

## **NETWORK/INTERNET USE**

### **Background**

The Mt. Lebanon School Board recognizes that telecommunications and other new technologies have changed the ways through which information may be accessed, communicated, transferred and exchanged by members of society. Those changes will also affect student instruction and learning. The Board is committed to the effective use of technology as a tool to advance the District's educational program and curriculum and to enhance the quality of student learning, as well as to promote the efficiency of District operations. The District's electronic communications system ("Network") will provide unprecedented opportunities for students and staff to communicate, learn, access, exchange and publish information. The resources available through this Network, and the electronic communication and information research skills that students will develop using it, are of significant and growing importance in the learning process and preparation of students for success in the future. The Network includes the Internet, which is a global information and communication network that provides a tremendous opportunity to bring previously unimaginable education and information opportunities to our students. The Internet is, however, a public space. As is true with all public spaces, there is a potential that students may come in contact with potentially harmful or inappropriate material or people through the Internet. Therefore, use of the Internet by students necessarily raises concerns about student safety and security. The District will provide guidance to help students learn to use the Internet in a safe and responsible manner. The Board believes that the advantages to students and staff from access to the valuable information and interaction available on the Network (including the Internet) outweigh the risk that users may misuse the Network for purposes which are inconsistent with the curriculum and educational goals of the District. The Board further believes that these risks can be reduced through the adoption of this policy and related procedures.

### **Definitions**

The term "Network" shall be interpreted to include any and all District owned computers, servers, any hardware or software, the District's local area network (LAN), Regional Wide Area Network (RWAN) all wireless access points, the Internet, Internet 2, the District Intranet, self contained electronic mail systems, and any other elements of the District's computer, telecommunications or electronic communication/information systems. "Network" shall include District issued Google accounts to students, teachers and administrators (Drive, Gmail, Docs, Sites, Apps, Chromebooks and Courseware), and other similar collaborative programs and software adopted by the District.

### **Objective**

To provide for and establish a reasonable and equitable policy for use of the Network by students and staff and for development of applicable rules and regulations regarding the acceptable use of the Network as a tool to support and advance the District's educational program, curriculum and internal operations and, at the same time, to promote a policy of Internet safety.

## Policy

### A. Acceptable Network Use

The Network may be used only as a tool to support and advance the functions of the District as well as its curriculum and educational programs. Access to the District's Network is a privilege and not a right. Users of the Network are responsible for their behavior and communications over the Network and access to Network services will be provided only to those staff and students who agree to act in a considerate and responsible manner and in accordance with the District's rules and regulations as may be adopted and amended from time to time. All staff and students (and/or the students' parents, depending upon the age of the student as specified by administrative procedures) who wish to use the Network must sign one or more Network agreements whenever requested by the District.

Students may use the Network only in support of educational activities consistent with the educational objectives of the District. Faculty and staff may use the Network primarily in support of education and research consistent with the educational objectives of the District. Faculty and staff may access the Network for limited personal use but not for any commercial or business use; however, such personal use may not violate any applicable rules and regulations or applicable administrative procedures or interfere with job performance. Use of the Network must be in compliance with applicable laws, including all copyright laws, and all materials on the Network should be presumed to be copyrighted.

Staff or students who claim that this policy is denying them access to material that is not within the prohibitions of this policy shall direct their claim, in writing, to the District's Director of Technology or his/her designee, who shall review the matter and respond promptly.

### B. Inappropriate Use and Activities

The District reserves the absolute right to define inappropriate behavior or improper use of the Network, adopt rules and regulations applicable to Network use, determine whether an activity constitutes inappropriate use of the Network, and determine the consequence of such inappropriate use. Inappropriate network use shall include (but not be limited to) obscene, pornographic or offensive matter; vulgarity, harassment, intimidation, insult or ridicule of another; damage or waste of property; use of another's password or misrepresenting one's identity; "hacking" and other illegal online activity; unauthorized disclosure, use, and dissemination of personal information regarding minors; use for commercial purposes or illegal purposes, or any other use deemed inappropriate by the District, or in violation of any other District policy, administrative procedure, law, regulation or code of conduct. Inappropriate use of the Network may, for students, result in disciplinary action up to and including suspension or expulsion from school or, for employees, suspension or termination of employment. Where circumstances warrant, inappropriate use of the Network may be referred to law enforcement authorities.

When a school administrator has a reasonable belief that a student has violated a school rule, policy or the law, and there are facts and inferences that would cause a reasonable person to

suspect that a search of the student's personal technology device(s) will reveal evidence of a violation of said school rule, policy or the law, the administrator shall have the authority to search such device, provided that the scope of the search relates to the suspected violation giving rise to the reasonable suspicion.

#### C. Protection and Filtering

The District shall employ appropriate technology protection measures with respect to use of the Internet by students. The District will use software programs and select online servers that are designed to block or filter access to visual depictions that are (among other inappropriate things) obscene, pornographic or harmful to minors. In addition, the filtering equipment will be used to ensure that the Network may not be used to access, use, disclose or disseminate personal identification information regarding students or staff as well as to screen out inappropriate text. The District will endeavor to keep the blocking and filtering technology up-to-date, but it is not possible to guarantee that all inappropriate content will be successfully blocked or filtered.

The District shall educate students and employees about appropriate/inappropriate online behavior, including interacting with other individuals on social networking websites and chat clients as well as cyber bullying awareness.

The District encourages the use of student-owned personal technology devices where such use is in support of student learning. When such student-owned technology is in use during the school day, students are required to access the Internet via the District's wireless network and not through a cellular network or non-District "hotspot." The use of student-owned technology devices to access the Internet shall be subject to all of the regulations contained in this policy. In order to protect the Network, users may not connect non-District computers or peripherals directly to the wired Network. Such devices may only be connected to the District's wireless network.

In addition, users may not use personal software programs on the Network or transfer files, programs, shareware or software from information services, third-party Networks or websites, or any other external source without the written permission of the Director of Technology. Data discs, memory sticks, and other temporary file storage devices may be used with District computers for the sole purpose of transferring user data files for appropriate school-related work.

#### D. Ownership and Retention

Any and all material or information placed in any file on the Network becomes District property. The District reserves the right to indefinitely store and access any such material or information on the Network, including personal and electronic mail files, and to dispose of any material or information contained therein without prior notice. The District further reserves the right to monitor online activities and review, record or log Network use. The District also reserves the right to limit content of District websites to District-approved information related to District curriculum and programs.

Administrative Responsibility

It shall be the responsibility of the Administration to develop and publish written administrative procedures and/or guidelines for the implementation of this policy, including taking steps related to: (i) rules and regulations for appropriate Network use; (ii) website access and website links; (iii) a Network agreement form; (iv) security measures including password procedures; (v) measures designed to restrict access to harmful or inappropriate matter on the Internet; (vi) procedures for promoting the safety and security of students when using electronic mail; and (vii) prevention of unauthorized access and any other matter deemed necessary or advisable to implement this policy.

Communication

This policy shall be communicated to:

1. All District Staff
2. Students and Parents
3. The Mt. Lebanon Community

Adopted December 15, 1997  
Revised May 21, 2001  
Revised July 19, 2004  
Revised April 18, 2005  
Revised April 19, 2010  
Revised February 20, 2012  
Revised May 23, 2016  
Reviewed September 11, 2023