

Coast Unified School District **Student Acceptable Use Policy**

General Statement of Policy

Coast Unified School District provides access to the district computer network for electronic mail and the Internet. Access to e-mail and the Internet enables students to have access to electronic information that enables them to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people around the world.

Coast Unified School District is committed to making advanced technology and increased access to learning opportunities available to students, faculty, and other district employees. The district's goal in providing this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. To be in compliance with the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA) as mandated by Congress, Coast Unified School District has implemented the following guidelines and procedures for using the Internet. This Acceptable Use Policy and Media Consent form is a legally binding document.

CIPA mandates school districts to certify that they have in place an Internet Safety Policy. These mandates and assurances must be in place in order to receive E-rate funds or funds under Title III of Elementary and Secondary Education Act of 1965. Coast Unified School District incorporates Internet filtering technology, remote monitoring technology, network transaction auditing and staff supervision to prohibit obscenity, child pornography and material harmful to minors in compliance with CIPA.

COPPA applies to the online collection of personal information from children under 13. School districts must be COPPA compliant in order to receive E-rate funds. Coast Unified School District does not disclose personal information about students on district websites or through any unsecured Internet communication and staff members are instructed not to allow students to enter personal information on any external website or through any other Internet communication in compliance with COPPA. A consent form must be signed prior to any personal student information or work being placed on any district provided website.

Limited Educational Purpose

With access to computers and people all over the world comes the potential for access to material that is illegal, defamatory, inaccurate or offensive to some people. The school district system has a limited educational purpose, which includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities. Users of the system are expected to use the Internet to further educational and personal goals consistent with the mission of the school district and school policies. Uses, which might be acceptable on a user's private personal account on another system, may not be acceptable on this limited purpose network.

Coast Unified School District has taken steps to restrict access to inappropriate resources and information on the network and to monitor student use of the network. However, on a global network it is impossible to effectively control student access to material. The primary responsibility for access will rest with the student. We believe that the benefits to students from access to the Internet exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying standards that children should follow when using media and information sources. To that end, Coast Unified School District supports and respects each family's right to decide whether or not to apply for school network access.

Use of the System is a Privilege

The use of the school district system is a privilege, not a right. All users are responsible for good behavior on school computer networks and individual computers just as they would be if in a classroom. General school rules for behavior and communication apply. Network administrators, teachers, and other appropriate district personnel may review student/user files and communication to prevent misuse and to ensure students/users are using the system responsibly and in compliance with laws and district policies. There is no expectation of privacy when using technology resources owned and/or provided to users through Coast Unified School District. Depending on the nature and degree of the violation and number of violations of the district policy, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages or repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; civil or criminal liability under applicable laws.

The following pages contain a list of unacceptable uses and student rights. Please read these carefully. Signatures are required by student and parent/guardian prior to the student being given access to the system.

Student Internet Access

- All students may have access to the school district network and the Internet World Wide Web information resources through their classroom, library or school computer lab under the guidance of a teacher, librarian, library technician, or other school administrator.
- Students may have e-mail access only under their teacher's direct supervision using a classroom e-mail account.
- Student use of district computers to access either directly or through a proxy server, social networking sites, such as, but not limited to, MySpace, Facebook and Friendster, is prohibited. Student/teacher relationships on Facebook and other social networking sites are strongly discouraged.

Unacceptable Uses. The following uses of the district network are considered unacceptable:

• Personal Safety

- You will not post personal contact information about yourself or other people. Personal contact information includes your address, telephone number, school address, work address, etc.
- You will not agree to meet someone you have met online without your parent's approval and participation. Your parent should accompany you to the meeting.
- You will promptly report to your teacher or other appropriate school employee any message that you receive that is inappropriate or makes you uncomfortable.
- Users will immediately report to a staff member an obscene, pornographic or offensive material found.

