LIBERTYVILLE ELEMENTARY SCHOOLS
District No. 70
Libertyville, Illinois

September 21, 2020

BOARD REPORT NO. 8.2

APPROVAL OF SCHOOL BOARD POLICIES

Board Report No. 8.2 seeks formal approval of the following School Board Policies, subsequent to their first reading on August 24, 2020:

4:180 **OPERATIONAL SERVICES**: Pandemic Preparedness

6:235 **INSTRUCTION**: Access to Electronic Networks and Internet Safety

NEW 7:345 **STUDENTS**: Use of Educational Technologies; Student Data Privacy and Security

ROLL CALL VOTE:

POSSIBLE MOTION:

I move that the School Board approve the Board Policies listed in this report, as they appear in Board Report No. 8.2, Exhibits A, B and C, respectively.

Operational Services

Pandemic Preparedness; Management; and Recovery

The School Board recognizes that the District will play an essential role along with the local health department and emergency management agencies in protecting the public's health and safety during a pandemic.

A pandemic is a global outbreak of disease. Pandemics happen when a new virus emerges to infect individuals and, because there is little to no pre-existing immunity against the new virus, it spreads sustainably.

To prepare the School District community for a pandemic, the Superintendent or designee shall: (1) learn and understand how the roles that the federal, State, and local government function; (2) form a pandemic planning team consisting of appropriate District personnel and community members to identify priorities and oversee the development and implementation of a comprehensive pandemic school action plan; and (3) build awareness of the final plan among staff, students, and community.

Emergency School Closing

In the case of a pandemic, the Governor may declare a disaster due to a public health emergency that may affect any decision for an emergency school closing. Decisions for an emergency school closing will be made by the Superintendent in consultation with and, if necessary, at the direction of the Governor, Ill. Dept. of Public Health, District's local health department, emergency management agencies, and/or Regional Office of Education.

During an emergency school closing, the Board President and the Superintendent may, to the extent the emergency situation allows, examine existing Board policies pursuant to Policy 2:240, *Board Policy Development*, and recommend to the Board for consideration any needed amendments or suspensions to address mandates that the District may not be able to accomplish or implement due to a pandemic.

Board Meeting Procedure; No Physical Presence of Quorum and Participation by Audio or Video

A disaster declaration related to a public health emergency may affect the Board's ability to meet in person and generate a quorum of members who are physically present at the location of a meeting. Policy 2:220, *School Board Meeting Procedure*, governs Board meetings by video or audio conference without the physical presence of a quorum.

Payment of Employee Salaries During Emergency School Closures

The Superintendent shall consult with the Board to determine the extent to which continued payment of salaries and benefits will be made to the District's employees, pursuant to Board policies 3:40, *Superintendent*, 3:50, *Administrative Personnel Other Than the Superintendent*, 5:35, *Compliance with the Fair Labor Standards Act*, 5:200, *Terms and Conditions of Employment and Dismissal*, and 5:270, *Employment At-Will, Compensation, and Assignment*, and consistent with: (1) applicable laws, regulations, federal or State or local emergency declarations, executive orders, and agency directives; (2) collective bargaining agreements and any bargaining obligations; and (3) the terms of any grant under which an employee is being paid.

Suspension of In-Person Instruction; Remote and/or Blended Remote Learning Day Plan(s)

When the Governor declares a disaster due to a public health emergency pursuant to 20 ILCS 3305/7, and the State Superintendent of Education declares a requirement for the District to use *Remote Learning Days* or *Blended Remote Learning Days*, the Superintendent shall approve and present to the Board for adoption a Remote and/or Blended Remote Learning Day Plan (Plan) that:

1. Recommends to the Board for consideration any suspensions or amendments to curriculum-related policies to reduce any Board-required graduation or other instructional requirements in excess of minimum curricular requirements specified in School Code that the District may not be able to provide due to the pandemic;
2. Implements the requirements of 105 ILCS 5/10-30; and
3. Ensures a plan for periodic review of and/or amendments to the Plan when needed and/or required by statute, regulation, or State guidance.

