



Kenton County School District | *It's about ALL kids.*

Issue Paper

DATE:

07/23/2026

AGENDA ITEM (ACTION ITEM):

Receive the Annual Data Security and Breach Notification Best Practice Guidelines for use with the District Technology and Confidential Information.

APPLICABLE BOARD POLICY:

01.61 Records Management

HISTORY/BACKGROUND:

As part of the annual data security and breach notification best practice guidelines, District Staff have reviewed and selected two (2) online video courses that best meet the intentions of this training requirement. Both videos are assigned to NEW District Staff to review through the SafeSchools Training System (Vector Solutions).

FISCAL/BUDGETARY IMPACT:

None

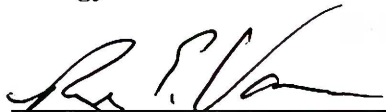
RECOMMENDATION:

Receive the Annual Data Security and Breach Notification Best Practice Guidelines for use with District Technology and Confidential Information.

CONTACT PERSON:

Matthew Winkler, Director of Technology

Principal/Administrator



District Administrator



Superintendent

Use this form to submit your request to the Superintendent for items to be added to the Board Meeting Agenda.

Principal –complete, print, sign and send to your Director. Director –if approved, sign and put in the Superintendent's mailbox.

Kenton County School District
Data Security and Breach Notification Guidebook
As of October 7, 2016

Board Policy – Records Management	1.61
--	-------------

The Kenton County School District Administration shall acknowledge to the Board of Education in a public meeting prior to August 31st of each year that the District has reviewed the Data Security and Breach Notification Best Practice Guide and implemented best practices that meet the needs for reasonable security protection over personal information.

Personal Information is defined as an individual's first and last name or first initial and last name; personal mark; or unique biometric or genetic print or image, along with any of the following data elements:

- Account number, credit or debit card number, that, in combination with any required security code, access code, or password would permit access to an account;
- Social Security number;
- Taxpayer identification number that incorporates a Social Security number;
- Driver's license number, state identification card number, or other individual identification number issued by any agency;
- Passport number or other identification number issued by the United States government; or
- [Individually identifiable health information as defined in 45 C.F.R. sec. 160.103 \(Appendix A\)](#) except for education records covered by the Family Educational Rights and Privacy Act, as amended, [20 U.S.C. sec. 1232g. \(Appendix B\)](#)

Security Breach is defined as an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one or more individuals; or the release of encrypted records along with the key or process necessary to unencrypt the records.

KRS 61.931 – House Bill 5

Procedures and practices to safeguard against security breaches must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.

For any contracts involving personal information that are entered into or amended after January 1, 2015, specific language requiring protection of the data must be included. The following Memorandum of Understanding was developed by the Kenton County School District legal counsel and shall be utilized with all software purchases:

[Memorandum of Understanding – See Appendix C](#)

The following guidelines were prepared around three major areas of consideration as identified by the Kentucky Department of Education:

- **Protection and Prevention**
 - **Preparation for Notification**
 - **Notification**
-

Protection and Prevention

All District employees are charged with protecting the confidentiality of personal information whether it pertains to customers, employees, parents, or students. The basic premise is to remain vigilant in the safekeeping of all paper records and all electronic records. Employees are encouraged to collect the minimum amount of personal information necessary to accomplish the given task and retain the information for the minimum time required by law.

The following Kenton County School District departments are identified and charged with the use, maintenance, and safeguard of records which contain personal and confidential information:

- Personnel
- Student Support Services
- Finance
- Technology
- Special Education
- Preschool
- Food Service
- Transportation
- Support Operations
- School Level Office Staff
- Nursing Services

There are many departments and employees that come into contact with and use information that can be considered personal and confidential. As such, all district employees will be provided a brief overview and basic training in order to strengthen our coverage and safeguard the protection of restricted personal records from unauthorized personnel.

Each department shall inventory all records which contain very personal and restricted information which must be considered for appropriate protection. These records shall be reviewed periodically (annually at a minimum) in order to determine the rights and privileges of district staff that have primary responsibility to utilize the restricted personal information. More importantly, the district staff charged with maintaining the records shall adhere to strict guidelines which are designed to protect the restricted information reflected in the documents.

The following guidelines are to be utilized by all district staff responsible for the safeguarding of personal and restricted information:

- Maintain an inventory of all electronic and paper records that contain personal information
- Classify information contained in all restricted records according to sensitivity and level of risk if that information was accidentally or intentionally accessed by anyone without a need to know
- Strictly adhere to the records retention requirements for all sensitive records
- Supervisors shall annually assess the access rights afforded to district staff as it pertains to restricted files and data bases
- Whenever practical, all high-risk information shall use data encryption to protect the sensitive files in combination with host protection and access control
- Remove rights and access privileges immediately upon severance of employment for employees that have the responsibility to use and maintain sensitive files; retrieve all keys and building access control devices; remove all staff from security alarm code systems
- All employees shall have awareness training regarding the importance of protecting and safeguarding restricted personal information contained in paper files and electronic data bases; the training shall also include a comprehensive review of Data Security and Breach Notification Best Practice Guide.
- All employees shall review the following awareness training videos located on the Safe Schools Training Site:
 - Cybersecurity Overview
 - Protection Against Malware
 - FERPA: Confidentiality of Records
- Use strong passwords or pass phrases and change them frequently
- Keep a password, PIN, or pass code on all devices including laptops, tablets, and smart phones
- Require all contract vendors that utilize personal information on behalf of the school district to sign and adhere to the guidelines established in the District Memorandum of Understanding; all MOU's must be maintained and renewed annually
- Each district staff member that is charged with the maintenance or access to personal restricted information shall adhere to appropriate office maintenance requirements designed to protect access to confidential records throughout the course of the work day and after work hours
 - Only print files or records that contain restricted personal information if necessary
 - Never leave restricted files on common space printers or copiers

- **Never leave restricted files on desk top computer screens or printed files laying on the desk surfaces when you are away from the work space**
- **File all confidential information in securely fastened spaces when not in use**
- **Properly manage and control all confidential conversations**
- **Pay attention to confidential information being displayed on monitors in an open setting**
- **Establish language for solicitation of Request for Proposals that reflects the desired restrictions and controls necessary to safeguard personal restricted information to be utilized as part of the third-party work**

Preparation for Notification of Affected Individuals

In the event there is a suspect data breach, the Kenton County School District will initiate the appropriate response plan. The Preparation for Notification of Affected Individuals was prepared using elements from the Best Practice Guide and pertinent data breach legislation. The Director of Technology shall be the Lead agent for the District and assume responsibility for the coordination of all internal investigation and notification procedures. The process for investigating a potential data breach is outlined in the following procedures:

