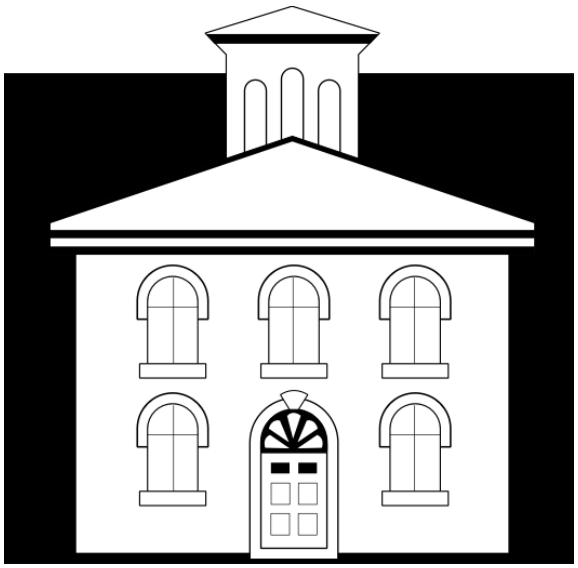
River Forest Public Schools District 90

Instructional Technology/Student Data Privacy Resource Guide

2026-2027



Dear District 90 Parents and Guardians,

We are pleased to provide you with a copy of our District 90 Instructional Technology/Student Data Privacy Resource Guide.

The informational materials included within are intended to serve as a practical resource for students and families who desire to learn more about the important elements of student and family privacy rights, and the procedures that are employed to protect them in River Forest District 90 ("District 90" or "D90"). Please note that this information is also included on the District 90 website. Among other subjects, the topics referenced include:

- Overview about student data/family privacy rights and pertinent laws
- Overview about relevant District 90 policies
- Explanation about D90 app/software privacy standards
- Explanation about D90 app/software approval process
- General description about categories of apps/software in use for instructional purposes
- Link to electronic inventory of apps/software in use (by grade level)
- Current D90 Acceptable Use Policy
- Current D90 Parental Consent Agreement

While student and family privacy has always been a priority, this issue continues to become more pronounced in the age of technology. Recent developments in the area of technology resources for classroom teaching are helping to improve the quality of instruction in ways never before seen. At the same time, the use of advanced learning software has implications for student privacy, reflecting the myriad ways in which "big data" concerns are present in every aspect of our lives. From an education perspective, the goal is to find balance between these forces whenever possible. We strive to provide our students with innovative and appropriate learning experiences while still meeting our obligations to student privacy and data security.

You likely recall having provided District 90 with parental consent during the registration process for your child to access our electronic networks for educational purposes, utilize District technology devices, and use District-approved computer apps and software. Please be assured that you have the ability to change or revoke your consent for these privileges at any time as may be necessary. Please contact your child's principal if you have questions or would like more information about matters pertaining to parental consent.

I hope that you find this resource guide informative, and that it helps to answer any questions you may have about District 90's procedures, expectations, and safeguards that have been established to comply with privacy requirements and protect student data to the greatest possible degree.

Best regards,

Ed 1. Co

Ed Condon, PhD
Superintendent

I. Overview of Pertinent Laws Governing Student Data Privacy

District 90 will comply with all applicable laws and regulations concerning the privacy of student data. District 90 will also take steps to ensure that any third parties who provide services to the District comply with these laws. The following is an overview of the various laws that govern the confidentiality of student information, including but not limited to electronic data, though this list is not exhaustive.

A. Federal Law

The *Children's Internet Protection Act* (CIPA) was enacted to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools that receive discounts for Internet access or through the e-rate program, which makes certain communications services and products more affordable for eligible schools. To be eligible to receive discounts, a school must have an Internet safety policy that includes protection measures to block or filter Internet access to pictures that are obscene, child pornography, or harmful to minors. A school is also required to include in its Internet safety policy that the school will monitor the online activities of children and educate children about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response. More information is available at *www.fcc.gov/consumers/guides/childrens-internet-protection-act*. (47 U.S.C. §254(h), (i); 47 C.F.R. §54.520.)