LEGAL REF.: 105 ILCS 5/10-16.7, 5/10-20.5, 5/10-20.56, and 5/10-30.
5 ILCS 120/2.01 and 120/7(e), Open Meetings Act.
20 ILCS 2305/2(b), Ill. Dept. of Public Health Act (Part 1).
20 ILCS 3305/, Ill. Emergency Management Agency Act.
115 ILCS 5/, Ill. Educational Labor Relations Act.

CROSS REF.: 1:20 (District Organization, Operations, and Cooperative Agreements), 2:20 (Powers and Duties of the School Board; Indemnification), 2:220 (School Board Meeting Procedure), 2:240 (Board Policy Development), 3:40 (Superintendent), 3:50 (Administrative Personnel Other Than the Superintendent), 3:70 (Succession of Authority), 4:170 (Safety), 5:35 (Compliance with the Fair Labor Standards Act), 5:200 (Terms and Conditions of Employment and Dismissal),5:270 (Employment At-Will, Compensation, and Assignment), 6:20 (School Year Calendar and Day), 6:60 (Curriculum Content), 6:300 (Graduation Requirements), 7:90 (Release During School Hours), 8:100 (Relations with Other Organizations and Agencies)

ADOPTED: April 27, 2020

REVISED: September 21, 2020

Instruction

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyberbullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,

4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the *Authorization for Access to the District's Electronic Networks* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use.

All users of the District's computers to access the Internet 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 network.

The failure of any student or staff member 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.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
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), 6:220 (Bring Your Own Technology (BYOT) Program; 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)

ADMIN. PROC.: 6:235-AP1 (Administrative Procedure - Acceptable Use of the District's Electronic Networks), 6:235-AP1, E1 (Student Authorization for Access to the District's Electronic Networks), 6:235-AP1, E2 (Exhibit - Staff Authorization for Access to the District's Electronic Networks)

ADOPTED: October 26, 1998

REVISED: December 17, 2007; December 19, 2011; September 21, 2020

Students

Use of Educational Technologies; Student Data Privacy and Security

Educational technologies used in the District shall further the objectives of the District's educational program, as set forth in Board policy 6:10, *Educational Philosophy and Objectives*, align with the curriculum criteria in policy 6:40, *Curriculum Development*, and/or support efficient District operations. The Superintendent shall ensure that the use of educational technologies in the District meets the above criteria.

The District and/or vendors under its control may need to collect and maintain data that personally identifies students in order to use certain educational technologies for the benefit of student learning or District operations.

Federal and State law govern the protection of student data, including school student records and/or *covered information*. The sale, rental, lease, or trading of any school student records or covered information by the District is prohibited. Protecting such information is important for legal compliance, District operations, and maintaining the trust of District stakeholders, including parents, students and staff.

Definitions

Covered information means personally identifiable information (PII) or information linked to PII in any media or format that is not publicly available and is any of the following: (1) created by or provided to an operator by a student or the student's parent/guardian in the course of the student's or parent/guardian's use of the operator's site, service or application; (2) created by or provided to an operator by an employee or agent of the District; or (3) gathered by an operator through the operation of its site, service, or application.

Operators are entities (such as educational technology vendors) that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes.

Breach means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of covered information maintained by an operator or the District.

Operator Contracts

The Superintendent or designee designates which District employees are authorized to enter into written agreements with operators for those contracts that do not require separate Board approval. Contracts between the Board and operators shall be entered into in accordance with State law and Board policy 4:60, *Purchases and Contracts,* and shall include any specific provisions required by State law.

Security Standards

The Superintendent or designee shall ensure the District implements and maintains reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. In the event the District receives notice from an operator of a breach or has determined a breach has occurred, the Superintendent or designee shall also ensure that the District provides any breach notifications required by State law.

LEGAL REF.: 20 U.S.C. §1232g, Family and Educational Rights and Privacy Act, implemented by 34 C.F.R. Part 99.
105 ILCS 10/, Ill. School Student Records Act.
105 ILCS 85/, Student Online Personal Protection Act.

CROSS REF.: 4:15 (Identity Protection), 4:60 (Purchases and Contracts), 6:235 (Access to Electronic Networks), 7:340 (Student Records)

ADOPTED: September 21, 2020

REVISED: