

Tippecanoe School Corporation Administrative Guidelines

7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

Staff members shall use School Corporation Technology Resources for educational and professional purposes only. Corporation Technology Resources may be used for incidental personal, non-work related purposes that do not interfere with the employee's performance of his/her job responsibilities, do not result in direct costs to the Corporation, do not affect other users use of the resources for education and work-related purposes, do not expose the Corporation to unnecessary risks, and do not violate applicable School Board policies, administrative guidelines, or applicable laws/regulations.

Use of Corporation Technology Resources is a privilege, not a right. When using Corporation Technology Resources, staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Staff members found to have engaged in unauthorized or inappropriate use of Corporation Technology Resources and/or Information Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the applicable collective bargaining agreement and Board policy, and/or civil or criminal liability. Prior to accessing or using Corporation Technology Resources and/or Information Resources, staff members must sign the Staff Technology Acceptable Use and Safety Agreement. Staff members must complete a mandatory training session/program before being permitted to access or use Corporation Technology Resources and/or Information Resources and/or being assigned a school email address.

This guideline also governs staff members' use of their personal communication devices (PCDs) when they are connected to the Corporation's Technology Resources, creating, using or transmitting Corporation Information Resources, or while the staff member is on Corporation-owned property or at a Corporation-sponsored activity. Staff are reminded that use of PCDs (including the sending of text messages) may generate a public record or an education record that needs to be maintained in accordance with the Board's record retention schedule and/or Federal and State law.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using Corporation Technology and/or Information Resources.

- A. All use of Corporation Technology and/or Information Resources must be consistent with the educational mission and goals of the Corporation.
- B. Staff members may access and use Corporation Technology and/or Information Resources only by using their assigned account and may send only school-related electronic communications using their Corporation-assigned email addresses. Use of another person's account/email address is prohibited. Staff members shall not allow other users to utilize their account/email address and shall not share their password with other users. Staff members may not go beyond their authorized access. Staff members are expected to take steps to prevent unauthorized access to their accounts by logging off or "locking" their computers, laptops, tablets, and personal communication devices when leaving them unattended.

- C. No user may have access to another's private files. Any attempt by users to access another user's or the Corporation's non-public files, or voicemail or e-mail messages is considered theft. Attempts to gain access to unauthorized resources or data/information either on the Corporation's computer or telephone systems or any systems to which the Corporation has access are prohibited. Similarly, staff members shall not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the Corporation's network.
- D. Staff members shall not intentionally disable any security features used on Corporation Technology Resources.
- E. Staff members shall not use Corporation Technology Resources or their personal communication devices to engage in vandalism, "hacking," or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; and the sale of illegal substances or goods).
 - 1. Slander and libel. In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Staff members shall not knowingly or recklessly post false or defamatory information about a person or organization. Staff members are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people, and harmful and false statements will be viewed in that light.
 - 2. Staff members shall not use Corporation Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, e-mails or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment is grounds for discipline, up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.

3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or data/information residing in Corporation Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of Corporation Technology Resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited.

Attempts to violate the integrity of private accounts, files or programs, deliberately infect the network or computers, laptops, tablets, etc., attached to the network with a "virus", and hack into any internal or external computer systems using any method will not be tolerated.

Staff members shall not engage in vandalism or use Corporation Technology Resources or their personal communication devices in such a way that would disrupt others' use of Corporation technology resources.

Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creating computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Staff members also must avoid intentionally wasting limited resources. Staff members must notify the building principal or IT personnel immediately if they identify a possible security problem. Staff members should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

4. Use of Corporation Technology Resources to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that 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 material that lacks serious literary, artistic, political or scientific value as to minors. If a staff member inadvertently accesses material that is prohibited by this paragraph, s/he shall disclose the inadvertent access to the building principal or IT personnel immediately. This will protect the user against an allegation that s/he intentionally violated this provision.

- F. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.
- G. Corporation Technology Resources shall not be used for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by staff members). Advertising, political lobbying, or campaigning is prohibited. This provision shall not limit the use of Corporation Technology Resources by staff members for the purpose of communicating with elected representatives or expressing views on political issues. Staff members may use Corporation Technology Resources for communication related to collective bargaining and union organizational activities.
- H. Staff members are expected to abide by the following generally accepted rules of network etiquette:
 - 1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing Corporation Technology Resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications made through or utilizing Corporation Technology Resources (including, but not limited to, public messages, private messages, and material posted on web pages).
 - 2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.
 - 3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a staff member is told by a person to stop sending him/her messages, the staff member must stop.
 - 4. Do not post information that, if acted upon, could cause damage or a danger of disruption.
 - 5. Never reveal names, addresses, phone numbers, or passwords of students while communicating on the Internet, unless there is prior written parental approval or it is otherwise permitted by Federal and/or State law.
 - 6. Check e-mail frequently and delete e-mail promptly to avoid excessive use of the electronic mail disk space. Nothing herein, alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public

record, student education record and/or a record subject to a Litigation Hold.

- I. All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected.
- J. Downloading of information onto school-owned equipment or contracted online educational services is prohibited, without prior approval from IT personnel; all downloads must be to floppy disk. If a staff member transfers files from information services and electronic bulletin board services, the staff member must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or software program that infects Corporation Technology Resources with a virus and causes damage, the staff member will be liable for any and all repair costs to make the Technology Resource once again fully operational.
- K. Privacy in communication over the Internet and through the Corporation's computer network is not guaranteed. To ensure compliance with these guidelines, the Corporation reserves the right to monitor, review and inspect any directories, files and/or messages stored on or sent/received using the Corporation's Technology Resources. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
- L. Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Corporation makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through Corporation Technology Resources will be error-free or without defect. The Corporation is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Corporation is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in class must be cited the same as references to printed materials. The Corporation is not responsible for financial obligations arising through the unauthorized use of its Technology Resources. Staff members will indemnify and hold the Corporation harmless from any losses sustained as the result of the staff member's misuse of Corporation Technology Resources.
- M. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form."

- N. Proprietary rights in the design of websites, apps and services hosted on the Corporation's servers remain at all times with the Corporation without prior written authorization.
- O. Staff members are reminded that student personally identifiable information is confidential and may not be disclosed without prior written parental permission.
- P. File-sharing is strictly prohibited. Staff members are prohibited from downloading and/or installing file-sharing software or programs on Corporation Technology Resources.
- Q. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the Corporation's users will be fully investigated and disciplinary action will be taken as appropriate.
- R. Preservation of Resources: Corporation Technology Resources are limited. Each staff member is permitted reasonable space to store e-mail, web, and school/work-related files. The Board reserves the right to require the purging of files in order to regain disk space.

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the acquisition and sharing of copyrighted materials is illegal and unethical.

Unauthorized Printing

Corporation printers may be used to print only school/work-related documents. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The Corporation monitors printing by user. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the staff member.

Any questions and concerns regarding these guidelines may be directed to the Technology Director.

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended
20 U.S.C. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246
20 U.S.C. 677, 9134 (2003)

Revised 3/11/15
Revised 1/10/18

© Neola 2017