The *Children's Online Privacy and Protection Act* (COPPA) also deals with children's online privacy. The primary goal of COPPA is to place parents in control over what information is collected from children under age 13. COPPA applies to commercial websites and online services. The term "online service" broadly covers any service available over the Internet (including mobile apps), or that connects to the Internet or a wide-area network. COPPA imposes requirements on: operators of websites and online services directed to children under 13 that collect, use, or disclose personal information from children; operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13; and operators of websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. More information is available at *www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy.* (15 U.S.C. §§6501-6505; 16 C.F.R. Part 312.)

The *Every Student Succeeds Act* (ESSA) provides, in part, that school districts may use federal funds to support efforts to effectively integrate technology into curricula and instruction in numerous ways and to teach staff about the appropriate use of student data. The ESSA supports "digital learning," which means any instructional practice that effectively uses technology to strengthen a student's learning experience and encompasses a wide spectrum of computer and Internet-based tools and practices.

More information is available at *www.ed.gov/ESSA*. (P.L. 114-95, December 10, 2015, 129 Stat 1802.)

The *Federal Educational Rights and Privacy Act* (FERPA) affords parents/guardians important rights concerning their children's school student records and the personally identifiable information in those records. FERPA gives parents/guardians the rights to: (1) inspect and review the student's records maintained by the school; (2) request that a school amend the student's records; (3) consent in writing to the disclosure of personally identifiable information from the student's records, except under certain permitted situations; and (4) file a complaint with the U.S. Department of Education's Family Policy Compliance Office regarding an alleged violation under FERPA. More information on FERPA is available at *https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html* . (20 U.S.C. § 1232g; 34 C.F.R. Part 99.)

The *Health Insurance Portability and Accountability Act* (HIPAA) was enacted, in part, to protect the privacy and security of individually identifiable health information. The U.S. Department of Health and Human Services has issued various rules, including a Privacy Rule, to implement HIPAA. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health care plans and providers that conduct certain health care transactions electronically. However, the HIPAA Privacy Rule specifically excludes from its coverage records that are protected by FERPA. Therefore, in general the HIPAA Privacy Rule does not apply to public elementary or secondary schools. More information is available at *http://www.hhs.gov/hipaa* and *https://studentprivacy.ed.gov/?src=fpco.* (Pub. L. 104-191; 45 CFR Parts 160, 164.)

The *Protection of Pupil Rights Amendment* (PPRA) applies to a school district's administration of surveys, analyses, or evaluations to students that concern one or more of the following areas: political affiliations or beliefs of the student or the student's parent; mental or psychological problems of the student or the student's family; sex behavior or attitudes; illegal, anti-social, self-incriminating, or demeaning behavior; critical appraisals of other individuals with whom the students have close family relationships; legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; religious practices, affiliations, or beliefs of the student or student's parent; or income (other than as required by law to determine eligibility for participation in a program or for receiving financial assistance under such program). School districts are required to provide notices to parents/guardians about their rights under the PPRA and any time that a school engages in activities in which certain information is collected from students. More information is available at *https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra.* (20 U.S.C. § 1232h; 34 C.F.R. Part 98.)

B. State Law

The *Children's Privacy Protection and Parental Empowerment Act* prohibits the sale or purchase of personal information of a child under age 16 without parent/guardian consent, unless a certain exception applies. (325 ILCS 17/1 *et seq*.)

The *Illinois School Student Records Act* (ISSRA) is similar to FERPA and also affords parents/guardians rights concerning their children's school student records and the individually identifiable information in those records. Like FERPA, the two primary purposes of the ISSRA are to ensure parent/guardian access to their child's records and to ensure the confidentiality of student records and the information in those records. (105 ILCS 10/1 *et seq*.; 23 Ill Admin. Code Part 375.)

