guide to help students and families make positive choices when interacting online. A copy of the district's policy is attached for your review. Although teachers will review the information in this policy with students, we expect parents to spend some time reviewing it with their student(s), as the rules apply to home usage as well. For additional information on talking with your children about Internet usage, consider the following resources: NET CETERA -- Chatting with Kids About Being Online (bit.ly/netcetera) and Common Sense Media (bit.ly/csmparents).

Please read and familiarize yourself with the Responsible Use Policy. Both parents/guardians and students must sign the agreement. The signed copy must be returned to the student's school for our records before devices can go home.

Thank you for being a part of the Crook County School District community. We look forward to supporting the continued growth and success together. If you have any further questions, please contact your school's administrator or the district's technology department.

Sincerely,

Crook County School District

Computer, Network, and Internet Responsible Use Policy

Overview

Crook County School District provides its students and staff access to a multitude of technology resources. These resources provide opportunities to enhance learning and improve communication within our community. Some of these tools include G Suite for Education (for more information on G Suite, please visit bit.ly/CCSGAFE), learning management systems, and other online resources. With the privilege of access comes the responsibility to exercise personal responsibility in the use of these resources. School district policies are intended to promote the most effective, safe, productive, and instructionally sound uses of networked information & communication tools. Crook County School District also makes a good faith effort to protect its students from exposure to Internet materials that are harmful or explicit. The school district maintains a system of Internet content filtering on district provided devices at school and at home.

Digital Citizenship

Crook County School District staff and students use technology in meaningful, safe, and responsible ways while at school and at home. Digital citizenship means:

- Respect for one's self: Users will nurture an appropriate and respectful online presence, and will purposefully consider information and images before and after posting online.
- Respect for others: Users will refrain from using technologies to bully, tease, or harass other people.
- Respect for Intellectual Property: Users will suitably cite any and all use of websites, books, media, etc. while adhering to Fair Use practices.
- Protect one's self and others: Users will protect themselves and others by immediately reporting abuse and by not forwarding inappropriate materials or communications.
- Protect personal data: Users will not share personal logins and passwords and are urged to update passwords regularly. Users should not share personal information (name, address, phone number, etc.) in online forums or other electronic communications. Users will not share information belonging to other users.

Expectations

Responsible use of Crook County School District's technology resources is to be ethical, respectful, academically honest, and supportive of the district's mission. Each user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators, or their designees, may review files and communications (including electronic mail) to ensure that users are using the system in accordance with school district policy. Users should not expect that files stored on district servers, within Google Drive, or on hard disks will be private. Users also should understand that school servers regularly record Internet activity in log files that are available to the public under RSA 91-A: Access to Public Records and Meetings.

Some activities are expressly prohibited by law.

Users must abide by the generally accepted rules of network etiquette while at school and at home. The following guidelines are intended to clarify expectations for conduct, but they should not be construed as all-inclusive:

- Use of electronic devices should be consistent with Crook County School District's educational objectives, mission and curriculum.
- Transmission of any material in violation of local, federal and state laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material, and threatening or obscene material.
- Intentional or unintentional use of networked resources to access or process proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
- Software and/or services may not be installed or downloaded on school devices without prior approval of the school's administration.
- Use of computer resources for commercial activities, product advertisement, or religious or political lobbying is prohibited.
- Users may be held personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred.
- Files stored on district-managed networks, G Suite for Education accounts, or on district assigned devices may be inspected at any time and should not be considered private.
- Materials published for electronic publication must be for educational purposes. School administrators, teachers and staff may monitor these materials to ensure compliance with content standards.

Policy Violations

Crook County School District reserves the right to deny or limit access to technology and/or Internet to anyone. Violating any portion of this policy may result in disciplinary action, including temporary or permanent ban on computer or Internet use, suspension or dismissal from school, and/or legal action. The School Department may cooperate with law enforcement officers in investigations related to illegal activities conducted through its network.

**AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT
(NON-SCHOOL 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 will result in suspension or revocation of system access and related privileges and/or referral to law enforcement officials.

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.

Signature _____

Home Address _____

Date _____ Home Phone Number _____

This space reserved for System Coordinator

Assigned Username: _____ Assigned Password: _____

**AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT
(STAFF 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 will result in suspension or revocation of system access and related privileges, and may include discipline, up to and including dismissal and/or referral to law enforcement officials.

I understand that I may use my personal electronic device (PED) for education related purposes and that certain district proprietary information may be downloaded to my PED. I agree that any district proprietary information downloaded on my PED will only be as necessary to accomplish district purposes, obligations or duties, and will be properly removed from my PED when the use on my PED is no longer authorized. I insure that the personal electronic device in use is owned by me, and I am in complete control of the device at all times.

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.

Staff will take precautions to secure their computers from use by students. This means that staff will lock their computer or log off their computer and not leave their computer unlocked and unattended when students are present in their rooms.

Signature _____

Home Address _____

Date _____ Home Phone Number _____

This space reserved for System Coordinator

Assigned Username: _____ Assigned Password: _____