

## Acceptable Use of the District's Electronic Resources

### **Applicability**

This section applies to all “users” of the District’s electronic resources, including students and employees.

### **Acceptable Use – General**

Only authorized users may access the District’s electronic resources. All of the District’s technology resources, including, but not limited to:

1. The District’s local-area and wide-area networks, including wireless networks (Wi-Fi), District-issued Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District’s networks or to any District-issued online account from any computer or device, regardless of location;
3. District-owned or District-issued computers, laptops, tablets, phones, or similar devices.

Access to the District’s electronic resources is intended for educational and extra-curricular purposes and District business. Employees may use District electronic resources for incidental personal use during non-work times as long as that use complies with the other parameters of this AUP and any implementing procedures and does not interfere with the employee’s job duties or the provision of education and services by the District. Students may only use the District’s electronic resources for incidental personal use during non-instructional times if the student is authorized to use the particular electronic resource at the time used, the use complies with the other parameters of this AUP and any implementing procedures, and the use does not violate any other District policy or state or federal law, including Policy 7:190 Student Behavior implementing procedures.

Users must take reasonable steps to protect the security of the District’s electronic resources. Among other things, users may not share passwords or allow others to access electronic resources using the user’s password or profile. Any user who becomes aware of a security breach must notify a District representative immediately.

Users are responsible for appropriately using the District’s electronic resources. If a user has questions about whether a particular use is acceptable, the user is expected to speak to a supervisor (for employees) or teacher or administrator (for students and all other users) before engaging in the particular use.

Upon separation from District 41, users will securely return to the District, or verify secure destruction of, any District 41 record in any format. Such records may not be retained, copied or transferred to anyone or any other electronic device or storage vehicle of any kind. These requirements do not apply to those records which the District has: 1) made available to the public; 2) made available to the record holder as an employee under the Illinois Personnel Records Act; or 3) advised the record holder in writing or electronically that the records are not exempt from disclosure under the Illinois Freedom of Information Act or any other confidentiality law, such as the Illinois School Student Records Act.

### **Acceptable Use - District-Issued Technology (Including One-To-One Programs)**

The District may issue technology to users, including students and employees, for educational or extra-curricular purposes and/or District business, including through a one-to-one program. Use of District-issued technology is governed by this AUP, including the Acceptable and Unacceptable Use provisions of this AUP, regardless of when, where, or for what purpose the use occurs. This includes use that occurs outside of normal school hours (for students), before or after work times (for employees), for personal purposes, and/or off District property or away from related events or activities.

The user is responsible for reasonable care of District-issued technology at all times during which the technology is issued to the user, regardless of whether the technology is on school property or at related events or activities. This includes the requirement that the user not allow others to use the technology without authorization from an administrator. The procedures implemented by the Superintendent or designee for this AUP may contain further guidelines regarding responsible use, as may handbooks and other guidelines issued at the school level. Costs associated with repair or replacement of technology damaged as a result of a user's failure to exercise reasonable care shall be the responsibility of the user, including any fees for insurance premiums and deductibles, regardless of whether the damage is caused by the user or a third party. Users may be required to obtain and/or pay for insurance for District-issued technology in order to be issued such technology by the District.

Students may only use or access District-issued technology outside of school with parental or guardian supervision. The District is not responsible for unacceptable use of District-issued technology by students at any time, including outside of school, although students may face consequences for such misuse under this and other District policies.

### **Unacceptable Use – General**

Users are expected to conform to general expectations of norms outlined in this AUP and other District policies when using the District's electronic resources. This AUP sets forth some general examples of unacceptable use, but does not attempt to set forth all prohibited uses.

The following are examples of uses of the District's electronic resources that are strictly prohibited:

- Any use at a time or in manner that is not authorized or approved, or in a manner that causes or reasonably could be foreseen to cause a substantial and material disruption to the educational environment or invasion of the rights of others;
- Knowingly or recklessly causing a security breach or disruption of service to an individual or system;
- Damaging District electronic resources or the electronic resources of others via District electronic resources, including accessing or attempting to access any content to which the user is not authorized, including "hacking";
- Misrepresenting one's identity or using another person's password, user profile, or technology or allowing another to use one's identity, password, or technology without authorization;
- Any use in a manner that violates State or federal law including using materials that are subject to intellectual property laws, such as copyright and trademark laws, without authorization;
- Any use that violates any Board policy, including policies addressing bullying, harassment, and hazing, and student and employee discipline policies or codes of conduct;
- Publishing or transmitting private information, including photographic, video, and audio depictions of others, without authorization;
- Any transmission, access, creation, or transmission of material that is sexually graphic or explicit, obscene, threatening, intimidating, abusive, harassing, or otherwise indecent, or that reasonably could

- be interpreted as promoting illegal activity, including illegal drug use;
- Any use for a commercial purpose where the user does not have the express written authorization of the Superintendent or designee;
  - Uploading or downloading material, including software, without express authorization of a member of the District's technology staff;
  - Accessing or participating in any games without the express authorization of a supervisor (for employees) or teacher or administrator (for students and other users), or using the District's electronic resources for more than incidental personal use;
  - Providing personal information, including photographs, about themselves or another; and
  - Any attempt to do any of the above.

