Created	Adopted	Amended
September 24, 2020	September 24, 2020	

ELECTRONIC STUDENT DATA AND RECORDS

The Board recognizes that every device and application with a connection to the Internet potentially collects student data including district email systems, use of virtual learning communities in the classroom and video-recording apps used in class via digital tablets. In order to protect the privacy of district students and staff in compliance with law the following guidelines will be used for overseeing the maintenance and management of electronic district records.

The Family Educational Rights and Privacy Act (FERPA) prohibits school districts from disclosing, except in limited instances, personally identifiable information (PII) contained in student education records without the consent of the parent or eligible student. Educational records may include a range of written and electronic files. The Board presumes that all data created by students, teachers, and staff related to students is an education record governed by FERPA and therefore directs the superintendent to take precautions to retain control over such data.

Under FERPA, elementary and secondary education records include records, files, documents, and other materials that contain information directly related to a student; and are maintained by the district or by a person acting for the district (see: 20 U.S.C. § 1232g(a)(4)(A)). Generally, FERPA requires that schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (see: 34 CFR § 99.31):

A. School officials with legitimate educational interest;
B. Other schools to which a student is transferring;
C. Specified officials for audit or evaluation purposes;
D. Appropriate parties in connection with financial aid to a student;
E. Organizations conducting certain studies for or on behalf of the school;
F. Accrediting organizations;
G. To comply with a judicial order or lawfully issued subpoena;
H. Appropriate officials in cases of health and safety emergencies; and
I. State and local authorities, within a juvenile justice system, pursuant to specific State law.

ELECTRONIC STUDENT DATA AND RECORDS (continued)

Many new technologies are likely to result in the storage or transmission of information that is considered an education record under FERPA. Although storing student information in the Cloud is permitted under FERPA schools are required to manage education records and student PII securely.

Contracting Practices

The district shall only retain the services of third-party technology providers who contractually agree to store and use data in compliance with FERPA and other laws as applicable for the privacy and confidentiality of information. The superintendent in consultation with the school attorney shall ensure the development contract language for Board approval that is consistent with the district FERPA requirements. The superintendent or his or her designee shall work with third-party technology providers on how data should be handled, used and with whom it can be shared.

Authorized Access to the District Network

A. Internet Filters
   To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter the Internet or other forms of electronic communications, and to restrict access to inappropriate information (see Board policy 6142.10 Internet Safety and Technology).
B. Access Security
   The superintendent in consultation with the Network Systems & IT Support Coordinator shall ensure that staff members and other authorized users of the district network are assigned appropriate access permission consistent with legitimate job responsibilities and that restrict unauthorized access to confidential information.

Authorized Access

According to the best practices suggested by the US Department of Education, the superintendent shall only authorize staff to use services in which the terms of service allow the school/district to retain enough control, and provide sufficient parental notice, to invoke the “school official” exception under FERPA.

The “school official” exception may include a contractor, consultant, volunteer, or other party to whom the district has outsourced institutional services or functions that the school or district would otherwise have used its own employees to perform. The district may use the “school official” exception for disclosure of education records to online service providers only when reasonable methods are set up to ensure that the service provider/school official accesses only student records in which:

A. It has a legitimate educational interest;
B. The service provider is under the direct control of the district with regard to the use and maintenance of the records; and
C. The provider uses FERPA-protected information only for the purposes for which the disclosure was made (34 C.F.R. § 99.33,a) and refrains from disclosure to other parties without authorization.

Use of Social Media and Interactive Technology in the Classroom

The superintendent or his or her designee shall review and approve instructional materials and resources including the use of social media and other interactive internet learning opportunities in accordance with Board policy 6161.1 Guidelines for the Evaluation and Selection of Instructional Materials.

ELECTRONIC STUDENT DATA AND RECORDS (continued)
Use of Social Media and Interactive Technology in the Classroom (continued)

Teaching staff members shall be required to have the approval of the superintendent before introducing online interactive learning opportunities in the classroom. The superintendent in consultation with the Network Systems & IT Support Coordinator shall review and approve for classroom use only virtual learning opportunities, online learning communities, social media sites and other interactive online activities that are consistent with district FERPA requirements, support the core content areas of the class or grade, and are consistent with other Board policies regarding student internet safety.