- 1) The lead staff member charged with managing the breach of data security process shall be (Director of Technology).
 - 2) The lead staff member shall immediately notify the Superintendent of Schools regarding any data breach incident.
 - 3) The Superintendent of Schools shall notify District legal counsel regarding any data breach incidents.
 - 4) The lead staff member shall engage the District Safety and Security Officer to assist with the investigation.
 - 5) The lead staff member shall work with the departmental supervisor to ascertain the scope of the data breach as well as the schedule of affected individuals for the notification process.
 - 6) Notification to affected individuals whose unencrypted personal information have been, or are reasonably believed to have been, acquired by an unauthorized person shall be prepared and disseminated within 35 days in accordance with House Bill 5. A draft notification letter to individuals is found in Appendix D.
 - 7) Outside law enforcement agencies with expertise in investigating crimes that involve technology shall be contacted for advice and assistance with any data breach incidents. Identify any and all agencies that may be of assistance with an investigation and secure contact information in the case of a data breach incident.
 - 8) Immediately assess and prepare strategies to contain, control, and correct any data security breach incidents. Document any issues discovered and response actions taken.
 - 9) Perform a thorough review of the actions and flaws with the District data security platform leading up to the data breach. Make any necessary adjustments to the structure in order to prevent future incidents.
 - 10) Consider the use of a Cyber Resilience Review to evaluate the operational resilience and cyber-security practices.
-

Notification

As of January 1, 2015, Kentucky requires notification of suspected or confirmed data breaches. KRS 61.931, ET SEQ. (HB 5), Kentucky School Districts are required to notify both the individual of a breach and various state officials. House Bill 5 addresses the safety and security for personal information held by public agencies and requires public agencies and nonaffiliated third parties to implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.

House Bill 232 requires consumer notification when a private party data breach reveals personally identifiable information. This bill also requires cloud computing service providers contracting with educational institutions to maintain security of student data. The District Technology Coordinator shall assume responsibility for approving and finalizing all cloud based service provider agreements.

The District Technology coordinator shall utilize the following forms developed by the Commonwealth Office of Technology for use in the event of a breach or a suspected breach of data.

- [Data Breach Notification Form FAC-001 – See Appendix E](#)
- [Delay of Notification Form FAC-002 – See Appendix F](#)

The notification requirements are designed to alert individuals of such data breaches and provide those affected individuals with an opportunity to take appropriate actions to mitigate the personal damage from potential identity theft or other harm. The following guidelines were established by the Kentucky Data Breach legislation:

- Prepare a description of the categories of information that were subject to the security breach, including elements of personal information that were believed to be acquired;
 - Contact information for the notifying agency, including the address, telephone number;
 - A description of the general acts of the agency, excluding disclosure of defenses used for protection of information from the following sources about steps the individual may take to avoid identity theft, for:
 - The major consumer credit reporting agencies;
-

- The Federal Trade Commission; and
- The Office of the Kentucky Attorney General

The data breach legislation that went into effect in January 2015, each District has a total of 35 days from the time of their formal notification of agency contacts to notify all individuals impacted by the security breach. If the internal investigation leads to a reasonable conclusion that an unauthorized person through criminal activity may be involved in the data breach then the local law enforcement should be notified.

The appropriate State staff should be notified within 48 Hours if the investigation finds that the misuse of personal information has occurred or is likely to occur. The length of the investigation is not established by this bill and will vary with each incident.

Within 72 hours of a suspected or confirmed breach, notification shall be sent utilizing form FAC-001 to KDEDataBreachNotification@Education.ky.gov and to the following agencies as required by KRS 61.933:

- Attorney General's Office
- Auditor of Public Accounts
- Finance and Administration Cabinet
- Kentucky State Police
- Kentucky Department of Library and Archives
- Commonwealth Office of Technology

The Department of Data Breach Notification at the Kentucky Department of Education will provide the most current contact information for each State agency representative. If the investigation involves law enforcement officials and prevents the full disclosure of information to the Department, then form FAC-002 shall be utilized as required by KRS 61.933. The investigation shall be conducted in a reasonable and prompt manner in order to determine whether the security breach resulted in or is likely to result in the misuse of personal information



Appendix A

Department of Health and Human Services

§ 160.103

this subchapter apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
- (b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.
- (c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

§ 160.103 Definitions.

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.
Administrative simplification provision means any requirement or prohibition established by:

- (1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;
- (2) Section 264 of Pub. L. 104-191;
- (3) Sections 13400-13424 of Public Law 111-5; or
- (4) This subchapter.

ALJ means Administrative Law Judge.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

- (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization

review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

- (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

- (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

- (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the

extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or penalty means the amount determined under § 160.404 of this part and includes the plural of these terms.

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

- (1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
- (2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Electronic media means:

- (1) Electronic storage material on which data is or may be recorded electronically, including, for example, de-

vices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of *protected health information* as specified in this section.

Employer is defined as it is in 26 U.S.C. 3401(d).

Family member means, with respect to an individual:

- (1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great

grandchildren, and children of first cousins.

Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

- (i) The individual's genetic tests;
- (ii) The genetic tests of family members of the individual;
- (iii) The manifestation of a disease or disorder in family members of such individual; or
- (iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

- (i) A fetus carried by the individual or family member who is a pregnant woman; and
- (ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

- (1) A genetic test;
- (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
- (3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Group health plan (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their de-

pendents directly or through insurance, reimbursement, or otherwise, that:

- (1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
- (2) Is administered by an entity other than the employer that established and maintains the plan.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

- (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

- (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Manifestation or *manifested* means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Modify or *modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Person means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

Appendix B

§ 1232g

TITLE 20—EDUCATION

Page 828

§ 1232g. Family educational and privacy rights

(a) Conditions for availability of funds to educational agencies or institutions; inspection and review of education records; specific information to be made available; procedure for access to education records; reasonableness of time for such access; hearings; written explanations by parents; definitions

(1)(A) No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children. If any material or document in the education record of a student includes information on more than one student, the parents of one of such students shall have the right to inspect and review only such part of such material or document as relates to such student or to be informed of the specific information contained in such part of such material. Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.

(B) No funds under any applicable program shall be made available to any State educational agency (whether or not that agency is an educational agency or institution under this section) that has a policy of denying, or effectively prevents, the parents of students the right to inspect and review the education records maintained by the State educational agency on their children who are or have been in attendance at any school of an educational agency or institution that is subject to the provisions of this section.

(C) The first sentence of subparagraph (A) shall not operate to make available to students in institutions of postsecondary education the following materials:

(i) financial records of the parents of the student or any information contained therein;

(ii) confidential letters and statements of recommendation, which were placed in the education records prior to January 1, 1975, if such letters or statements are not used for purposes other than those for which they were specifically intended;

(iii) if the student has signed a waiver of the student's right of access under this subsection in accordance with subparagraph (D), confidential recommendations—

(I) respecting admission to any educational agency or institution,

(II) respecting an application for employment, and

(III) respecting the receipt of an honor or honorary recognition.

