POLICY

13000-03

GENERAL COMMITMENTS - ACCEPTABLE USE OF TECHNOLOGY AND INTERNET USE POLICY

Adoption Date: August 10, 1999; Revised October 4, 2011;
Revised November 15, 2016; April 18, 2017;
Revised January 1, 2022

Legal Ref: 20 U.S.C. § 1232g; 34 CFR Part 99 (Family Educational Rights and Privacy Act, "FERPA"); 16 CFR 312 (Children's Online Privacy Protection Rule, "COPPA"); I.C. 5-14-3 (Indiana Access to Public Records Act).

Cross Ref:

I. Purpose

The purpose of this policy is to set forth practices, parameters, and guidelines for access to and use of Westfield Washington Schools' (WWS) electronic technologies, including electronic communications, WWS's network, and Internet social networking tools.

Definitions

The following definitions apply to this Policy:

"Confidential information" means information that is declared or permitted to be treated as confidential by state or federal law or WWS Policy, including the Family Educational Rights and Privacy Act (FERPA).

"Proprietary information" means information in which an individual or entity has a recognized property interest, such as a copyright or trademark.

"Electronic technologies" includes WWS owned, loaned, or leased computers and computer systems (including laptops, desktop computers, and work stations), public and private networks such as the Internet and WWS network access, phone networks, cable networks, electronic mail, telephone systems and cellular devices (including voicemail and text messaging), digital media players, copiers, fax machines (including transmission and receipt), audio-visual systems, tablets and e-readers, radio communications, computer-based research and/or communication, and any similar equipment or processes as they become available.

"School property" includes any building owned or leased by WWS; on WWS property or grounds (including parking lots, athletic facilities, etc.); in vehicles owned, leased, or operated by WWS; and during WWS events, even if held outside of WWS property (for example, prom or field trips).

"User" means a WWS employee, student, volunteer, contractor or subcontractor, or any other individual or entity using electronic technologies as defined above.

III. Educational Purposes

WWS employees shall use electronic technologies to: 1) further WWS's educational mission, vision, and goals; and 2) to support classroom activities, educational research, or professional enrichment. Use of WWS electronic technologies is a privilege, not a right. WWS's network, an educational technology, is a limited forum. WWS may restrict speech for educational reasons.

IV. Unacceptable Uses of Electronic Technologies and WWS Network

Electronic technologies are assets of WWS and are protected from unauthorized access, modification, destruction, or disclosure. The following uses of the electronic technologies at WWS are considered unacceptable:

A. Users **will not** use WWS electronic technologies to send, view, access, review, upload, download, complete, store, print, post, receive, transmit or distribute:

1. Pornographic, obscene, or sexually explicit material or other visual depictions;
2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process; and/or
4. Materials that use language or images that advocate violence or discrimination towards other people or that may constitute harassment, discrimination, or threatens the safety of others.
5. Materials that are harmful to minors, as defined by I.C. 35-49-2-2.

B. Users **will not** use WWS electronic technologies for political campaigning.

C. Users shall not alter, delete, or destroy data, information, or programmatic instructions contained on or in WWS electronic technologies without permission from the Superintendent or his or her designee (typically, Technology Services Group (TSG)). Personally generated files and documents may be deleted by the User who created them, unless they may include propriety information, a student's personally identifiable information, and/or information potentially subject to litigation.

D. Users shall not add, delete, or modify the default setup on individual lab computers or files on the file server without permission from authorized personnel from TSG. This includes changing screen savers, enabling file sharing capabilities, or installing personal software on hard drives or

network drives. Lab systems will be periodically checked and anything not authorized will be deleted.

E. Users shall not use a computer anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise to escape responsibility for their actions.

F. If a User creates a password, code, or encryption device to restrict or inhibit access to electronic technologies, the User shall provide access to that information when requested by the User's supervisor, teacher, TSG staff, or designee. The Superintendent, TSG staff, or a designee shall be authorized to override any password or encryption device to access the technology. **A User shall never use another User's password, or account, even with permission from the User.**

G. Users shall not take any action that could cause damage to electronic technologies, including knowingly transmitting a computer virus or other malware that is known by the User to have the capability to damage or impair the operation of electronic technologies, or the technology of another person, provider, or organization.

H. It is not the practice of TSG staff to routinely review the contents of a computer file or email associated with an individual's account; however, Users **do not** have an expectation of privacy in any use of electronic technologies or the content of any communication using electronic technologies. The Superintendent, TSG staff, or a designee may monitor the use of electronic technologies without notice to Users and examine all system activities in which the User participates. Monitoring shall not include monitoring a live communication between two or more parties unless at least one user is aware of the monitoring. Users' history of use, and all data stored on or sent to/from electronic technologies, shall at all times be subject to inspection by the Superintendent, TSG staff, or a designee without notice to the User before or after the inspection. In addition, use of electronic technologies may be subject to production pursuant to the Indiana Access to Public Records Act.