• Illegal Activities

- You will not attempt to gain access to the district network or to any other computer system through the district network or go beyond your authorized access. This includes attempting to log on through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing".
- You will not make deliberate attempts to disrupt the computer system or network, or destroy data by spreading computer viruses, loading illegal files, or by any other means. These actions are illegal.
- You will not use the district network to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.
- You will not post, submit, publish, or display harmful matter or material that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- You will not use the system to engage in commercial or other for-profit activities.
- You will not use district resources to solicit, create, forward, or reply to any email that could be classified as a chain letter (SPAM).

• System Security

- You are responsible for your network account and should take all reasonable precautions to prevent others from being able to use your account. Under no circumstances should you provide your password to another person.
- You will immediately notify a teacher, school administrator, librarian or district technology department if you have identified a possible security problem. Do not go looking for security problems; this may be construed as an illegal attempt to gain access.
- You will not download software or install programs unless it is under the direct supervision of a teacher and only with permission from the school administrator or technology coordinator.
- You will do nothing that could disrupt the use of the system for others, including installing programs or files, deleting programs or files, modifying settings, changing passwords, or reconfiguring the system.
- *Any use of personal electronic devices (including but not limited to laptops, tablets, smart phones, cell phones, USB drives, iTouch devices, MP3 players) must be checked by the Technology Department in order to be on school premises.*
- You will not in any manner physically modify, harm, or destroy any computer or network hardware.
- Any student identified as a security risk may be denied access.

• Inappropriate Language

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.
- You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

- You will not post information that could cause damage or pose a danger of disruption.
- You will not engage in personal attacks, including prejudicial or discriminatory attacks, cyber bullying, intimidation, hazing or other conduct that causes or threatens to cause bodily harm or emotional suffering.
- You will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by the person to stop sending messages, you must stop.
- You will not knowingly or recklessly post false or defamatory information about a person or organization.

• Respect for Privacy

- You will not re-post a message that was sent to you privately without the permission of the person who sent you the message.
- You will not post private information about another person.
- You will not access another individual's materials, information or files without permission.
- You will not use someone else's password, user account, or logon.
- You will not gain unauthorized access to resources.

• Respecting Resource Limits

- You will use the system only for educational and career development activities.
- You will not download large files unless approved by the teacher in charge. If necessary, you will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer.
- You will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- You will not download and/or listen to radio streaming, video streaming, using any online telephone resource, or sharing music and/or video due to bandwidth restrictions.
- You will not download or install from any other sources any non-curriculum software unless approved by a principal or network administrator. This includes, but not limited to, non-educational games, peer-to-peer file-sharing software, remote control software, optimizing utilities, networking utilities, shareware software, freeware software, and Internet messengers. All software installed on district computers must be licensed and approved. Pirated software will not be tolerated.
- You will not intentionally waste limited resources.

• Plagiarism and Copyright Infringement

- You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. Reproduction of a work includes using the work in another written form or posting the work or portion of the work, on the Internet. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be confusing. If you have questions, you should ask your teacher.

• Inappropriate Access to Material

- You will not use the school district network to access harmful matter or material that is profane or obscene (pornography), that advocates illegal acts, or advocates violence or discrimination towards other people (hate literature). This may include certain song lyrics and related materials.
- If you mistakenly access inappropriate information, you should immediately tell the teacher or school administrator in charge. This will protect you against any claim that you have intentionally violated this policy.
- Your parent/guardian should instruct you if there is additional material that they think it would be inappropriate for you to access. The district fully expects that you will follow your parents' instructions in this matter.

• Your Rights

- Free Speech
 - Your right to free speech, as set forth in the district's disciplinary code, applies also to your communication on the district's network and on the Internet, except as otherwise set forth in the Acceptable Use Policy. The school

district network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict your speech for valid educational reasons.

