# Elmwood Local School District--STAFF
# Acceptable Use Policy for Technology and Network Use

Technology tools and resources have had a profound influence in education, in the workplace, and in everyday life. Users of technology are challenged with discerning appropriate boundaries of use and recognizing potential risks of constantly emerging technologies.  It is the Elmwood Local School District's intention to provide a framework of digital citizenship by which all technology users within the District will co-exist.  This document establishes a standard of expected behavior of good digital citizens.

In order for the Elmwood Local School District to be able to continue to make its computer network and Internet access available, all staff must take responsibility for appropriate and lawful use  of this access.  Staff must understand that one staff member's misuse of the network and Internet access may jeopardize the network.  Staff will be expected to frequently change passwords based on cyber security and NIST  best practices.  Staff will use Multi Factor Authentication based on cyber security and NIST best practices.

## Elements of Digital Citizenship

*I. Guiding Question:  Does your behavior represent good work ethic and productivity?*

    A. Select appropriate task

- Work at school.  Users are expected to use technology effectively and efficiently to complete their work, learning, collaboration, and educational research.  Use is monitored and no privacy should be assumed.  The District owns all data in the system.
- Separate work and personal. Elmwood staff  are expected to use District provided and authorized accounts and services for school work and personal accounts for personal activities. Staff should limit online communication/interaction with students to Elmwood Schools provided or authorized services. Also, we recommend not using personal accounts on district devices.
- Play at home.  Personal, entertainment, and social use of technology should not be done during the school day and not with school resources.
- Promote at home.  Use of school technology resources for political, religious, or commercial purposes is unlawful and is strictly forbidden.
- Access appropriate material.  While Internet access in District schools is filtered.  Users may not create, access, distribute or share information about unsuitable material.

    B. Use of Web 2.0 Tools for Twenty First Century Learning.

- Any online services provided to students, staff and/or parents, including but not limited to-- BrainPop, Dropbox.com, Google Workspace for Education, Microsoft 365 Online, and  any Educational Websites,  should be for educational purposes.
- In addition many of these services have individual End Use Licensing Agreements (EULA) which users must agree to.

*II. Guiding Question:  Does your behavior diminish technology resources for other users in the District community?*

    A. Care for technology resources

- Leave resources in good working condition for the next user.
- Report technical problems to IT Staff so  problems can be resolved.
- Avoid any behavior that interferes with the operation of school technology and network services. Disconnecting, changing configurations, hacking, breaking, mishandling, or other alterations will be viewed as vandalism.

Board Approved March 2024

B. Conserve resources

- Bandwidth.  Our Internet and network bandwidth is shared amongst nearly 1600 users.  Video, audio, games, and animations use a lot of bandwidth that will affect network and Internet speed.  Only use what is needed.
- Server space/Google or Microsoft OneDrive storage space.  Users have plenty of Cloud Storage to  store their work.  Only store files necessary to do your work and clean out obsolete files.  Users may not store anything that is not directly related to work on school drives.
- Consumables.  Please do not waste consumables (paper, ink, etc.).  Create, edit, submit, and present electronically when possible.  Only print portions needed and final products.
- Please restart/shutdown equipment frequently.  Please do not leave laptops, Chromebooks, or other devices with batteries, plugged in through the evening or holiday/summer break.

*III. Guiding Question:  Does your product improve knowledge and understanding?*

A. Create responsibly

- Be sure presentations shared with others in the online community contain well-documented, well-researched, accurate, and reliable information that is cited when appropriate.
- Proudly cite the work you have relied upon from other authors to build your knowledge base.
- Learn the difference between synthesizing from others' work and plagiarism. Never plagiarize.

*IV. Guiding Questions:  Does your conduct impact the safety, security or reputation of yourself and others? Is your behavior honest and legal?*

A. Safety

- Keep private information offline.
- Be careful how you present yourself online.  What you post may be viewed by anyone.
- Treat others with kindness and respect.
- Protect yours and others' personal and professional reputations.  High standards of online manner and conduct are expected from all users.  Users should refrain from any behavior/activities that would reflect negatively on themselves and/or the District.
- Create a positive environment.  Bullying, harassment, intimidation, or any behavior which disrupts a safe and positive working environment is strictly prohibited.

B. Security

- Protect your network accounts.  Do not share usernames or passwords; do not leave an account unattended or allow others to use it. Please sign out/lock your device before leaving it unattended.
- Create secure passwords with letters, numbers, and special characters.
- Only access your accounts and network locations.  You may not use or access others' accounts.  Do not access, modify, forward, or delete files created by another user without their permission.
- Be watchful to prevent viruses, spyware, and other malware from infecting the computer/network.
- Privacy of email or any electronic communication is not guaranteed and may become public information.
- Users are responsible for maintaining security of student information and other personally identifiable data and for upholding FERPA (20 U.S.C. § 1232g), the student confidentiality law (Ohio Revised Code Section 3319.321), the Ohio Privacy Act (Chapter 1347 of the Ohio Revised Code), and any other applicable privacy policies and regulations regardless of how information is accessed, transmitted, or stored.

C. Law and Ethics

- Users are responsible for following District rules and guidelines and state and federal law in their use of technology.
- Users will respect the ownership rights of work, ideas, or products and comply with plagiarism, copyright,

Board Approved March 2024

and/or piracy laws.  No illegal copying is permitted.  Citing sources of information is expected.