(D) A student or a person applying for admission may waive his right of access to confidential statements described in clause (iii) of subparagraph (C), except that such waiver shall apply to recommendations only if (i) the student is, upon request, notified of the names of all per-

sons making confidential recommendations and (ii) such recommendations are used solely for the purpose for which they were specifically intended. Such waivers may not be required as a condition for admission to, receipt of financial aid from, or receipt of any other services or benefits from such agency or institution.

(2) No funds shall be made available under any applicable program to any educational agency or institution unless the parents of students who are or have been in attendance at a school of such agency or at such institution are provided an opportunity for a hearing by such agency or institution, in accordance with regulations of the Secretary, to challenge the content of such student's education records, in order to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading or otherwise inappropriate data contained therein and to insert into such records a written explanation of the parents respecting the content of such records.

(3) For the purposes of this section the term "educational agency or institution" means any public or private agency or institution which is the recipient of funds under any applicable program.

(4)(A) For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which—

(i) contain information directly related to a student; and

(ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

(B) The term "education records" does not include—

(i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

(ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;

(iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or

(iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such

records can be personally reviewed by a physician or other appropriate professional of the student's choice.

(5)(A) For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

(B) Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent.

(6) For the purposes of this section, the term "student" includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution.

(b) **Release of education records; parental consent requirement; exceptions; compliance with judicial orders and subpoenas; audit and evaluation of federally-supported education programs; recordkeeping**

(1) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a) of this section) of students without the written consent of their parents to any individual, agency, or organization, other than to the following—

(A) other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests, including the educational interests of the child for whom consent would otherwise be required;

(B) officials of other schools or school systems in which the student seeks or intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record;

(C)(i) authorized representatives of (I) the Comptroller General of the United States, (II) the Secretary, or (III) State educational authorities, under the conditions set forth in paragraph (3), or (ii) authorized representatives of the Attorney General for law enforcement purposes under the same conditions as apply to the Secretary under paragraph (3);

(D) in connection with a student's application for, or receipt of, financial aid;

(E) State and local officials or authorities to whom such information is specifically allowed to be reported or disclosed pursuant to State statute adopted—

(i) before November 19, 1974, if the allowed reporting or disclosure concerns the juvenile justice system and such system's ability to effectively serve the student whose records are released, or

(ii) after November 19, 1974, if—

(I) the allowed reporting or disclosure concerns the juvenile justice system and such system's ability to effectively serve, prior to adjudication, the student whose records are released; and

(II) the officials and authorities to whom such information is disclosed certify in writing to the educational agency or institution that the information will not be disclosed to any other party except as provided under State law without the prior written consent of the parent of the student.¹

(F) organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted;

(G) accrediting organizations in order to carry out their accrediting functions;

(H) parents of a dependent student of such parents, as defined in section 152 of title 26;

(I) subject to regulations of the Secretary, in connection with an emergency, appropriate persons if the knowledge of such information is necessary to protect the health or safety of the student or other persons;

(J)(i) the entity or persons designated in a Federal grand jury subpoena, in which case the court shall order, for good cause shown, the educational agency or institution (and any officer, director, employee, agent, or attorney for such agency or institution) on which the subpoena is served, to not disclose to any person the existence or contents of the subpoena or any information furnished to the grand jury in response to the subpoena; and

(ii) the entity or persons designated in any other subpoena issued for a law enforcement purpose, in which case the court or other issuing agency may order, for good cause shown, the educational agency or institution (and any officer, director, employee, agent, or attorney for such agency or institution) on which the subpoena is served, to not disclose to any person the existence or contents of the subpoena or any information furnished in response to the subpoena; and

(K) the Secretary of Agriculture, or authorized representative from the Food and Nutrition Service or contractors acting on behalf of

¹So in original. The period probably should be a semicolon.

the Food and Nutrition Service, for the purposes of conducting program monitoring, evaluations, and performance measurements of State and local educational and other agencies and institutions receiving funding or providing benefits of 1 or more programs authorized under the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq.) or the Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.) for which the results will be reported in an aggregate form that does not identify any individual, on the conditions that—

(i) any data collected under this subparagraph shall be protected in a manner that will not permit the personal identification of students and their parents by other than the authorized representatives of the Secretary; and

(ii) any personally identifiable data shall be destroyed when the data are no longer needed for program monitoring, evaluations, and performance measurements.

Nothing in subparagraph (E) of this paragraph shall prevent a State from further limiting the number or type of State or local officials who will continue to have access thereunder.

(2) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of this subsection, unless—

(A) there is written consent from the student's parents specifying records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents, or

(B) except as provided in paragraph (1)(J), such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.

(3) Nothing contained in this section shall preclude authorized representatives of (A) the Comptroller General of the United States, (B) the Secretary, or (C) State educational authorities from having access to student or other records which may be necessary in connection with the audit and evaluation of Federally-supported education programs, or in connection with the enforcement of the Federal legal requirements which relate to such programs: *Provided*, That except when collection of personally identifiable information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements.

(4)(A) Each educational agency or institution shall maintain a record, kept with the education

records of each student, which will indicate all individuals (other than those specified in paragraph (1)(A) of this subsection), agencies, or organizations which have requested or obtained access to a student's education records maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information. Such record of access shall be available only to parents, to the school official and his assistants who are responsible for the custody of such records, and to persons or organizations authorized in, and under the conditions of, clauses (A) and (C) of paragraph (1) as a means of auditing the operation of the system.

(B) With respect to this subsection, personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student. If a third party outside the educational agency or institution permits access to information in violation of paragraph (2)(A), or fails to destroy information in violation of paragraph (1)(F), the educational agency or institution shall be prohibited from permitting access to information from education records to that third party for a period of not less than five years.

(5) Nothing in this section shall be construed to prohibit State and local educational officials from having access to student or other records which may be necessary in connection with the audit and evaluation of any federally or State supported education program or in connection with the enforcement of the Federal legal requirements which relate to any such program, subject to the conditions specified in the proviso in paragraph (3).

(6)(A) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing, to an alleged victim of any crime of violence (as that term is defined in section 16 of title 18), or a nonforcible sex offense, the final results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime or offense with respect to such crime or offense.

(B) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing the final results of any disciplinary proceeding conducted by such institution against a student who is an alleged perpetrator of any crime of violence (as that term is defined in section 16 of title 18), or a nonforcible sex offense, if the institution determines as a result of that disciplinary proceeding that the student committed a violation of the institution's rules or policies with respect to such crime or offense.

(C) For the purpose of this paragraph, the final results of any disciplinary proceeding—

(i) shall include only the name of the student, the violation committed, and any sanction imposed by the institution on that student; and

(ii) may include the name of any other student, such as a victim or witness, only with the written consent of that other student.