The *Illinois Mental Health and Developmental Disabilities Confidentiality Act* (MHDDCA) governs the confidentiality of communications and records concerning mental health or developmental disability services provided to a student by school personnel who meet the definition of a "therapist" under the MHDDCA, such as a school psychologist, social worker, or nurse. The MHDDCA affords parents/guardians (and students age 12 or older) with rights to access records and provide written consent prior to disclosure of records or communications, except under specific circumstances. (740 ILCS 110/1 *et seq*.)

The *Local Records Act* provides requirements for how local governments, such as school districts, maintain day-to-day recordkeeping and destroy records prepared or received in the course of public business. (50 ILCS 205/1 *et seq*.; 44 Ill. Admin. Code Part 4500.)

The *Right to Privacy in the School Setting Act* provides that schools must give notice to students and parents/guardians about privacy of students' passwords for their social networking profiles/websites, unless there is specific information about activity on the student's account that violates a school disciplinary rule or policy. (105 ILCS 75/1 *et seq*.)

The *Personal Information Protection Act* governs the protection of personal information data, which is defined as individuals' names in combination with their social security numbers, driver's license numbers, State identification card numbers, or financial account information. When there is a breach in the security of such data, notice must be provided to the affected individuals that includes information required by the *Act*. (815 ILCS 530/1 *et seq*.)

The *Student Online Personal Protection Act* (SOPPA) is similar to COPPA and protects the privacy and security of student data when collected by educational technology companies operating online websites, online services, or online/mobile applications. The SOPPA allows data to be used to benefit students, including as a way to provide personalized learning and educational technology. The SOPPA bars the use of student data for targeted advertising and prohibits the sale of student information gathered during the students' use of the educational technology. (105 ILCS 85/1 *et seq*.)

II. District 90 Board Policies

A number of District 90 Board policies may apply to the collection, use, and disclosure of student data. Please note that this Section summarizes the Board policies for a point of reference and does not provide the entire content of these policies.

Policy 6:40, Curriculum Development: This Policy states that the Superintendent will recommend curriculum and develop a review program to monitor the current curriculum and suggest changes to make the curriculum more effective, incorporate improved teaching methods and materials, and be responsive to social change, technological developments, student needs, and community expectations.

Policy 6:210, Instructional Materials: This Policy provides that all District classrooms and learning centers will have access to teaching tools, textbooks, workbooks, audio-visual materials, and equipment selected to meet the students' needs. The Superintendent will approve the selection of all textbooks and instructional materials.

Policy 6:212, Instructional Materials Selection and Adoption: This Policy provides that textbooks and instructional materials, both print and non-print, will be selected based upon their quality and educational value. The Superintendent will approve the selection of all textbooks and instructional materials.

Policy 6:235, Computer Network and Internet Safety, Access and Use: This Policy governs all use of District's "computer network", meaning all District computers, the District's local and/or wide area network, and access to the Internet through District computers or the District's local and/or wide area network. The Policy states that the District must have safety measures in place to ensure that students do not have access to inappropriate content through use of the District's computer network, including through the Internet.

Policy 6:236, District Web Publications – Students and Staff: This Policy provides that the District's website is a closed forum for expression and District 90 has sole authority concerning what materials may be published on the website. The Policy states the types of subject matter that is prohibited from being on the District's website and provides safeguards to maintain privacy of student information.

Policy 6:260 Complaints About Curriculum, Instructional Materials, and Programs: This Policy provides that parents/guardians have the right to inspect any instructional material used as part of their child's educational curriculum. The Policy provides parents/guardians, employees, and community members with the process to submit complaints and/or suggestions related to curriculum, instructional materials, or programs. The Policy also provides parents/guardians with the process to request that their child be exempt from using a particular instructional material or program.

Policy 7:15, Student and Family Privacy Rights: This Policy provides requirements when surveys or evaluations are administered to students and the confidentiality of information disclosed by students in those surveys or evaluations. The Policy states that parents/guardians may opt out their children from participating in certain surveys. Also, the Policy prohibits employees and school officials from marketing or selling students' personal information students or otherwise providing that information to others for that purpose, unless the parents/guardians have consented or the information is exclusively for educational purposes.