A user should notify the District's Complaint Manager or Nondiscrimination Coordinator immediately under Board Policy 2:260 Uniform Grievance Policy upon receipt of a communication through the District's electronic resources that the user believes is inappropriate or that makes the user feel threatened or uncomfortable.

### **Internet Filtering, Safety, and Security Measures**

The District will implement technology protection measures on each District computer with Internet access, including filtering devices to block user access to visual depictions of material that is obscene, pornographic, or otherwise harmful to minors as defined by the Children's Internet Protection Act (CIPA). The procedures implemented by the Superintendent or designee for this AUP shall allow users to make requests, including anonymous requests, to disable the filter for bona fide research or other lawful purposes.

The District also will take steps, to the extent practical, to promote the safety and security of users of its electronic resources. The steps taken shall include efforts to prevent inappropriate network use such as: (a) unauthorized access, including "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors. The steps taken also shall include efforts to protect student and employee privacy, safety, and security when using electronic communications.

The District and its employees shall take steps, to the extent practical, to educate, supervise, and monitor students' uses of electronic resources as required by CIPA and other federal and state laws.

### **Confidentiality of Private Information**

Users of the District's electronic resources must comply with all policies and procedures that govern confidentiality of private information, including policies governing school student records and personnel records or information, when using the District's electronic resources.

### **Violations**

The failure of any user to follow the terms of the District's administrative procedure, Acceptable Use of the District's Electronic Networks, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

### **Maintenance of Records**

Certain laws require the District to maintain business records, including public records, school student records, and personnel records, for certain periods of time. Users of the District's electronic resources are responsible for maintaining records as required by District policy, District procedures, and/or relevant laws. This may include maintaining school student records and local records as required by state and federal law.

### **Disclaimer, Limitation of Liability, and Indemnification**

The District does not guarantee the quality of the services provided through its electronic resources. The District makes no guarantees about the accuracy of information accessed through its electronic resources. The District is not responsible for: (i) any loss or damages resulting from the unavailability or failure of its electronic resources; (ii) any information that is rendered unavailable because of its electronic resources or lack thereof; or (iii) any inaccurate information accessed through its electronic resources.

All users assume full responsibility for any costs, liabilities, or damages arising from their use of the District's electronic resources, and must reimburse the District for any loss, including reasonable attorney's fees, incurred as a result of their use to the extent allowed by law. The District is not liable for the actions of users of its electronic resources.

### **No Expectation of Privacy**

Users of the District's electronic resources have no expectation of privacy with respect to use of the District's electronic resources, including access of the District's Internet or Wi-Fi using personal technology, or with respect to any material created, transmitted, accessed, or stored via District electronic resources. This includes material created, transmitted, accessed, or stored for personal use, including incidental personal use, on or through the District's electronic resources. The District reserves the right to monitor users' activities on District electronic resources at any time for any reason without prior notification; to access, review, copy, store, and/or delete any electronic information accessed or stored therein; and to disclose such information to others as it deems necessary and/or as required by law. Users should be aware that information may remain on the District's electronic resources even after it has been deleted by the user. This section of this policy may only be altered through amendment of this policy, and may not be altered or diminished by the verbal or written assurances of any employee or representative of the District

LEGAL REF.:           20 U.S.C. §7131, Elementary and Secondary Education Act.  
                          47 U.S.C. §254(h) and (l), Children's Internet Protection Act.  
                          47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.  
                          115 ILCS 5/14(c-5), Ill. Educational Labor Relations Act.  
                          720 ILCS 5/26.5.

CROSS REF.:           5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials),; Responsible Use and Conduct), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools), 7:345 (Use of Educational Technologies; Student Data Privacy and Security) 9:10 (Student Use of Personal Technology)

ADMIN. PROC.:       9:00, E1 (Acceptable Use of the District's Electronic Resources Authorization Form (Student),  
                          9:00, E2 (Acceptable Use of the District's Electronic Resources Authorization Form

(Staff), 9:00, E1 (Acceptable Use of the District's Electronic Resources Authorization Form (Board)

Reviewed: December 8, 2014, February 10, 2020, August 16, 2021  
Adopted: January 12, 2015  
Revisions Adopted: February 24, 2020, September 20, 2021