Data and Privacy

The superintendent in consultation with the Network Systems & IT Support Coordinator and members of the technology team shall ensure that the data systems, security measures, and support systems that protect the district network are in place, maintained and updated so that a range of accurate, reliable data sets and associated reports are available, on demand, to authorized users only. The superintendent or his or her designee may oversee the data and privacy of the district network by:

A. Evaluating proposed and existing use of Internet-based educational services that may use student information;
B. Recommending policies and best practices, and acting as a liaison between the school district and the community on privacy issues;
C. Reviewing for Board to approval, specific apps and services;
D. Reviewing and evaluating policies, procedures, and practices that address the privacy and security of data, and the use of data, technologies, and the Internet that meet or exceed legal requirements and federal guidelines;
E. Performing regular network systems penetration checks that verify that the district's digital data systems provide for secure data collection, analysis, reporting, storage, exchanges, and archiving for authorized users;
F. Using evidence-based reasoning and data-driven decision making in the purchase and application of network security systems including hiring qualified staff or consulting companies to set up and oversee district security measures;
G. Educating all staff and students in the procedures and skills for accessing and using the district network and online educational resources according to the school policies and procedures for safety and acceptable use;
H. Training staff on data analysis to inform instruction, curriculum, assessment, and professional practices;
I. Implementing educational programs for students and staff that teach Internet safety and ethical and responsible digital citizenship; and
J. Consistently, clearly, and regularly communicating with students, parents, and the community about privacy rights and district policies and practices with respect to student data privacy, including annual notification to parents regarding the types of information transferred to service providers.

Resources used in policy development:

US Department of Education, "*Family Educational Rights and Privacy Act (FERPA).*"
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
National School Boards Association, *"Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Era,"* (April 2014).

ELECTRONIC STUDENT DATA AND RECORDS (continued)

Legal References:

N.J.S.A. 2A:4A-60 et al.	Disclosure of juvenile information; penalties for disclosure
N.J.S.A. 18A:3619	Pupil records; creation, maintenance and retention, security and access; regulations; nonliability
N.J.S.A. 18A:3619a	Newly enrolled students; records and identification
N.J.S.A. 18A:36-19.1	Military recruiters; access to schools and student information directories
N.J.S.A. 18A:3635	Disclosure of certain student information on Internet prohibited without parental consent
N.J.S.A. 18A:404	Examination for physical defects and screening of hearing of students; health records
N.J.S.A. 18A:4019	Records and reports of tuberculosis testing; disposition; inspection
N.J.S.A. 26:5C-7 through -14	Acquired Immune Deficiency Syndrome
N.J.S.A. 47:1A-1 et seq.	Examination and copies of public records (Open Public Records Act)
N.J.S.A. 47:315 et seq.	Destruction of Public Records Law
N.J.S.A. 52:17B-9.8a through -9.8c	Marking of missing child's school record
N.J.A.C. 6A:8-4.2	Documentation of student achievement
N.J.A.C. 6A:14-1.1 et seq.	Special Education

See particularly:
N.J.A.C. 6A:14-1.3, -2.3, -2.9, -7.9

N.J.A.C. 6A:16-1.1 et seq.	Programs to Support Student Development

See particularly:
N.J.A.C. 6A:16-1.4, -2.2,-2.4, -3.2, -5.4, -6.5, -10.2

N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts
N.J.A.C. 6A:32-2.1	Definitions
N.J.A.C. 6A:327.1 et seq.	Student records
N.J.A.C. 6A:32-8.1	School register
N.J.A.C. 6A:3214.1	Review of mandated programs and services
N.J.A.C. 8:612.1	Attendance at school by students or adults infected by Human Immunodeficiency Virus (HIV)
N.J.A.C. 15:32	Records retention

20 U.S.C.A. 1232g - Family Educational Rights and Privacy Act
42 U.S.C.A. 4541 et seq. - Comprehensive Alcohol Abuse and Alcoholism Prevention Treatment and Rehabilitation Act of 1980
42 CFR Part II
Owasso Independent School District No. -001 v. Falvo, 534 U.S. (2002)
Plainfield Board of Education v. Cooperman, 105 NJ 587 (1987)
No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

ELECTRONIC STUDENT DATA AND RECORDS (continued)

Cross References:

1110	Media
1120	Board of education meetings
3570	District records and reports
5113	Absences and excuses
5124	Reporting to parents/guardians
5125	Student records
5131	Conduct/discipline
5131.6	Drugs, alcohol, tobacco (substance abuse)
5141.2	Illness
5141.3	Health examinations and immunizations
5142	Student safety
6145.1/6145.2	Intramural competition; interscholastic competition
6147.1	Evaluation of individual student performance
6164.2	Guidance services
6171.4	Special education
9322	Public and executive sessions