Policy 7:17, Directory Information: This Policy identifies specific information concerning students that may be disclosed to the general public and outside organizations without parent/guardian written consent, unless a parent/guardian requests that such information not be released without first seeking consent.

Policy 7:140, Search and Seizure: This Policy notifies parents/guardians and students that District 90 may not request or require a student or his or her parent/guardian to provide a password or other related account information to gain access to the student's account or profile on a social networking website. However, District 90 may conduct an investigation or require a student to cooperate in an investigation if there is specific information about activity on the student's social networking account or profile that violates a school disciplinary rule or policy. During an investigation, the student may be required to share the content from his or her account or profile for District 90 to determine whether the student violated a school rule or policy.

Policy 7:310, Restrictions on Publications; Elementary Schools: This Policy provides that school-sponsored publications, productions, and websites are part of the curriculum and are not a public forum for general student use, which means that District 90 may edit or delete such material. A publication includes any off-line or online written or electronic print material, audio-visual material on any medium, or information or material on electronic devices. The Policy also provides requirements and restrictions for the distribution of non-school-sponsored publications at school or school-related activities. The Policy states that students may be disciplined for distributing non-school-sponsored publications on or off school grounds if the publication causes a substantial disruption or a foreseeable risk of a substantial disruption to school operations, or interferes with the rights of other students or staff members.

Policy 7:340, Student Records: This Policy provides the requirements for access to and confidentiality of students' school student records and the information contained in those records. Unless an exception applies, student records/information may not be released without parent/guardian prior written consent.

One exception to parent consent is that District 90 may release student records/information to District employees or school officials who have a current, demonstrable educational or administrative interest in the student, in furtherance of such interest. A "current, demonstrable educational or administrative interest" means that the person requires access to the student record information to perform his or her required services

or functions for the District. A "school official" is defined, in part, as a contractor, consultant, or other party to whom the District has outsourced institutional services or functions, provided that the outside party: (1) performs an institutional service or function for which the District would otherwise use employees; (2) is under the direct control of the District with respect to the use and maintenance of student record information; and (3) is subject to the confidentiality requirements for the use and redisclosure of individually identifiable information from student records.

This means that "school officials" may be third-party Internet or cloud-based educational service providers used by the District, including but not limited to, the products, software, subscriptions, tools, and mobile applications provided by the service providers/vendors. Some examples of Internet or cloud-based educational services are:

- Cloud storage (e.g., Apple School Manager, Google Docs,),
- Document sharing and editing applications (e.g., Google Docs),
- Differentiated instruction (e.g., Explain Everything),
- E-mail services (e.g., Gmail),
- Game-based learning applications (e.g., BrainPop, Kahoo.it),
- Learning platforms/management systems (e.g., Schoology, SeeSaw),
- Library management systems, subscriptions/e-book websites (e.g., Alexandria),
- Notification systems (e.g., BrightArrow), and
- Productivity tools (e.g., Google Apps for Education)

Policy 7:345 Use of Educational Technologies; Student Data Privacy and Security: This Policy provides that all educational technologies used in the District shall further the objectives of the District's educational program, align with the curriculum criteria established by Board Policy, and/or support efficient District operations. It requires the Superintendent ensure that the use of educational technologies in the District
meets established criteria. This Policy prohibits the sale, rental, lease, or trading of any school records or covered information in compliance with SOPPA. The Policy also requires the Superintendent to ensure that the District implements and maintains reasonable security procedures and practices to protect covered information from unauthorized access, destruction, use, modification or disclosure.

III. District 90 Privacy Standards

The District's privacy standards are established in accordance with applicable federal and State law and Board policy, and are intended to reflect the District's mission and values. These guiding concepts are intended to provide direction about many elements of the District's practice, including the educational value of instructional technology, the primacy of children's safety, and the importance of family rights.

