5.84/6.27

ACCEPTABLE AND RESPONSIBLE USE OF TECHNOLOGY FOR STAFF AND STUDENTS

The board provides its students and staff access to a variety of technological resources, including laptop computers. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school district's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The board intends that students and employees benefit from board owned and/or provided resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks and all devices that connect to those networks.

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

School district technological resources may only be used by students, staff and others expressly authorized by the Superintendent or designee. The use of school district technological resources, including access to the Internet, is a privilege, not a right.

Individual users of the school district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school district technological resources is use that is ethical, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Student Code of Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school district computers or electronic devices or who accesses the school network or the Internet using school district resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Furthermore, all students must adhere to the Technology Use Guidelines as set forth in the Student Code of Conduct. All students will be trained about appropriate on-line behavior as provided in policy, Internet Safety.

Before using school district technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School district technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school district technological resources for political purposes or for commercial gain or profit is prohibited. Student personal use of school district technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school district business and is not otherwise prohibited by board policy or procedure.
2. School district technological resources are installed and maintained by members of the Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Superintendent or designee.
3. Under no circumstance may software purchased by the school district be copied for personal use.
4. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Student Code of Conduct.
5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.
6. The use of anonymous proxies to circumvent content filtering is prohibited.
7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account

information or social security number of themselves or fellow students. In addition, school employees must not disclose on school district websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA). Users also may not forward or post personal communications without the author’s prior consent.

10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.
11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the technology director or designee.
12. Users are prohibited from engaging in unauthorized or unlawful activities, such as “hacking” or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.
13. Users are prohibited from using another individual’s ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.
14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner’s express prior permission.
15. Employees shall not use passwords or user IDs for any data system for an unauthorized or improper purpose.
16. If a student user identifies a security problem on a technological resource, he or she must immediately notify an administrator. Users must not demonstrate the problem to other users.
17. Teachers shall make reasonable efforts to supervise students’ use of the Internet during instructional time, to ensure that such use is appropriate for the student’s age and the circumstances and purpose of the use.
18. Views may be expressed on the Internet or other technological resources as representing the view of the school district or part of the school district only with prior approval by the superintendent or designee.
19. Without permission by the Superintendent or designee, users may not connect any personal technologies such as laptops and workstations, wireless access points and routers, etc. to a district owned and maintained local, wide or metro area network. Connection of personal devices such as iPods, smartphones, PDAs and printers is permitted but not supported by Oxford City School technical staff. The School System is not responsible for

the content accessed by users who connect to the Internet via their personal mobile telephone technology.

20. Users must back up data and other important files regularly.
21. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.
22. Students and Staff who are issued district owned and maintained laptops must also follow these guidelines:
    a. Keep the laptop secure and damage free.
    b. Use the provided protective book bag style case at all times.
    c. Do not loan out the laptop, charger or cords.
    d. Do not leave the laptop in your vehicle.
    e. Do not leave the laptop unattended.
    f. Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.
    g. Do not allow pets near the laptop.
    h. Do not place the laptop on the floor or on a sitting area such as a chair or couch.
    i. Do not leave the laptop near table or desk edges.
    j. Do not stack objects on top of the laptop.
    k. Do not leave the laptop outside.
    l. Do not use the laptop near water such as a pool.
    m. Do not check the laptop as luggage at the airport.
    n. Back up data and other important files regularly. Oxford City Schools Technology Department will at times perform maintenance on the laptops by imaging. All files not backed up to storage devices will be deleted during this process.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school district personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language. The superintendent or designee shall ensure that technology protection measures are used as provided in policy Internet Safety, and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology.

D. PARENTAL CONSENT

The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's e-mail communication by school personnel. In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary to create and manage such third party accounts.

E. PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

Under certain circumstances, the board may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

F. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the board's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

G. PERSONAL WEBSITES

The superintendent or designee may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school district or individual school names, logos or trademarks without permission.

H. DISCLAIMER

The board makes no warranties of any kind, whether express or implied, for the service it is providing. The board will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

SOURCE: Oxford City Board of Education, Oxford, AL
ADOPTED: July 22, 2008; Revised October 22, 2009; August 20, 2013, Re-adopted November 23, 2021
LEGAL REF: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq*.; 20 U.S.C. 6777; G.S. 115C-325(e).

INTERNET SAFETY POLICY

Introduction

This policy has been adopted in compliance with the Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (l).

It is the policy of the Oxford City School System (System) to provide technology resources, including Internet access, to its students and employees in order to more fully support the system's mission statement and to meet educational and instructional goals set by the system and the state. It is the intention of the Board that all technology resources will be used in accordance with any and all school/system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. This policy applies to all technology resources, regardless of purchase date, location, or funding source.

All users, in the process of logging onto the system's network, will agree to abide by all school and system policies. Students and staff must have the appropriate Acceptable Use Policy on file with the system prior to use. Visitors to the system must have the permission of school staff in order to access the Internet. Such permission may not be shared or transferred.

This Internet Safety Policy will be displayed in each school media center and computer lab. A copy of the policy will also be available in each school's office. Any questions about this policy, its interpretation, or specific circumstances shall be directed to the System Technology Coordinator before proceeding. Violators of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action. The administrators of each school will be responsible for establishing specific practices to enforce this policy at individual schools.