**Google Workspace for Education Policy (Elmls.net)**

In order to use Google's services as provided to Elmwood Local Schools, all participants must be aware of, agree to, and adhere to the following:

- When utilizing *Google Workspace for Education* services, you are bound by the Elmwood Local Schools Acceptable Use Policy, found at http://www.elmwood.k12.oh.us.
- Anyone in the Elmwood Local Schools utilizing *Google Workspace for Education* services must agree and adhere to the Google Terms of Service that will be presented for review when creating your account.
- Anyone in the Elmwood Local Schools utilizing *Google Workspace for Education* services must be aware that their data may be stored in data centers outside the borders of the United States.
- As stated in the Elmwood Local Schools AUP, anyone in the Elmwood Local Schools utilizing *Google Workspace for Education* services acknowledges that Elmwood Local Schools has the ability to monitor, use, or disclose their data, and that Google provides Elmwood Local Schools the ability to do so.
- Anyone in the Elmwood Local Schools utilizing *Google Workspace for Education* services will be supported through the Elmwood Local IT Staff.
- Anyone in the Elmwood Local Schools utilizing *Google Workspace for Education* services must acknowledge that Google can terminate their account if they fail to abide by the Google Terms of Service.

**Apps For Education**

- All Apps added to devices must follow COPPA and FERPA laws.
- Research the App and creator before submitting it for review.
- Each APP must be submitted for review with the proper screening work completed by the staff member requesting the APP.
- Additional APPS may collect student data,  examples are EDPuzzle and Screencastify, but are not limited to these APPS
- Any student age 13 or under will need parental consent to use third party web apps according to COPPA.

## ELECTRONIC MAIL (E-MAIL)

### Non-Acceptable Uses of Electronic Mail:

- Transmission of any material in violation of any US or state regulation.  This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secrets.
- Use for-profit activities (consulting for pay, sales, etc.) or use for-profit institutions.
- Extensive private or personal use.
- Any malicious attempt to alter, destroy or reduce the usability of data of another user, agency, or network connected to the Elmwood Schools network through NOECA.  Viruses, trojan horses, and worms are prohibited.
- Abusive language, vulgarities, obscenities and other inappropriate language, including reposting or quoting obscene and/or inappropriate material.
- Sending or forwarding or participating in chain letters

### SOCIAL MEDIA

- Use school social media for school related material.
- We highly recommend creating a separate social media account for school related material.  Do not post student pictures/material on personal social media accounts.
- Keep social media accounts to Facebook, Twitter, and Instagram.  Any other platform will need administrator approval.
- Be cautious adding students directly to your accounts
- Always check which students are NOT allowed to have their photos/information on social media.

Board Approved March 2024

Electronic mail (e-mail) is not guaranteed to be private.  Mail may be delayed, misdirected or not be deliverable.  System administrators reserve the right to monitor system resources and user accounts while respecting the privacy of the user account.  School district administration may request access to electronic mail with due cause. The Elmwood Local School District retains the right to refuse an email account to any person without further justification.

## Personal Devices

Malware attacks on school districts continue to rise across the world.  To ensure our technology environment remains safe for all users, staff are **<u>NOT</u>** to bring personal computers/devices into the school and/or connect to our network.

## Consequences of Improper Use

Use of personal equipment to violate this Policy on school property is prohibited and is subject to search and seizure for up to thirty (30) days.  Consequences for individuals violating the Acceptable Use Policy vary depending on the nature and seriousness of the violation.  Consequences might include disciplinary action, loss of technology access, reimbursement of expenses and/or damages, and/or involvement of law enforcement agencies.

The technology department has the right to disable network accounts when an incident is reported and the account will remain disabled until an investigation is conducted.

## No Warranties Created

The Elmwood Local School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this Policy.  It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy.  By signing this Policy, users are taking full responsibility for his or her use, and hold the School, the Elmwood Local School District, the Data Acquisition Site that provide the computer and Internet access opportunity to the Elmwood Local School District and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user.  The user agrees to cooperate with the School in the event of the School initiating an investigation of a user's use of his or her access to its computer  network and the Internet, whether that use is on a School computer or on another computer outside the Elmwood Local School District's network.

**Elmwood Local Schools
Internet Authorization Form**


##      EMPLOYEE AGREEMENT

***Every employee, regardless of age, must read and sign below:***


    I have read, understand and agree to abide by the terms of the Acceptable Use, E-Mail & Internet Safety Policy of the Elmwood Local School District. Should I commit any violation or in any way misuse my access to the Elmwood Local School District's computer network and the Internet, I understand and agree that my access privilege may be revoked and disciplinary action may be taken against me.


_____

Employee name   (PRINT CLEARLY)         Home phone


_____

Employee signature                      Date


_____

Address


\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

*Legal References*:             Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
                          Communications Act of 1934, as amended (47 U.S.C. 254[h],[l])
                          Elementary and Secondary Education Act of 1965, as amended (20 U.S.C.
                                6801 et seq., Part F)

                                              6801 et seq., Part F)


\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

*Legal References*:             Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
                          Communications Act of 1934, as amended (47 U.S.C. 254[h],[l])
                          Elementary and Secondary Education Act of 1965, as amended (20 U.S.C.
                                  6801 et seq., Part F)

                                              6801 et seq., Part F)


Board Approved March 2024