(7)(A) Nothing in this section may be construed to prohibit an educational institution

from disclosing information provided to the institution under section 14071² of title 42 concerning registered sex offenders who are required to register under such section.

(B) The Secretary shall take appropriate steps to notify educational institutions that disclosure of information described in subparagraph (A) is permitted.

(c) Surveys or data-gathering activities; regulations

Not later than 240 days after October 20, 1994, the Secretary shall adopt appropriate regulations or procedures, or identify existing regulations or procedures, which protect the rights of privacy of students and their families in connection with any surveys or data-gathering activities conducted, assisted, or authorized by the Secretary or an administrative head of an education agency. Regulations established under this subsection shall include provisions controlling the use, dissemination, and protection of such data. No survey or data-gathering activities shall be conducted by the Secretary, or an administrative head of an education agency under an applicable program, unless such activities are authorized by law.

(d) Students' rather than parents' permission or consent

For the purposes of this section, whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student.

(e) Informing parents or students of rights under this section

No funds shall be made available under any applicable program to any educational agency or institution unless such agency or institution effectively informs the parents of students, or the students, if they are eighteen years of age or older, or are attending an institution of postsecondary education, of the rights accorded them by this section.

(f) Enforcement; termination of assistance

The Secretary shall take appropriate actions to enforce this section and to deal with violations of this section, in accordance with this chapter, except that action to terminate assistance may be taken only if the Secretary finds there has been a failure to comply with this section, and he has determined that compliance cannot be secured by voluntary means.

(g) Office and review board; creation; functions

The Secretary shall establish or designate an office and review board within the Department for the purpose of investigating, processing, reviewing, and adjudicating violations of this section and complaints which may be filed concerning alleged violations of this section. Except for the conduct of hearings, none of the functions of the Secretary under this section shall be carried out in any of the regional offices of such Department.

² See References in Text note below.

(h) Disciplinary records; disclosure

Nothing in this section shall prohibit an educational agency or institution from—

(1) including appropriate information in the education record of any student concerning disciplinary action taken against such student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community; or

(2) disclosing such information to teachers and school officials, including teachers and school officials in other schools, who have legitimate educational interests in the behavior of the student.

(i) Drug and alcohol violation disclosures

(1) In general

Nothing in this Act or the Higher Education Act of 1965 [20 U.S.C. 1001 et seq., 42 U.S.C. 2751 et seq.] shall be construed to prohibit an institution of higher education from disclosing, to a parent or legal guardian of a student, information regarding any violation of any Federal, State, or local law, or of any rule or policy of the institution, governing the use or possession of alcohol or a controlled substance, regardless of whether that information is contained in the student's education records, if—

(A) the student is under the age of 21; and

(B) the institution determines that the student has committed a disciplinary violation with respect to such use or possession.

(2) State law regarding disclosure

Nothing in paragraph (1) shall be construed to supersede any provision of State law that prohibits an institution of higher education from making the disclosure described in subsection (a) of this section.

(j) Investigation and prosecution of terrorism

(1) In general

Notwithstanding subsections (a) through (i) of this section or any provision of State law, the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring an educational agency or institution to permit the Attorney General (or his designee) to—

(A) collect education records in the possession of the educational agency or institution that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18, or an act of domestic or international terrorism as defined in section 2331 of that title; and

(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such records, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

(2) Application and approval

(A) IN GENERAL.—An application under paragraph (1) shall certify that there are specific

and articulable facts giving reason to believe that the education records are likely to contain information described in paragraph (1)(A).

(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

(3) Protection of educational agency or institution

An educational agency or institution that, in good faith, produces education records in accordance with an order issued under this subsection shall not be liable to any person for that production.

(4) Record-keeping

Subsection (b)(4) of this section does not apply to education records subject to a court order under this subsection.

(Pub. L. 90-247, title IV, § 444, formerly § 438, as added Pub. L. 93-380, title V, § 513(a), Aug. 21, 1974, 88 Stat. 571; amended Pub. L. 93-568, § 2(a), Dec. 31, 1974, 88 Stat. 1858; Pub. L. 96-46, § 4(o), Aug. 6, 1979, 93 Stat. 342; Pub. L. 101-542, title II, § 203, Nov. 8, 1990, 104 Stat. 2385; Pub. L. 102-325, title XV, § 1555(a), July 23, 1992, 106 Stat. 840; renumbered § 444 and amended Pub. L. 103-382, title II, §§ 212(b)(1), 249, 261(h), Oct. 20, 1994, 108 Stat. 3913, 3924, 3928; Pub. L. 105-244, title IX, §§ 851, 952, Oct. 7, 1998, 112 Stat. 1835, 1836; Pub. L. 106-386, div. B, title VI, § 1601(d), Oct. 28, 2000, 114 Stat. 1538; Pub. L. 107-56, title V, § 507, Oct. 26, 2001, 115 Stat. 387; Pub. L. 107-110, title X, § 1062(3), Jan. 8, 2002, 115 Stat. 2088; Pub. L. 111-296, title I, § 103(d), Dec. 13, 2010, 124 Stat. 3192.)

REFERENCES IN TEXT

The Richard B. Russell National School Lunch Act, referred to in subsec. (b)(1)(K), is act June 4, 1946, ch. 281, 60 Stat. 230, which is classified generally to chapter 13 (§ 1761 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 1751 of Title 42 and Tables.

The Child Nutrition Act of 1966, referred to in subsec. (b)(1)(K), is Pub. L. 89-642, Oct. 11, 1966, 80 Stat. 885, which is classified generally to chapter 13A (§ 1771 et seq.) of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 1771 of Title 42 and Tables.

Section 14071 of title 42, referred to in subsec. (b)(7)(A), was repealed by Pub. L. 109-248, title I, § 129(a), July 27, 2006, 120 Stat. 600.

This Act, referred to in subsec. (1)(1), is Pub. L. 90-247, Jan. 2, 1968, 80 Stat. 783, known as the Elementary and Secondary Education Amendments of 1967. Title IV of the Act, known as the General Education Provisions Act, is classified generally to this chapter. For complete classification of this Act to the Code, see Short Title of 1968 Amendment note set out under section 6301 of this title and Tables.

The Higher Education Act of 1965, referred to in subsec. (1)(1), is Pub. L. 89-328, Nov. 8, 1965, 79 Stat. 1219, which is classified generally to chapter 28 (§ 1001 et seq.) of this title and part C (§ 2751 et seq.) of subchapter I of chapter 34 of Title 42, The Public Health and Welfare. For complete classification of this Act to the Code, see Short Title note set out under section 1001 of this title and Tables.

PRIOR PROVISIONS

A prior section 444 of Pub. L. 90-247 was classified to section 1232c of this title prior to repeal by Pub. L. 103-382.