The District utilizes filters (*e.g.*, 'securely' content filter) and other safety measures (*e.g.*, firewalls, etc.) to prevent students from accessing harmful information on the Internet as well as to protect the privacy of student information.

The District also uses a tool provided by a third party, Education Framework, to determine whether websites, software, or apps are safe to use as part of instructional programming. Education Framework offers a student data privacy manager, EdPrivacy, which applies a scoring system to rate the privacy measures in place for a particular website, software or app. Based on the rating issued by EdPrivacy and other available information, the District decides if that particular website, software or app has adequate privacy measures to protect student data. If the privacy measures are found adequate, the District will approve the website, software or app for use by staff, students and/or parents. In some circumstances, the website, software or app will be only be approved for use in a limited manner, or only approved for use by staff members.

IV. District 90 Approval Procedure

As described in Section III (**District 90 Privacy Standards**), EdPrivacy uses a privacy quality scoring system based on 5 main components:

1. **Data privacy –** what information is collected from students and what are the purposes for collecting that student data;

2. **Data deletion** - the ability of parents/guardians to review and/or delete personal information collected from their children;

3. **Data security** - whether data transferred over the Internet is encrypted and whether there are security policies and procedures that are reasonably designed to protect personal student information against risks, such as unauthorized access or unintended or inappropriate destruction, modification, or disclosure;

4. **Data integrity** - whether student data is backed up on a regular schedule; and

5. **Data retention** - whether there is a data retention policy stating that data will only be retained for as long as it serves an educational purpose.

The District ultimately decides whether or not to use the particular website, software or app based on the privacy quality score by provided by EdPrivacy and/or The Student Data Privacy Consortuim (SDPC) and any other relevant information. Other relevant information may include consideration about the group of individuals who will be using the website, software or app, the manner in which the website, software or app will be deployed, and the intended reasons for use.

V. Examples of Platforms, Systems, Software and Application Types Used in District 90

While the following list is not exhaustive, it provides an overview of the significant technology-based resources that are currently in use within District 90 schools. This list is intended to illustrate the variety of resources that are utilized and provide some of the general categories of use.

Curricular/Instructional Resources:

- Apple Suites (Pages, Numbers, Keynote, etc)
- BookCreator
- BrainPop
- Canva - Graphic Design & Photo Editing app
- ClassKick
- Google Apps for Education
- Kodable
- Learning Ally
- Notability
- Padlet
- PicCollage Edu
- Quizlet
- SeeSaw
- Sora by Overdrive
- Stop Motion Studio
- Swift Playgrounds
- Zoom

Standardized Assessments/Progress Monitoring Resources:

- AIMSweb

- MAP
- Ages and Stages-SE online parent questionnaire

Technology-Based Intervention/Remediation Resources

- Lexia
- Learning Ally

Communication Systems/Tools Resources:

- AtoZ Directory
- BrightArrow
- PowerSchool
- Survey Monkey

VI. Electronic Inventory of Platforms, Systems, Software and Applications Used in District 90

The links below provide lists of the platforms, systems, software and applications used in each grade level. As technology-based resources used for instructional purposes are frequently updated and changed, this list will be revised on a periodic basis. Please contact your child's building principal if you have questions or concerns about a particular tool.

Resources in use in River Forest District 90

VII. District 90 Incident Response

Should a breach in the privacy of student data occur, the District will take appropriate measures to mitigate the breach and ensure that security measures are reviewed and, if necessary, modified to prevent any future breaches. This includes, but is not limited to, (a) complying with any applicable law, (b) implementing the District's data breach response plan and/or procedures, and (c) implementing and/or enforcing privacy terms and conditions set forth in any technology-based vendor agreements. The District's response to a breach will be handled in a manner consistent with the following Board policies:

- Policy 6:235, *Computer Network and Internet Safety, Access and Use*
- Policy 6:236, *District Web Publications - Students and Staff*
- Policy 7:15, *Student and Family Privacy Rights*
- Policy 7:17, *Directory Information*
- Policy 7:340, *Student Records*
- Policy 7:345, *Use of Educational Technologies; Student Data Privacy and Security*

In addition, the District will take appropriate measures to address any computer conduct by students or school officials that violates federal or State law, Board policy or school rules. The District's response to computer misconduct will take into consideration any student privacy implications and will be handled in a manner consistent with the following Board policies:

- Policy 2:260, *Uniform Grievance Procedure*
- Policy 5:125, *Personal Technology and Social Media; Usage and Conduct*
- Policy 5:130, *Responsibilities Concerning Internal Information*
- Policy 7:20, *Harassment of Students Prohibited*
- Policy 7:22, *Bullying*
- Policy 7:180, *Prevention of and Response to Bullying, Intimidation, and Harassment*
- Policy 7:190, *Student Behavior*
- Policy 7:230, *Misconduct by Students with Disabilities*
- Policy 7:340, *Student Records*

VIII. District 90 Acceptable Use Policy

Policy 6:235, *Computer Network and Internet Safety, Access and Use*

Purpose and Application

This Policy and its implementing Rules and Regulations are intended to serve as a guide to the scope of the District's authority over and the safe and acceptable use of the District's computers, computer network, and Internet access. This Policy governs all use of District computers, hardware, software, communication systems, networks,

electronic equipment, data and other technologies, whether now existing or subsequently developing, including any access to the Internet using such resources which will be collectively referred to in this Policy and its implementing Rules and Regulations as the District's "computer network."

Individuals covered by this Policy include, but are not limited to, students, Board of Education members, employees, school officials, parents, and visiting guests who have access to the District's computer network. Except as otherwise provided in this Policy, the provisions of this Policy shall apply to the use of technology in any District school building, on school grounds, at a school-sponsored activity, and at any location in any manner that would otherwise violate this Policy.

Access to the computer network shall be consistent with and beneficial to the educational mission of the District. Such access shall serve as a natural extension of the educational lessons learned within the classroom by providing access to educational resources and reference materials, by reinforcing the specific subject matter taught, by requiring the use of critical thinking skills, by promoting tolerance for diverse views, and by teaching socially appropriate forms of civil discourse and expression. Therefore, users shall be allowed access to the computer network consistent with the District's curriculum, educational mission and this Policy and its implementing Rules and Regulations.

Rights and Responsibilities

The computer network is part of the educational curriculum and is not a public forum for general use. Access to and use of the computer network is a privilege, not a right, that is extended to staff, students, parents, and other members of the District community. District 90's code of conduct applies to the use of the District's computer network.

The manner in which the computer network is used should not conflict with the basic educational mission of the District. Use of the computer network may be restricted in light of the maturity level of students involved and the special characteristics of the school environment. Therefore, the District shall not permit use of the computer network which: (a) disrupts the proper and orderly operation and discipline of schools in the District; (b) threatens the integrity or efficient operation of the District's computer network; (c) violates the rights of others; (d) is socially inappropriate or inappropriate for a student's age or maturity level; (e) is primarily intended as an immediate

solicitation of funds; (f) is illegal or for illegal purposes of any kind; or (g) constitutes gross disobedience or misconduct.

The Board owns the contents of the District's computer network and reserves the right to inspect the contents of the computer network. Individuals using the computer network have no expectation of privacy in any material stored, transmitted, or received via the computer network, including but not limited to District e-mail accounts. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

The District is not responsible for any information, including its accuracy or quality, obtained or transmitted through use of the Internet (except for the District's website). The District is not responsible for any information that may be lost or damaged, or become unavailable when using the computer network, or for any information that is retrieved or transmitted via the Internet.

Curriculum

The use of the District's computer network and technologies available through the District's computer network shall be consistent with Board Policies 6:60, *Curriculum Content,* and 6:210, *Instructional Materials*.