WWS employees, students, and visitors must remember that when using electronic technologies, including accessing WWS wireless internet, all communications can be reviewed at any time.

V. Employee and Student Use of Social Media and Personal Websites

WWS employees and students use social media, networking websites, personal websites, blogs, and similar Internet sites and applications on their personal time, but these activities may affect the educational environment. As such, WWS employees and students shall abide by the Acceptable Use of Technology administrative guidelines regarding social media use. Employees and students who violate the administrative guidelines may be subject to discipline as described below.

VI. Liability

Use of WWS educational technologies is at the User's own risk. The system is provided on an "as is, as available" basis. WWS is not responsible for any damage Users may suffer. WWS is not responsible for the accuracy or quality of any advice or information obtained through or stored on the WWS system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. WWS is not responsible for financial obligations arising through unauthorized use of the WWS educational technologies or the Internet.

Users accessing the Internet through personal devices (cellular devices, smart phones, laptops, tablets and e-readers, handhelds or any other similar device that is not the property of WWS) connected to or through WWS electronic technologies shall comply with this Policy. Users connecting personal devices do so at their own risk.

VII. Property

The electronic technologies provided by WWS and all information stored by that technology is at all times the sole property of WWS. Documents and other works created or stored on the WWS electronic technologies are the sole property of WWS and are not the private property of the User. This includes all information created using technology and/or placed on a website, blog, and/or other storage device.

Any recording made in or on school property, or connected to WWS technology by a wired or wireless link, may be subject to copyright and/or privacy laws, including personally identifiable information about a student protected by FERPA. If the Superintendent, TSG staff, or designee has reasonable suspicion to believe a recording, data, or image was made in violation of this Policy, the technologies or device may be confiscated by WWS employees and appropriate discipline imposed.

Users shall not copy, file share, install or distribute any copyrighted material such as software, database files, documentations, articles, music, video, graphic files, and other information, unless the User has confirmed in advance that WWS has a license permitting copying, sharing, installation, or distribution of the material from the copyright owner.

VIII. Training

All students and employees who work directly with students shall receive annual training on social media safety, cyber bullying, and appropriate responses.

IX. Fee for Services and Terms & Conditions

No User shall allow charges or fees for services or access to a database to be charged to WWS except as specifically authorized in advance by the Superintendent, TSG staff, or designee. A fee or charge mistakenly incurred shall be immediately reported to the Superintendent or TSG staff. Incurring fees or charges for services to be paid by WWS for personal use or without prior authorization may result in discipline as described below.

Users shall thoroughly review terms and conditions of any programs, software, or applications prior to accepting the terms and conditions. Users are responsible for ensuring the terms and conditions comply with WWS Policy and procedures and state and federal law. Users who are unsure of the terms and conditions shall contact the Superintendent or TSG staff prior to accepting any terms and conditions. Accepting terms and conditions that violate WWS policy or procedures or state or federal law may result in discipline as described below.

IX. Filter

In order to comply with the Children's Internet Protection Act ("CIPA") and IC 20-26-5-40.5, WWS shall use hardware or install software on computers and other technology devices owned by WWS to filter or block Internet access to materials that are harmful to minors. Access to inappropriate materials despite the presence of the filter shall be reported immediately to the TSG staff. The filtering software shall not be disabled or circumvented without the written authorization of TSG staff or designee.

IX. Violation

Violations of this Policy, including but not limited to, misuse of WWS electronic technologies or inappropriate use of social networking, may result in denial of access to technology or discipline. A violation by an employee may result in suspension or termination of employment. A violation by a student may result in suspension or expulsion. A violation by a third party contractor or subcontractor rendering services to WWS may result in immediate cancellation of the contract and pursuing damages.

Any User who has reason to believe anyone has violated this Policy shall immediately report the suspected violation to the employee's immediate supervisor or student's teacher or principal. Any User who has reason to believe he or she accidentally violated this Policy shall report the suspected violation immediately. An accidental violation, if reported immediately, may result in a reprieve from discipline. Users shall be responsible for immediately reporting any conduct that may qualify as bullying, threats, harassment, discrimination, or any other communications or conduct that may constitute a violation of WWS Policy, Student Code of Conduct, or the law.

If the Superintendent, TSG staff, or designee has reasonable suspicion to believe a User has violated this Policy or WWS rules related to technology, they may

investigate to determine if a violation has occurred. A decision made to discipline a User for violation of this Policy may be appealed in writing to the Superintendent within five (5) calendar days of WWS issuing the decision to the User. The Superintendent's decision concerning the discipline shall be final.