AMENDMENTS

2010—Subsec. (b)(1)(K). Pub. L. 111-296, which directed that par. (1) be amended by adding subpar. (K) "at the end", was executed by adding subpar. (K) after subpar. (J), to reflect the probable intent of Congress.

2002—Subsec. (a)(1)(B). Pub. L. 107-110, § 1062(3)(A), realigned margins.

Subsec. (b)(1). Pub. L. 107-110, § 1062(3)(C), substituted "subparagraph (B)" for "clause (B)" in concluding provisions.

Subsec. (b)(1)(J). Pub. L. 107-110, § 1062(3)(B), realigned margins.

Subsec. (b)(7). Pub. L. 107-110, § 1062(3)(D), realigned margins.

2001—Subsec. (j). Pub. L. 107-56 added subsec. (j).

2000—Subsec. (b)(7). Pub. L. 106-386 added par. (7).

1994—Subsec. (b)(1)(C). Pub. L. 105-244, § 851(1), amended subpar. (C) generally. Prior to amendment, subpar. (C) read as follows: "authorized representatives of (i) the Comptroller General of the United States, (ii) the Secretary, or (iii) State educational authorities, under the conditions set forth in paragraph (3) of this subsection;"

Subsec. (b)(6). Pub. L. 105-244, § 851(2), designated existing provisions as subpar. (A), substituted "or a non-forcible sex offense, the final results" for "the results", substituted "such crime or offense" for "such crime" in two places, and added subpars. (B) and (C).

Subsec. (i). Pub. L. 105-244, § 952, added subsec. (i).

1994—Subsec. (a)(1)(B). Pub. L. 103-382, § 249(1)(A)(ii), added subpar. (B). Former subpar. (B) redesignated (C).

Subsec. (a)(1)(C). Pub. L. 103-382, § 249(1)(A)(i), (iii), redesignated subpar. (B) as (C) and substituted "subparagraph (D)" for "subparagraph (C)" in cl. (iii). Former subpar. (C) redesignated (D).

Subsec. (a)(1)(D). Pub. L. 103-382, § 249(1)(A)(i), (iv), redesignated subpar. (C) as (D) and substituted "subparagraph (C)" for "subparagraph (B)".

Subsec. (a)(2). Pub. L. 103-382, § 249(1)(B), substituted "privacy rights" for "privacy or other rights".

Subsec. (a)(4)(B)(ii). Pub. L. 103-382, § 261(h)(1), substituted semicolon for period at end.

Subsec. (b)(1)(A). Pub. L. 103-382, § 249(2)(A)(i), inserted before semicolon "including the educational interests of the child for whom consent would otherwise be required".

Subsec. (b)(1)(C). Pub. L. 103-382, § 261(h)(2)(A), substituted "or (iii)" for "(iii)" an administrative head of an education agency (as defined in section 1212e-3(c) of this title), or (iv)".

Subsec. (b)(1)(E). Pub. L. 103-382, § 249(2)(A)(ii), amended subpar. (E) generally. Prior to amendment, subpar. (E) read as follows: "State and local officials or authorities to whom such information is specifically required to be reported or disclosed pursuant to State statute adopted prior to November 19, 1974:"

Subsec. (b)(1)(H). Pub. L. 103-382, § 261(h)(2)(B), substituted "the Internal Revenue Code of 1986" for "the Internal Revenue Code of 1954", which for purposes of codification was translated as "title 26" thus requiring no change in text.

Subsec. (b)(1)(J). Pub. L. 103-382, § 249(2)(A)(iii)-(v), added subpar. (J).

Subsec. (b)(2). Pub. L. 103-382, § 249(2)(B)(i), which directed amendment of matter preceding subpar. (A) by substituting "unless—" for the period, was executed by substituting a comma for the period before "unless—" to reflect the probable intent of Congress.

Subsec. (b)(2)(B). Pub. L. 103-382, § 249(2)(B)(ii), inserted "except as provided in paragraph (1)(J)," before "such information".

Subsec. (b)(3). Pub. L. 103-382, § 261(h)(2)(C), substituted "or (C)" for "(C)" an administrative head of an education agency or (D)" and "education programs" for "education program".

Subsec. (b)(4). Pub. L. 103-382, § 249(2)(C), inserted at end "If a third party outside the educational agency or institution permits access to information in violation of paragraph (2)(A), or fails to destroy information in

violation of paragraph (1)(F), the educational agency or institution shall be prohibited from permitting access to information from education records to that third party for a period of not less than five years."

Subsec. (c). Pub. L. 103-382, §249(3), substituted "Not later than 240 days after October 20, 1994, the Secretary shall adopt appropriate regulations or procedures, or identify existing regulations or procedures, which" for "The Secretary shall adopt appropriate regulations to".

Subsec. (d). Pub. L. 103-382, §261(h)(3), inserted a comma after "education".

Subsec. (e). Pub. L. 103-382, §249(4), inserted "effectively" before "informa".

Subsec. (f). Pub. L. 103-382, §261(h)(4), struck out ", or an administrative head of an education agency," after "The Secretary" and substituted "enforce this section" for "enforce provisions of this section", "in accordance with" for "according to the provisions of", and "comply with this section" for "comply with the provisions of this section".

Subsec. (g). Pub. L. 103-382, §261(h)(5), struck out "of Health, Education, and Welfare" after "the Department" and "the provisions of" after "adjudicating violations of".

Subsec. (h). Pub. L. 103-382, §249(6), added subsec. (h). 1992—Subsec. (a)(4)(B)(ii). Pub. L. 102-325 amended cl. (ii) generally. Prior to amendment, cl. (ii) read as follows: "if the personnel of a law enforcement unit do not have access to education records under subsection (b)(1) of this section, the records and documents of such law enforcement unit which (i) are kept apart from records described in subparagraph (A), (ii) are maintained solely for law enforcement purposes, and (iii) are not made available to persons other than law enforcement officials of the same jurisdiction.".

1990—Subsec. (b)(6). Pub. L. 101-542 added par. (6).

1979—Subsec. (b)(6). Pub. L. 96-46 added par. (6).

1974 Subsec. (a)(1). Pub. L. 93-568, §2(a)(1)(A)-(C), (2)(A) (C), (3), designated existing par. (1) as subpar. (A), substituted reference to educational agencies and institutions for reference to state or local educational agencies, institutions of higher education, community colleges, schools, agencies offering preschool programs, and other educational institutions, substituted the generic term education records for the enumeration of such records, and extended the right to inspect and review such records to parents of children who have been in attendance, and added subpars. (B) and (C).

Subsec. (a)(2). Pub. L. 93-568, §2(a)(4), substituted provisions making the availability of funds to educational agencies and institutions conditional on the granting of an opportunity for a hearing to parents of students who are or have been in attendance at such institution or agency to challenge the contents of the student's education records for provisions granting the parents an opportunity for such hearing, and inserted provisions authorizing insertion into the records a written explanation of the parents respecting the content of such records.