The Superintendent or designee shall monitor the use of the Internet and materials available through the Internet as part of the curriculum. Staff members may use the Internet and materials available through the Internet as part of the curriculum in accordance with Board policy and any expectations set by the Superintendent or designee.

As required by federal law and Policy 6:60, students will be educated about appropriate Internet behavior, including but not limited to: (a) education about appropriate online behavior, (b) interacting with other individuals on social networking websites and in chat rooms, and (c) cyberbullying awareness and response.

Acceptable Use

All use of the District's computer network must be: (1) in support of education and/or research, and be in furtherance of the District's educational mission, or (2) for a legitimate school business purpose. General rules for behavior and communications apply when using the computer network.

The District's computer network is not intended to be used for non-academic or non-administrative functions, or for personal or recreational use, which include, but are not limited to, illegal, commercial, political, religious or entertainment purposes as more fully described below.

Uses of the computer network that are not acceptable include, but are not limited to, the following:

1. Installing, modifying, uploading or downloading programs, software, or applications that do not comply with Board policy, applicable administrative procedures, and terms of the *Acceptable Use* form.
2. Engaging in acts of vandalism, which is defined as any malicious attempt to harm or destroy data of another user or the District, including the creation or use of computer viruses.
3. Accessing, submitting, posting, publishing, transmitting or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing or illegal material; this includes using the electronic network to engage in cyberbullying as defined by State law.
4. Posting District work product (e.g., test materials, procedures, District publications) on the Internet for public access without prior approval from the Superintendent or designee.
5. Posting, publishing, transmitting, receiving or displaying material for commercial gain.
6. Accessing data maintained by the District in which the individual has not been given proper authorization.
7. Accessing the electronic network when such privilege has been suspended or revoked by the District.
8. Using the electronic network in violation of State or federal law.

E-Mail Use

The District provides e-mail accounts to employees and students as part of the learning environment. The Superintendent or designee shall monitor the use of e-mail. Employees and students may use e-mail only in accordance with Board policy and any expectations set by the Superintendent or designee.

Internet Safety

The District shall implement technology protection measures to protect students from inappropriate content on the Internet. The measures shall include a filtering device(s) that protects against Internet access by users to visual depictions that are obscene, pornographic, or harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce and monitor the use of such filtering device(s). The Superintendent or designee shall establish and implement administrative procedures to address students' use of the Internet, including but not necessarily limited to the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities,
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as names and addresses, and
6. Measures to restrict student access to harmful materials.

DISCLAIMER. In compliance with the federal *Children's Internet Protection Act* (CIPA), the District endeavors to protect users of the District's computer network from websites containing material that is illegal for minors, including, but not limited to, pornography. The District also endeavors to address the safety and security of minors when using e-mail and other forms of direct electronic communications through the computer network. However, the use of employee-provided and student-provided technology to access the Internet cannot be subjected to measures used by the District such as content filters, blocking lists, or monitoring of Internet website traffic for patterns of usage that could indicate inappropriate network usage. Accordingly, employees and students who provide their own technology and/or access to the Internet shall assume any risk associated therewith. The District expressly disclaims any responsibility for imposing content filters, blocking lists or monitoring of employee or student-provided technology and/or devices.

Authorization for Computer Network Access

Each staff member must sign the District's *Authorization for Computer Network Access/Use* form as a condition for using the District's computer network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization for Computer Network Access/Use* form before being granted unsupervised use.

Confidentiality

All users of the District's computer network shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the computer network or transmitted through the Internet. Users must be aware that the *Freedom of Information Act* and other laws may require the disclosure of records, including but not limited to e-mails, maintained on the District's computer network.

Disciplinary Action

The failure of any user to follow this Policy or the terms stated in the *Authorization for Computer Network Access/Use* form will result in the loss of privileges, disciplinary action, and/or appropriate legal action at the discretion of the Superintendent or designee. In the case of employees, a violation may result in suspension without pay or dismissal of employment. In the case of students, a violation may result in out-of-school suspension or expulsion.

