Purpose

It is the intention of Ridley School District in publishing an Acceptable Use Policy to maintain the district's established culture of openness, trust and integrity. The Board is committed to protecting the district, its students, and employees from illegal or damaging actions by individuals, either knowingly or unknowingly, using the computer and other electronic systems of the district.

All technology devices will be used for instructional purposes in serving the needs of the district and its students, faculty and community. Any internet or network systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet and Intranet browsing, File Transfer Protocol (FTP), and voicemail systems (hereinafter the "Information Systems") will be used in the academic environment. It is the responsibility of every user of the Information Systems to know these guidelines and to conduct his/her activities accordingly. To ensure enforcement of this policy, the district shall reasonably monitor the use of technology resources through direct supervision and other electronic monitoring tools.

Authority

All information that is available or received via the Information Systems does not imply endorsement by the Board of the content, nor does the Board guarantee the accuracy of information received. The Board shall not be responsible for any information that may be lost, damaged or unavailable when using the Information Systems or for any information that is retrieved via the Information Systems.

The Board provides employees, students, and guests (users) with hardware, software, access to the district's electronic communication systems and network, which includes Internet access, whether wired, wireless, virtual, cloud or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, parents/guardians, Board members, vendors and consultants.

The Board recognizes that as technologies affect the manner in which information may be accessed, communicated and transferred by members of society, those changes may also alter instruction and student learning. Telecommunications, electronic information services and networked services significantly alter the information landscape by opening schools, classrooms and library media centers to a broader array of resources. The Board supports access by students to rich information resources, along with the development by staff of appropriate skills to analyze and evaluate such resources.

In making decisions regarding student access to telecommunications and networked information resources, the teaching staff should consider the district's stated educational mission and goals.
instructional software and hardware should support and enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of the students.

It is the responsibility of all district users to use the computer network resources in a manner that adheres to all guidelines included in this document and protects the privacy and rights of all students and other staff members.

The Board reserves the right to log, monitor and review Internet, email and other network uses. Any user of district computers, servers, network resources, and other technology devices agrees and consents to this monitoring. Users should expect that data stored on district servers, computers, or on other devices that are district approved (i.e. cloud-based services) will not be private. District administrators may, as deemed necessary, review student and/or staff content and communications to maintain system integrity.

The district maintains an Internet filter as a protection measure pursuant to the Children's Internet Protection Act (C.I.P.A). No Internet filter is foolproof, and it remains the responsibility of staff to monitor student use of any network or electronic resource. Any inappropriate content received over the district network on personal or district-owned devices should be immediately removed and reported to a teacher, building or district administrator.[1]

All students, teachers and administrators who use networked resources including the Internet and electronic mail must be familiar with this policy and sign a form that they have reviewed it and agree to the limitations herein.

**Guidelines**

**Equipment and Network Access**

Access is a privilege, not a right. Access entails personal responsibility. The network services are provided for educationally related communication, research and other instructional activities. Access to network services will be provided to students who agree to act in a considerate and responsible manner. Abuse of equipment or disregard of the district student guidelines for its use will result in disciplinary actions.[2][3]

**Electronic Mail**

Students may use electronic mail accounts for sending and receiving documents and correspondence that conform to curriculum needs. The district is not responsible for monitoring or supporting non-district email accounts on district or personal devices. Students are not permitted to use district computers, network resources, or any other electronic devices, both district-owned or personal, to check their electronic email accounts for noninstructional purposes.

**Content Development**

Students may create and collaborate using any Web 2.0 tools, district or personal devices, or other Internet-based resources only under the direction of a teacher or administrator, and activities must be related to curriculum and instruction.

Users should assume that all materials available on the Internet are protected by copyright. Users shall not forward, download, or upload any copyrighted material without prior approval of the supervising teacher, the Director of Technology, the Assistant to the Superintendent, or the Superintendent or designee. Any material obtained from the Internet and included in one's own work must be cited and credited by name or by electronic address or path on the Internet. Information obtained through email or news sources must also be credited as to sources. It is the responsibility of all students to cite resources using a proper citation format. The district and its Internet service make no guarantees, implied or otherwise, regarding the factual reliability of data collected through the Internet.[4][5]

Not all material accessible through the Internet is of educational value. Students are expected to refrain from seeking, accessing, or downloading material that is not relevant to their assignments or course work. No students may upload or download material to or from Internet sites without permission from his/her teacher. Students must not access chat rooms unless discussions pertain to
instructional objectives. Games must not be played, accessed or downloaded unless they are approved by the building principal and the teacher in charge. The district will take reasonable precautions to filter out controversial materials; however, it is impossible to monitor all materials and controversial information.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.
2. Cyberbullying awareness and response.

Other Collaboration Software

The district recognizes that part of 21st century learning is adapting to the changing methods of communications via collaborative networking websites. Students are encouraged to use district-approved collaborative networking tools as an extension of the instructional setting.

Collaborative networking should be used for instructional purposes only and should follow the guidelines listed below:

1. Students should only access approved collaborative networking sites under the guidance of their teachers, which is in accordance with the approved curricula of the Ridley School District.
2. Students are expected to keep their collaborative networking site content consistent with honesty, respect, and consideration that would be used in a face-to-face environment and be in accordance with the highest academic and behavioral standards.

Restrictions on the Use of the District Network

The following activities are not permitted on the district network, on district devices, on personal devices used on school premises, or district-approved websites by staff, students, and guests:

1. Use for inappropriate or illegal purposes.
2. Use for commercial or for-profit purposes.
3. Use for lobbying or political purposes.
4. Use to infiltrate or interfere with a computer system to damage or remove data, files, operations, software or hardware components.
5. Use for hate mail, harassment, discriminatory remarks, threatening statements and other antisocial communication on the network. This includes accessing or disseminating information concerning guns, bombs, explosives or any weapon.
6. Illegal installation, distribution, reproduction or use of copyrighted software or files (such as MP3 files). Any loading of unauthorized games, programs, files music or other electronic media on district computers will result in lack of privileges and/or criminal prosecution.
7. Use to access, view, obtain, or disseminate pornography of any kind.
8. Use to transmit material likely to be offensive or objectionable to recipients.
9. Use to obtain, copy or modify files, passwords, data or information belonging to other users.
10. Use to misrepresent other users on the network including use of another's email address or user account.
11. Use to upload, create or attempt to create a computer virus.
12. Unauthorized disclosure, use or dissemination of personal information regarding minors.
13. Use which involves any copyright violation or for copying, downloading or distributing copyrighted material without the owner's permission, unless permitted in accordance with the
Fair Use Guidelines. All students should be familiar with the Fair Use Guidelines which can be found on the district website.[5]

14. Use that is inconsistent with network etiquette and other generally accepted etiquette. This includes, but is not limited to, the following:

   a. Do not become abusive in messages to others.
   b. Do not swear or use vulgarities or other inappropriate language.
   c. Do not reveal any personal information such as but not limited to: address, phone number, social security numbers, and passwords.
   d. Recognize that district-provided email is not private or confidential.
   e. Respect the rights of others to an open and hospitable technology environment regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital or handicap status.[6]

15. Users must not vandalize school computers by causing physical damage, reconfiguring the computer system, attempting to disrupt the computer system, or destroying data by spreading computer viruses by any other means.

Security on any computer system is a high priority, especially when the system involves many users. Each user is required to report any security problems to a teacher, building administrator or central office administrator.

Disclaimers

Students should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on district devices and computer networks or stored in his/her district-provided resource. A teacher, building or district administrator may, at any time, review the subject, content and appropriateness of electronic communications or other computer files, and remove them if warranted, reporting any violation of rules to the building or district administration or law enforcement officials.

The staff, the school and the district are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on district resources, or for personal property used to access district resources.

The district will not be responsible for the accuracy, nature, or quality of information stored on district resources or gathered through student access.

The district will not be responsible for personal damages incurred due to information stored or posted on any network, both Internet and district networks.

The district will not be responsible for unauthorized financial obligations resulting from use of district-provided access.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means for enforcing the provisions of this policy.

Consequences of Inappropriate Use

The user, whether a student, employee, or guest is responsible for damages to equipment, systems or software resulting from deliberate or willful acts including neglecting proper student supervision.

In addition to other appropriate disciplinary procedures, failure to adhere to the policies outlined in this document may result in the loss of access to the Internet, email and/or network resources.[2][3]

Illegal activities, such as downloading of copyrighted music files, or use may be reported to the appropriate legal authorities for possible prosecution.
Guidelines for violations can be found in the individual building's student handbooks.

Legal

1. 47 CFR 54.520
2. Pol. 218
3. Pol. 233
4. 17 U.S.C. 101 et seq
5. Pol. 814
6. Pol. 103
18 Pa. C.S.A. 5903
18 Pa. C.S.A. 6312
18 U.S.C. 2256
20 U.S.C. 6777
24 P.S. 4601 et seq
47 U.S.C. 254