Subsec. (a)(3) to (6). Pub. L. 93-568, §2(a)(1)(G), (2)(F), (5), added pars. (3) to (6).

Subsec. (b)(1). Pub. L. 93-568, §2(a)(1)(D), (2)(D), (6), (8)(A)-(C), (10)(A), in provisions preceding subpar. (A), substituted "educational agency or institution which has a policy of permitting the release of education records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a) of this section)" for "state or local educational agency, any institution of higher education, any community college, any school, agency offering a preschool program, or any other educational institution which has a policy or practice of permitting the release of personally identifiable records or files (or personal information contained therein)", in subpar. (A), substituted "educational agency, who have been determined by such agency or institution to have" for "educational agency who have", in subpar. (B), substituted "the student seeks or intends to" for "the student intends to", in

subpar. (C), substituted reference to "section 408(c)" for reference to "section 409 of this Act" which for purposes of codification has been translated as "section 1221e-3(c) of this title", and added subpars. (E) to (I).

Subsec. (b)(2). Pub. L. 93-568, §2(a)(1)(E), (2)(E), substituted "educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of this subsection" for "state or local educational agency, any institution of higher education, any community college, any school, agency offering a preschool program, or any other educational institution which has a policy or practice of furnishing, in any form, any personally identifiable information contained in personal school records, to any persons other than those listed in subsection (b)(1) of this section".

Subsec. (b)(3). Pub. L. 93-568, §2(a)(6)(D), substituted "information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements" for "data is specifically authorized by Federal law, any data collected by such officials with respect to individual students shall not include information (including social security numbers) which would permit the personal identification of such students or their parents after the data so obtained has been collected".

Subsec. (b)(4). Pub. L. 93-568, §2(a)(9), substituted provisions that each educational agency or institution maintain a record, kept with the education records of each student, indicating individuals, agencies, or organizations who obtained access to the student's record and the legitimate interest in obtaining such information, that such record of access shall be available only to parents, school officials, and their assistants having responsibility for the custody of such records, and as a means of auditing the operation of the system, for provisions that with respect to subsecs. (c)(1), (c)(2), and (c)(3) of this section, all persons, agencies, or organizations desiring access to the records of a student shall be required to sign forms to be kept with the records of the student, but only for inspection by the parents or the student, indicating specifically the legitimate educational or other interest of the person seeking such information, and that the form shall be available to parents and school officials having responsibility for record maintenance as a means of auditing the operation of the system.

Subsec. (e). Pub. L. 93-568, §2(a)(1)(F), substituted "to any educational agency or institution unless such agency or institution" for "unless the recipient of such funds".

Subsec. (g). Pub. L. 93-568, §2(a)(7), (10)(B), struck out reference to sections 1232c and 1232f of this title and inserted provisions that except for the conduct of hearings, none of the functions of the Secretary under this section shall be carried out in any of the regional offices of such Department.

EFFECTIVE DATE OF 2010 AMENDMENT

Amendment by Pub. L. 111-296 effective Oct. 1, 2010, except as otherwise specifically provided, see section 445 of Pub. L. 111-296, set out as a note under section 1751 of Title 42, The Public Health and Welfare.

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107-110 effective Jan. 8, 2002, except with respect to certain noncompetitive programs and competitive programs, see section 6 of Pub. L. 107-110, set out as an Effective Date note under section 6301 of this title.

EFFECTIVE DATE OF 1998 AMENDMENT

Amendment by Pub. L. 105-244 effective Oct. 1, 1998, except as otherwise provided in Pub. L. 105-244, see section 6301 of this title.

tion 3 of Pub. L. 105-244, set out as a note under section 1001 of this title.

EFFECTIVE DATE OF 1992 AMENDMENT

Section 1555(b) of Pub. L. 102-325 provided that: "The amendment made by this section [amending this section] shall take effect on the date of enactment of this Act [July 23, 1992]."

EFFECTIVE DATE OF 1979 AMENDMENT

Amendment by Pub. L. 96-46 effective Oct. 1, 1978, see section 8 of Pub. L. 96-46, set out as a note under section 930 of this title.

EFFECTIVE DATE OF 1974 AMENDMENT

Section 2(b) of Pub. L. 93-583 provided that: "The amendments made by subsection (a) [amending this section] shall be effective, and retroactive to, November 19, 1974."

EFFECTIVE DATE

Section 513(b)(1) of Pub. L. 93-380 provided that: "The provisions of this section [enacting this section and provisions set out as a note under section 1221 of this title] shall become effective ninety days after the date of enactment [Aug. 21, 1974] of section 438 [now 444] of the General Education Provisions Act [this section]."

§ 1232h. Protection of pupil rights

(a) Inspection of instructional materials by parents or guardians

All instructional materials, including teacher's manuals, films, tapes, or other supplementary material which will be used in connection with any survey, analysis, or evaluation as part of any applicable program shall be available for inspection by the parents or guardians of the children.

(b) Limits on survey, analysis, or evaluations

No student shall be required, as part of any applicable program, to submit to a survey, analysis, or evaluation that reveals information concerning--

- (1) political affiliations or beliefs of the student or the student's parent;
- (2) mental or psychological problems of the student or the student's family;
- (3) sex behavior or attitudes;
- (4) illegal, anti-social, self-incriminating, or demeaning behavior;
- (5) critical appraisals of other individuals with whom respondents have close family relationships;
- (6) legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- (7) religious practices, affiliations, or beliefs of the student or student's parent; or
- (8) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

without the prior consent of the student (if the student is an adult or emancipated minor), or in the case of an unemancipated minor, without the prior written consent of the parent.

(c) Development of local policies concerning student privacy, parental access to information, and administration of certain physical examinations to minors

(1) Development and adoption of local policies

Except as provided in subsections (a) and (b) of this section, a local educational agency

that receives funds under any applicable program shall develop and adopt policies, in consultation with parents, regarding the following:

(A)(i) The right of a parent of a student to inspect, upon the request of the parent, a survey created by a third party before the survey is administered or distributed by a school to a student; and

(ii) any applicable procedures for granting a request by a parent for reasonable access to such survey within a reasonable period of time after the request is received.

(B) Arrangements to protect student privacy that are provided by the agency in the event of the administration or distribution of a survey to a student containing one or more of the following items (including the right of a parent of a student to inspect, upon the request of the parent, any survey containing one or more of such items):

- (i) Political affiliations or beliefs of the student or the student's parent.
- (ii) Mental or psychological problems of the student or the student's family.
- (iii) Sex behavior or attitudes.
- (iv) Illegal, anti-social, self-incriminating, or demeaning behavior.
- (v) Critical appraisals of other individuals with whom respondents have close family relationships.
- (vi) Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers.
- (vii) Religious practices, affiliations, or beliefs of the student or the student's parent.
- (viii) Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

(C)(i) The right of a parent of a student to inspect, upon the request of the parent, any instructional material used as part of the educational curriculum for the student; and

(ii) any applicable procedures for granting a request by a parent for reasonable access to instructional material within a reasonable period of time after the request is received.