Implementation

The Superintendent and Building Principals are authorized to implement this Policy and its Rules and Regulations, and to designate appropriate staff members to assist them in doing so. The Superintendent and Building Principals may also promulgate additional rules, regulations, and other terms and conditions of computer network use as may be necessary to ensure the safe, proper, and efficient operation of the computer network and the individual District schools.

LEGAL REF.:

20 U.S.C. §7131, Elementary and Secondary Education Act.

Family Educational Rights and Privacy Act. 20 U.S.C. §1232g.

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.

105 ILCS 5/27-23.7.

105 ILCS 5/26.5.

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 (General Copyright Restrictions and Copyright Restrictions Involving the Development of Instructional Materials and Computer Programs by Employees), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:212 (Instructional Materials Selection and Adoption), 6:230 (Library Media Program), 6:236 (District Web Publications – Students and Staff), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:15 (Student and Family Privacy Rights), 7:130 (Student Rights and Responsibilities), 7:140 (Search and Seizure), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools), 7:340 (Student Records), 7:345 (Use of Educational Technologies; Student Data Privacy and Security).

ADOPTED: August 20, 2012

REVISED: April 18, 2016; January 16, 2018; August 16, 2021

IX. Parent/Guardian Consent for Technology Access and Use

Authorization for Computer Network Access/Use Form

Students must have a parent/guardian read and agree to the following before being granted unsupervised access.

By signing below, I, the parent/guardian of the student named below, confirm that I have read and understand the following:

1. I have had the opportunity to review Board Policy 6:235, *Computer Network and Internet Safety, Access and Use,* and its administrative procedures.

2. I understand that all use of the District's computer network, including the Internet, shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication.

3. I understand that access to the District's computer network is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the computer network.

4. I understand that my child is responsible for his/her use of the District's computer network at all times. I accept full responsibility for supervision if and when my child uses District technology outside of school. I have discussed Board Policy 6:235, *Computer Network and Internet Safety, Access and Use,* with my child.

5. I understand that my child's failure to follow the terms of Board Policy 6:235, *Computer Network and Internet Safety, Access and Use,* its administrative procedures, and school rules for use of technology will result in the loss of privileges, disciplinary action (which may include suspension or expulsion), and/or appropriate legal action.

6. I understand that District 90 uses third-party Internet or cloud-based educational service providers, including but not limited to platforms, systems, software and applications, for educational purposes. I understand that District 90 has an approval process for third-party educational service providers, and, once approved, the educational service provider is a District "school official" that may access my child's personally identifiable information without my prior written consent or prior notice given to me.

7. I understand that when my child uses technology from third-party Internet or cloud-based educational service providers, information about my child will be collected and stored electronically by the educational service provider. I understand that such stored information may be accessible to someone other than my child, me and District employees or school officials by virtue of this online environment.

8. I understand that District employees and school officials may access and monitor my child's use of technology from third-party Internet or cloud-based educational service providers, including accessing and searching any material stored, transmitted, or received through the technology.

9. I understand that I may revoke my consent for my child to access and use technology from third-party Internet or cloud-based educational service providers at any time.

10. I understand that I may ask for my child's account/information to be removed from technology from third-party Internet or cloud-based educational service providers at any time.

_____ YES, I give permission for my child to access and use the District's computer network, including the Internet and any platforms, systems, software and applications from approved third-party Internet or cloud-based educational service providers.

_____ NO, I do not give permission for my child to access and use the District's computer network, including the Internet and any platforms, systems, software and applications from approved third-party Internet or cloud-based educational service providers.

_____
Parent/Guardian Name (please print)

_____ _____
Parent/Guardian Signature Date

Students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the above Authorization for Computer Network Access/ Use. I understand that the District and/or its agents may access and monitor my use of

the Internet, including my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's computer network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's computer network, including the Internet.

_____

Student Name (please print)

_____ _____

Student Signature Date