

Internet Safety Policy

The Colmesneil School District has set in place an Internet Safety Policy that is based upon three parts: the Children's Internet Safety Act, our District Acceptable Use Policies and an Internet Safety Curriculum. The goal of the Colmesneil School District is to teach twenty-first century skills to our students while maintaining a safe environment for them to learn in.

Part 1 – Children's Internet Protection Act

It is the policy of the Colmesneil School District following the guidelines set forth by the Children's Internet Protection Act to:

- prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
- prevent unauthorized access and other unlawful online activity;
- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

To the extent practical, the Barracuda shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, the Barracuda may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

- unauthorized access, including so-called 'hacking,' and other unlawful activities; and
- unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

It shall be the responsibility of all members of the Colmesneil School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Procedures for the disabling or otherwise modifying any of the filtering on the Barracuda shall be the responsibility of the Technology Committee or designated representatives.

Part 2 – Pieces of our Acceptable Use Policies

The Colmesneil School District enforces guidelines set forth in our Acceptable Use Policies that are signed yearly by students who use our network for educational purposes and signed once by our staff. These policies are updated yearly to conform to our ever changing technology.

Network Use:

- All use of the system must be in support of education and research and consistent with the mission of the district. District reserves the right to prioritize use and access to the system.

- Any use of the system must be in conformity to state and federal law, and district acceptable use policy. Use of the system for commercial solicitation is prohibited.
- No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.
- Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on the system and/or damage the components of an entity on the network is prohibited.
- Users are responsible for the appropriateness of the material they transmit over the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
- Use of the system to access, store, or distribute obscene or pornographic material is prohibited.

Security:

- System logins or accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
- Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity on the network.
- Users should change passwords regularly and avoid easily guessed passwords.

Personal Security:

- Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian.
- Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
- Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications.

Copyright:

- The unauthorized installation, use, storage, or distribution of copyrighted software or materials on district computers is prohibited. All users of the network shall comply with current copyright laws.

Filtering and Monitoring:

- Filtering rules are applied on all student computers with access to the Internet along with a filtering system on the network itself to cover onsite filtering. This blocks access to visual depictions that are obscene, child pornography, or harmful to minors.
- Educational staff will, to the best of their ability, monitor minors' use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet, and restrict their access to materials harmful to minors.

General Use:

- No person shall have access to the network without having a signed Acceptable Use Policy must be on file with the district.
- Nothing in these regulations is intended to preclude the supervised use of the network while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.

For security and administrative purposes the district reserves the right for authorized personnel to review network use and content. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity. Violation of any of the conditions of use may be cause for disciplinary action.

Part 3 – Internet Safety Curriculum

The Colmesneil School District has set in place the following Internet Safety Curriculum to further educate our students. The curriculum has been integrated into the current computer classes/lessons and also integrated into the counseling curriculum.

The curriculum covers the following information:

- Unit 1 – Safety & Security Online
 - Private Identity Information
 - Meeting People Online
 - Security
 - Online Privacy
- Unit 2 – Manners, Bullying, and Ethics
 - Cyber Bullying
 - Cyber Citizenship
 - Ethics and Property
 - Netiquette
- Unit 3 – Research and Information Fluency
 - Search Engines and Directories
 - The Nuts and Bolts of Searching
 - Evaluating Web Sites
 - Homework Help
 - What about the Library?
 - Recognizing Commercial Intentions
- Unit 4 – Authentic Learning and Creativity
 - Authentic Learning
 - Creativity
- Unit 5 – Twenty-First Century Challenges
 - Communication Inventions
 - What is Cyberspace?
 - How Does the Internet Work?
 - Into the Future

The Colmesneil School District recognizes technology as a basic skill necessary for success in the 21st century. Because no aspect of communication or employment has been left untouched by the Information Age, it is essential that students be equipped with the fundamentals and be given the opportunity to acquire advanced capabilities. While learning these tools it is imperative for the students to be in a safe and secure environment onsite as well as offsite.