(D) The administration of physical examinations or screenings that the school or agency may administer to a student.

(E) The collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose), including arrangements to protect student privacy that are provided by the agency in the event of such collection, disclosure, or use.

(F)(i) The right of a parent of a student to inspect, upon the request of the parent, any instrument used in the collection of personal information under subparagraph (E) before the instrument is administered or distributed to a student; and

(ii) any applicable procedures for granting a request by a parent for reasonable access to such instrument within a reasonable period of time after the request is received.

Appendix C

MEMORANDUM OF UNDERSTANDING BETWEEN _____ AND THE KENTON COUNTY BOARD OF EDUCATION TO DESIGNATE AN AUTHORIZED REPRESENTATIVE FOR THE KENTON COUNTY BOARD OF EDUCATION FOR THE AUDIT/EVALUATION OF EDUCATION PROGRAMS AND TO AUTHORIZE THE RELEASE AND USE OF CONFIDENTIAL DATA

*** **

THIS AGREEMENT is made and entered into by and between the Kenton County Board of Education ("KCBOE") and _____ (hereafter "Authorized Representative") and establishes the procedures relating to an exchange of information between the Parties.

WHEREAS, the KCBOE is the public local education agency organized under Kentucky Law and its duties include audit or evaluation functions of federal or state-supported education programs or enforcement or compliance with federal or state legal requirements that relate to those education programs (audit, evaluation or enforcement or compliance activity) in its role as the local education agency and in evaluation of education programs to identify or develop the best education practices to be used in public schools of Kenton County Kentucky;

WHEREAS, the Authorized Representative is an entity performing audit or evaluation functions at the direction and under the control of the KCBOE and the Authorized Representative is a contractor acting in the place of the KCBOE to perform the KCBOE's audit or evaluation functions of federal or state-supported education programs or to enforce or comply with federal legal requirements that relate to those education programs (audit, evaluation or enforcement or compliance activity) in its role as the state education agency and in evaluation of education programs, as described below;

WHEREAS, various elements of the data maintained by the agencies are protected by the Privacy Act of 1974, 5 U.S.C. 552a; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g); the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.;

NOW THEREFORE, the KCBOE and the Authorized Representative hereby mutually agree as follows:

Section 1. Designation of Authority.

- A. The KCBOE hereby designates the Authorized Representative and its subcontractors identified below as an "authorized representative" of the KCBOE, as defined in 34 C.F.R. 99.31 (a)(3) and 99.35, with respect to the provision of audit or evaluation functions of federal or state-supported education programs or to enforce or comply with federal or state legal requirements that relate to those education programs (audit, evaluation or enforcement or compliance activity) in the KCBOE's role as the local education agency and in evaluation of education programs ("audit/evaluation services") and, specifically, with respect to the use of confidential data disclosed under this agreement.
-

B. The KCBOE and the Authorized Representative hereby agree that, if free or reduced price lunch eligibility data (i.e., free or reduced price lunch eligibility data which is the student poverty indicator for most education programs) is to be released to the Authorized Representative, then the KCBOE shall identify the Authorized Representative as a contractor acting in the place of the KCBOE; shall ensure that the audit/evaluation services include a "need to know" this data as required by 7 C.F.R. 245.6 (f); and shall ensure that the data will only be disclosed to the Authorized Representative upon written request utilizing the U.S. Department of Agriculture Prototype Agreement. The completed USDA Prototype Agreement shall be attached in Exhibit A and incorporated into this agreement as if set forth fully herein and KCBOE's agreement that the Authorized Representative meets the requirements for disclosure set forth in 7 C.F.R. 245.6 (f) and that the Authorized Representative has demonstrated a "need to know" shall be evidenced by the KCBOE's agreement to enter the USDA Prototype Agreement.

Section 2. Acknowledgment of Release of Confidential Data, Identification of Confidential Data to be Released to the Authorized Representative and Description of Use of Data by the Authorized Representative.

A. The parties acknowledge that the KCBOE is releasing confidential data including student and non-student information to the Authorized Representative for the purposes outlined herein, and that the release of the KCBOE confidential data including student and non-student information to the Authorized Representative is necessary for the completion of the KCBOE's audit/evaluation services. The confidential data including student and non-student information to be disclosed is described in a document attached to this agreement as Exhibit A. The Authorized Representative shall notify the KCBOE and the KCBOE shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the provision of audit/evaluation services. The Authorized Representative will use personally identifiable information from education records and other records in order to perform the audit/evaluation services described in Exhibit A. The description of the audit/evaluation services, as included in Exhibit A, shall include the purpose and scope of the audit/evaluation services, specific description of the methodology of disclosure and an explanation as to the need for confidential data including student and non-student information to perform these audit/evaluation services. The Authorized Representative shall notify the KCBOE and the KCBOE shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the audit/evaluation services or any changes to the scope or purpose of the audit/evaluation services themselves. Any agreed upon changes to the data disclosed or to the audit/evaluation services shall be reduced to writing and included in Exhibit A to this agreement.

B. If free or reduced price lunch eligibility data (i.e., free or reduced price lunch eligibility data which is the student poverty indicator for most education programs) is to be released to the Authorized Representative, then the KCBOE shall disclose this data to the Authorized Representative, upon written request utilizing the U.S. Department of Agriculture prototype request and confidentiality agreement, and upon the KCBOE agreeing that the Authorized Representative has demonstrated that disclosure is allowed by 7 C.F.R. 245.6. A description of any data protected by 7 C.F.R. 245.6 which is to be disclosed under this agreement shall be included in Exhibit A, Section III. Any agreed upon changes to the data disclosed or to the audit/evaluation services shall be reduced to writing and included in Exhibit A, Section III to this agreement.

Section 3. The Authorized Representative and the Authorized Users' Obligations.

A. The Authorized Representative shall not share these confidential data with anyone, except those employees of the Authorized Representative and the Authorized Representative's subcontractors, ("Authorized Users") that are directly involved and have a legitimate interest under FERPA or a "need to know" (as defined in 7 C.F.R. 245.6 in the case of disclosure of free or reduced price lunch eligibility data which is the student poverty indicator for education programs) in the performance of the audit/evaluation

services according to the terms of this agreement or any overarching agreement between the KCBOE and the Authorized Representative in which the Authorized Representative agrees to perform these audit/evaluation services on the KCBOE's behalf ("Master Agreement").