- **Search and Seizure**

- You should be aware that computer files and communications on the district's network and all over the Internet are not private or secure.
- *Use of mobile wireless Internet devices (including but not limited to Hotspots, MiFi's, personal Bluetooth) other than those provided by the district is prohibited and subject to seizure.*
- Students will limit their use of the system to classroom activities, teacher-directed activities, library-related research, or career development. Use of the system for any other purpose, personal or otherwise, is prohibited unless approved in advance.
- The district may monitor your use of the Internet and the district's computer resources, *(including but not limited to laptops, tablets, smart phones, cell phones, USB drives, iTouch devices, MP3 players)*, your e-mail, personal electronic devices, Internet files, and Internet access, at any time without advance notice or consent when there is a reasonable need to do so. Passwords must be reported. Monitoring of the system may lead to discovery that you have violated the Acceptable Use Policy, the district's disciplinary codes or the law. *The district reserves the right to suspend the use of personal electronic devices.*
- Your parent/guardian has the right at any time to see the contents of your files.

- **Due Process**

- Violating this policy may result in one or all of the following: restricting network access; loss of network access; disciplinary or legal action including, but not limited to, suspension or expulsion and/or criminal prosecution under appropriate local, state and federal laws; assessment of the cost of damages to hardware/software.
- The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school district network.
- In the event there is a claim that you have violated this Policy of the district's disciplinary code in your use of the school district network, you will be provided with written notice of the suspected violation and an opportunity to be heard in the manner set forth in the district's disciplinary code.
- Major violations of the district's Acceptable Use Policy by a student will result in the loss of use of all computing equipment and Internet access, even if this causes the student to fail a class. The student may be able to regain computing privileges the following school year. If this occurs, the student will be given the opportunity to remove his/her school-related files.
- If the violation also involves a violation of the district's disciplinary code, it will be handled in a manner described in the district's disciplinary code. Additional restrictions may be placed on the student's use of their network account.

- **Limitation of Liability**

The district makes no warranties of any kind, either express or implied, that the functions or services provided through the school district network will be error-free or without defect. The district will not be responsible for any claims, damages, or injury of any nature whatsoever, which users may suffer as a result, whether directly or indirectly, of any use of the school district network, including, but not limited to, personal injury, emotional distress or suffering, or loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising from the unauthorized use of the school district network, including, but not limited to, the purchase of products or services.

REV. 0313Revisions italicized.

Coast Unified School District **Student Acceptable Use Policy**

General Statement of Policy

Coast Unified School District provides access to the district computer network for electronic mail and the Internet. Access to e-mail and the Internet enables students to have access to electronic information that enables them to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people around the world.

Coast Unified School District is committed to making advanced technology and increased access to learning opportunities available to students, faculty, and other district employees. The district's goal in providing this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. **To be in compliance with the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA)** as mandated by Congress, Coast Unified School District has implemented the following guidelines and procedures for using the Internet. This Acceptable Use Policy and Media Consent form is a legally binding document.

CIPA mandates school districts to certify that they have in place an Internet Safety Policy. These mandates and assurances must be in place in order to receive E-rate funds or funds under Title III of Elementary and Secondary Education Act of 1965. Coast Unified School District incorporates Internet filtering technology, remote monitoring technology, network transaction auditing and staff supervision to prohibit obscenity, child pornography and material harmful to minors in compliance with CIPA.

COPPA applies to the online collection of personal information from children under 13. School districts must be COPPA compliant in order to receive E-rate funds. Coast Unified School District does not disclose personal information about students on district websites or through any unsecured Internet communication and staff members are instructed not to allow students to enter personal information on any external website or through any other Internet communication in compliance with COPPA. A consent form must be signed prior to any personal student information or work being placed on any district provided website.

Limited Educational Purpose

With access to computers and people all over the world comes the potential for access to material that is illegal, defamatory, inaccurate or offensive to some people. The school district system has a limited educational purpose, which includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities. Users of the system are expected to use the Internet to further educational and personal goals consistent with the mission of the school district and school policies. Uses, which might be acceptable on a user's private personal account on another system, may not be acceptable on this limited purpose network.