Technology Protection Measures

Filtering and Blocking

The System will make a reasonable effort to filter and block access to "visual depictions" that are obscene, contain child pornography, are harmful to minors, or that the Board determines is "inappropriate for minors." The software will filter all incoming Internet sites based on both URL (web site name) and IP address. URLs and IP addresses may be added to the filtered list in cases where the filtering system may not have accurately identified inappropriate sites as defined above.

All users are required to report any sites that contain inappropriate materials or materials harmful to minors. Students must report this information to their teacher. Teachers or staff members must report the information to the System Technology Coordinator. This includes any text, audio segment, picture, image, graphic image file, or other visual depiction that:

- taken as a whole, appeals to an interest in nudity, sex, or excretion,
- 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
- taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

Adult staff members may request a review of filtered sites. Adults, who are engaged in bona fide research or need access to blocked sites for other lawful purposes, may request a temporary release of specific sites at specific workstations to complete their work. Such requests should be directed to the System Technology Coordinator.

Monitoring

It is the responsibility of all teachers and employees to properly inform students/staff under their charge of this policy and to see that the policy is strictly enforced. Students using the Internet and World Wide Web will be under the direct supervision of the instructor. In addition, the system may use software to monitor Internet activity, as needed. Teachers will be provided a list of students and their current status regarding use of the Internet. Teachers who will be presenting Internet sites to students as part of the instructional process, must preview the sites they plan to incorporate to ensure their safety and suitability. If students are to independently access the Internet on a computer, the teacher must ensure that they have a signed Acceptable Use Policy on file. In addition, any student under the age of 18 must also have a signed Parent Permission Form on file. Finally, teachers must give students specific permission to independently access the Internet and monitor their activity while they are online.

Communicating Electronically

The System permits students to engage in electronic communications on a limited basis for educational purposes under the direct supervision of their teacher. All such communications are subject to school rules, the Student Acceptable Use Policy, any applicable laws, and the following safety and security measures.

In compliance with the Children’s Internet Protection Act, electronic communications (including but not limited to e-mail, chat and instant messaging) may not be used for: Unsafe practices such as:

- Contacting strangers or communicating with unknown individuals or
- organizations;
- Posting or forwarding other users' personal communication without the author's consent;
- Sending mass e-mails without the consent of the Principal or System Technology Coordinator;
- Sending or attempting to send anonymous messages;
- Disclosing, using, or disseminating personal information without authorization regarding minors including, but not limited to the following:

    - home and/or school address
    - work, home, school, or cellular phone numbers
    - full name
    - social security number, etc

- Harmful, malicious or unlawful practices such as:

    - Spreading viruses;
    - Spamming;
    - Hacking of any type;
    - Copyright infringement;
    - Engaging in any other unlawful activities.

- Commercial practices such as:

    - Selling or advertising products or services;
    - Purchasing products or services.

Posting to the Web

All users wishing to post pages or information on the System's web site must obtain prior permission and comply with Oxford City Schools Web Page Design Requirements. Students may not use technology resources operated by the school system to post information or graphics to personal web pages on the Internet.

The System prohibits posting of the following to school or system websites:

- Pictures of employees without their written consent.
- Pictures and other personally identifiable information without the permission in writing from the parent/guardian of the student involved.
- Pictures of students along with their full names. (Only first name and last initial of students may be used.)
- Personal information of any kind including but not limited to:
- Home and/or school address, work address;
- Home and/or school phone numbers;

- Full name;
- Social security number.
- Materials that infringe on any copyright held by others without
- Permission and acknowledgement.
- Any obscene, harassing or threatening materials.

The System does permit the posting of faculty/staff listings with their school contact information (phone extension, e-mail address, etc.) In addition, webmasters may link to other web sites provided the content on the linked site(s) meet, the safety and professional standards set out in system policies and the linking page contains a disclaimer for the downstream website content and links.

Online Behavior Education

All students will receive education about appropriate online behavior, including cyberbullying awareness and response and interacting with other individuals on social networking sites and in chat rooms. This education will be provided through the implementation of the Technology Course of Study, through Internet Safety awareness and education programs at each school, and through additional efforts made by the Student Services and other departments. In addition, educational materials and links regarding cyberbullying as well as safe and appropriate behavior will be placed on the System's website for access by parents and students.

Downloading from the Internet

Students may not download files of any type without the specific permission of their supervising teacher. Under no circumstances will students be permitted to download graphic, video, or audio files in any format that violate the letter or intention of this or any other school/system policy. No user may download any files which violate copyright laws.

Limitations of Liability

The System and its employees make no guarantee that the functions or the services provided by or through the system's network will be error-free or without defect. The Oxford City School System will not be responsible for any damage suffered by the user, including but not limited to, loss of data or interruptions of service. The System will not be responsible for any financial obligations arising from the unauthorized or inappropriate use of system technology.

Notice of Right to Change

With Board approval, this policy may be changed as deemed necessary to continue to ensure the safety of students and compliance with any and all laws and regulations.

Additional Restrictions

This policy is intended to work in concert with other system policies, procedures, and guidelines in order to ensure the safe, ethical, and educational use of all technology within the system.

SOURCE:	Oxford City Board of Education, Oxford, AL
ADOPTED:	July 22, 2008, Revised January 19, 2010