Coast Unified School District has taken steps to restrict access to inappropriate resources and information on the network and to monitor student use of the network. However, on a global network it is impossible to effectively control student access to material. The primary responsibility for access will rest with the student. **We believe that the benefits to students from access to the Internet exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying standards that children should follow when using media and information sources. To that end, Coast Unified School District supports and respects each family's right to decide whether or not to apply for school network access.**

Use of the System is a Privilege

The use of the school district system is a privilege, not a right. All users are responsible for good behavior on school computer networks and individual computers just as they would be if in a classroom. **General school rules for behavior and communication apply.** Network administrators, teachers, and other appropriate district personnel may review student/user files and communication to prevent misuse and to ensure students/users are using the system responsibly and in compliance with laws and district policies. There is no expectation of privacy when using technology resources owned and/or provided to users through Coast Unified School District. Depending on the nature and degree of the violation and number of violations of the district policy, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use of access privileges; payments for damages or repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; civil or criminal liability under applicable laws.

unfortunately can't be true at APS bc of teachers assigning work that must be done online.

The following pages contain a list of unacceptable uses and student rights. Please read these carefully. Signatures are required by student and parent/guardian prior to the student being given access to the system.

Student Internet Access

- All students may have access to the school district network and the Internet World Wide Web information resources through their classroom, library or school computer lab under the guidance of a teacher, librarian, library technician, or other school administrator.
- Students may have e-mail access only under their teacher's direct supervision using a classroom e-mail account.
- Student use of district computers to access either directly or through a proxy server, social networking sites, such as, but not limited to, MySpace, Facebook and Friendster, is prohibited. Student/teacher relationships on Facebook and other social networking sites are strongly discouraged.

Unacceptable Uses. The following uses of the district network are considered unacceptable:

• Personal Safety

- You will not post personal contact information about yourself or other people. Personal contact information includes your address, telephone number, school address, work address, etc.
- You will not agree to meet someone you have met online without your parent's approval and participation. Your parent should accompany you to the meeting.
- You will promptly report to your teacher or other appropriate school employee any message that you receive that is inappropriate or makes you uncomfortable.
- Users will immediately report to a staff member an obscene, pornographic or offensive material found.

• Illegal Activities

- You will not attempt to gain access to the district network or to any other computer system through the district network or go beyond your authorized access. This includes attempting to log on through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing".
- You will not make deliberate attempts to disrupt the computer system or network, or destroy data by spreading computer viruses, loading illegal files, or by any other means. These actions are illegal.
- You will not use the district network to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.
- You will not post, submit, publish, or display harmful matter or material that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- You will not use the system to engage in commercial or other for-profit activities.
- You will not use district resources to solicit, create, forward, or reply to any email that could be classified as a chain letter (SPAM).

• System Security

- You are responsible for your network account and should take all reasonable precautions to prevent others from being able to use your account. Under no circumstances should you provide your password to another person.
- You will immediately notify a teacher, school administrator, librarian or district technology department if you have identified a possible security problem. Do not go looking for security problems; this may be construed as an illegal attempt to gain access.
- You will not download software or install programs unless it is under the direct supervision of a teacher and only with permission from the school administrator or technology coordinator.
- You will do nothing that could disrupt the use of the system for others, including installing programs or files, deleting programs or files, modifying settings, changing passwords, or reconfiguring the system.
- *Any use of personal electronic devices (including but not limited to laptops, tablets, smart phones, cell phones, USB drives, iTouch devices, MP3 players) must be checked by the Technology Department in order to be on school premises.*
- You will not in any manner physically modify, harm, or destroy any computer or network hardware.
- Any student identified as a security risk may be denied access.

• Inappropriate Language

- Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.
- You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

- You will not post information that could cause damage or pose a danger of disruption.
- You will not engage in personal attacks, including prejudicial or discriminatory attacks, cyber bullying, intimidation, hazing or other conduct that causes or threatens to cause bodily harm or emotional suffering.
- You will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by the person to stop sending messages, you must stop.
- You will not knowingly or recklessly post false or defamatory information about a person or organization.

• **Respect for Privacy**

- You will not re-post a message that was sent to you privately without the permission of the person who sent you the message.
- You will not post private information about another person.
- You will not access another individual's materials, information or files without permission.
- You will not use someone else's password, user account, or logon.
- You will not gain unauthorized access to resources.

• **Respecting Resource Limits**

- You will use the system only for educational and career development activities.
- You will not download large files unless approved by the teacher in charge. If necessary, you will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer.
- You will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- You will not download and/or listen to radio streaming, video streaming, using any online telephone resource, or sharing music and/or video due to bandwidth restrictions.
- You will not download or install from any other sources any non-curriculum software unless approved by a principal or network administrator. This includes, but not limited to, non-educational games, peer-to-peer file-sharing software, remote control software, optimizing utilities, networking utilities, shareware software, freeware software, and Internet messengers. All software installed on district computers must be licensed and approved. Pirated software will not be tolerated.
- You will not intentionally waste limited resources.

• **Plagiarism and Copyright Infringement**

- You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. Reproduction of a work includes using the work in another written form or posting the work or portion of the work, on the Internet. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be confusing. If you have questions, you should ask your teacher.

• **Inappropriate Access to Material**

- You will not use the school district network to access harmful matter or material that is profane or obscene (pornography), that advocates illegal acts, or advocates violence or discrimination towards other people (hate literature). This may include certain song lyrics and related materials.
- If you mistakenly access inappropriate information, you should immediately tell the teacher or school administrator in charge. This will protect you against any claim that you have intentionally violated this policy.
- Your parent/guardian should instruct you if there is additional material that they think it would be inappropriate for you to access. The district fully expects that you will follow your parents' instructions in this matter.

• **Your Rights**

- Free Speech
 - Your right to free speech, as set forth in the district's disciplinary code, applies also to your communication on the district's network and on the Internet, except as otherwise set forth in the Acceptable Use Policy. The school

district network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict your speech for valid educational reasons.

- **Search and Seizure**

- You should be aware that computer files and communications on the district's network and all over the Internet are not private or secure.
- *Use of mobile wireless Internet devices (including but not limited to Hotspots, MiFi's, personal Bluetooth) other than those provided by the district is prohibited and subject to seizure.*
- Students will limit their use of the system to classroom activities, teacher-directed activities, library-related research, or career development. Use of the system for any other purpose, personal or otherwise, is prohibited unless approved in advance.
- The district may monitor your use of the Internet and the district's computer resources, *(including but not limited to laptops, tablets, smart phones, cell phones, USB drives, iTouch devices, MP3 players)*, your e-mail, personal electronic devices, Internet files, and Internet access, at any time without advance notice or consent when there is a reasonable need to do so. Passwords must be reported. Monitoring of the system may lead to discovery that you have violated the Acceptable Use Policy, the district's disciplinary codes or the law. *The district reserves the right to suspend the use of personal electronic devices.*
- *Your parent/guardian has the right at any time to see the contents of your files.*

- **Due Process**

- Violating this policy may result in one or all of the following: restricting network access; loss of network access; disciplinary or legal action including, but not limited to, suspension or expulsion and/or criminal prosecution under appropriate local, state and federal laws; assessment of the cost of damages to hardware/software.
- The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school district network.
- In the event there is a claim that you have violated this Policy of the district's disciplinary code in your use of the school district network, you will be provided with written notice of the suspected violation and an opportunity to be heard in the manner set forth in the district's disciplinary code.
- Major violations of the district's Acceptable Use Policy by a student will result in the loss of use of all computing equipment and Internet access, even if this causes the student to fail a class. The student may be able to regain computing privileges the following school year. If this occurs, the student will be given the opportunity to remove his/her school-related files.
- If the violation also involves a violation of the district's disciplinary code, it will be handled in a manner described in the district's disciplinary code. Additional restrictions may be placed on the student's use of their network account.

- **Limitation of Liability**

The district makes no warranties of any kind, either express or implied, that the functions or services provided through the school district network will be error-free or without defect. The district will not be responsible for any claims, damages, or injury of any nature whatsoever, which users may suffer as a result, whether directly or indirectly, of any use of the school district network, including, but not limited to, personal injury, emotional distress or suffering, or loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising from the unauthorized use of the school district network, including, but not limited to, the purchase of products or services.

REV. 0313Revisions italicized.