B. The Authorized Representative shall require all Authorized Users to comply with FERPA and other applicable state and federal student and non-student privacy laws. The Authorized Representative shall require and maintain confidentiality agreements or the KCBOE's Nondisclosure Statement(s) with each Authorized User of confidential data. If a confidentiality agreement with each Authorized User is used which is different from the KCBOE's Nondisclosure Statement(s), then the terms of the Authorized Representative's confidentiality agreements shall contain, at a minimum, the terms and conditions of this agreement and a copy of the current Authorized Representative's confidentiality agreement or the KCBOE's Nondisclosure Statement(s), as appropriate, shall be attached to this agreement as Exhibit B.

C. Authorized Representative that receive Personal Information as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act.

"Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- a) An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
- b) A Social Security number;
- c) A taxpayer identification number that incorporates a Social Security number;
- d) A driver's license number, state identification card number or other individual identification number issued by an agency;
- e) A passport number or other identification number issued by the United States government; or
- f) Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

As provided in KRS 61.931(5), a "non-affiliated third party" means "any person or entity that has a contract or agreement with the Commonwealth and receives (accesses, collects or maintains) personal information from the Commonwealth pursuant to the contract or agreement."

Contractor shall not redisclose, without written consent of the KCBOE, any "personal information," as defined in KRS 61-931, or any other personally identifiable information of a student or other persons, such as employees.

D. The Authorized Representative hereby agrees to cooperate with the Commonwealth in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

E. The Authorized Representative shall notify as soon as possible, but not to exceed seventy-two (72) hours, the Kentucky Department of Education, the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Commonwealth Office of Technology of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)2 applies and the vendor abides by the requirements set forth in that exception. If the agency is a unit of government listed in KRS 61.931(1)(b), the vendor shall notify the Commissioner of the Department of Local Government in the same manner as above. If the agency is a public school district listed in KRS 61.931(1)(d), the vendor shall notify the Commissioner of the Department of Education in the same manner as above. If the agency is an educational entity listed under KRS 61.931(1)(e), the vendor shall notify the Council on Postsecondary Education in the same manner as above. Notification shall be in writing on the form developed by the Commonwealth Office of Technology and incorporated by reference into Kentucky Regulation 200 KAR 1:015.

F. The Authorized Representative hereby agrees that the Commonwealth may withhold payment(s) owed to the vendor for any violation of the Identity Theft Prevention Reporting Requirements.

G. The Authorized Representative hereby agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

H. Upon conclusion of an investigation of a security breach of Personal Information as required by KRS 61.933, the Authorized Representative hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.

I. In accordance with KRS 61.932(2)(a) the Authorized Representative shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth Office of Technology:
<http://technology.ky.gov/ciso/Pages/InformationSecurityPolicies.StandardsandProcedures.aspx>.

J. If Authorized Representative is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person or entity other than an educational institution that operates cloud computing services"), Authorized Representative does further agree that:

- Authorized Representative shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. The Authorized Representative shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data".
 - With a written agreement for educational research, Authorized Representative may assist an educational institution to conduct educational research as permitted by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C. sec. 1232g.
 - Pursuant to KRS 365.734, Authorized Representative shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
 - Pursuant to KRS 365.734, Authorized Representative shall not sell, disclose, or otherwise process student data for any commercial purpose.
-

K. Pursuant to KRS 365.734, Authorized Representative shall certify in writing to the agency that it will comply with KRS 365.734(2).

The Authorized Representative shall protect confidential and otherwise personally identifiable data in a manner that does not permit personal identification of students and their parents, and non-students by anyone except those bound by this agreement and the KCBOE. The Authorized Representative shall store all confidential data on secure data servers using current industry best practices. The Authorized Representative shall notify the KCBOE as soon as practicable if the Authorized Representative learns of any security breach to the server containing the confidential and otherwise personally identifiable data or of any disclosure of confidential and otherwise personally identifiable data to anyone other than the Authorized Representative's Authorized Users or the KCBOE officials authorized to receive confidential and otherwise personally identifiable data. The Authorized Representative shall cooperate and take all reasonable means prescribed by the KCBOE to secure any breaches as soon as practicable.

L. The Authorized Representative shall not redisclose the KCBOE's confidential and otherwise personally identifiable data to any other party without the prior consent of the parent or eligible student except as allowed by applicable federal and state law.

M. The Authorized Representative certifies that it has the capacity to restrict access to confidential and otherwise personally identifiable data solely to Authorized Users and to ensure that the confidential and otherwise personally identifiable data is accessed only for the purposes described in this agreement. A copy of the Authorized Representative's data security policies and procedures is attached to this agreement as Exhibit C.

N. The Authorized Representative shall destroy all confidential and otherwise personally identifiable data within forty-five (45) days after it is no longer needed to perform the audit/evaluation services described in this agreement, upon KCBOE's request or upon termination of this agreement, whichever occurs first unless agreed otherwise in writing. The Authorized Representative's description of the method(s) which will be used to destroy all confidential data shall be attached to this agreement as Exhibit D. The Authorized Representative shall provide written verification of the data destruction to the KCBOE within forty-five (45) days after the data is destroyed.

O. The Authorized Representative shall permit the KCBOE, at the KCBOE's cost and upon written reasonable request, to audit the Authorized Representative to confirm that the Authorized Representative is complying with the data security policies and procedures in Exhibit C and/or that the Authorized Representative has destroyed the data as verified.

P. The Authorized Representative shall collect and use these confidential and otherwise personally identifiable data only for the purpose of helping the KCBOE perform audit/evaluation services related to the activities outlined in this agreement or in any Master Agreement.

Q. The Authorized Representative shall obtain prior written approval from the KCBOE before accessing confidential and otherwise personally identifiable data for activities beyond the scope specified in this agreement or in a Master Agreement; and, any access beyond the scope of this agreement or a Master Agreement shall be consistent with federal and state law requirements. Any confidential and otherwise personally identifiable data collected by the Authorized Representative under activities approved by the KCBOE under this section, which are not regularly collected within the scope of this agreement but are consistent with the activities described in this agreement, shall be subject to the terms and conditions of this agreement.

R. If the Authorized Representative becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then the Authorized Representative shall use all reasonable efforts to provide the KCBOE with prior notice before disclosure so that the KCBOE may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure the KCBOE's compliance with the confidentiality requirements of federal or state law; provided, however, that the Authorized Representative will use all reasonable efforts to maintain the confidentiality of confidential and otherwise personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, the Authorized Representative will only disclose that portion of confidential and otherwise personally identifiable data that the Authorized Representative is legally required to disclose.

S. The Authorized Representative shall abide by and be bound by the requirements of the U.S. Department of Education, Family Policy Compliance Office's Guidance for Reasonable Methods and Written Agreements issued pursuant to the requirements of the Family Educational Rights and Privacy Act ("Guidance"). The Guidance is available by clicking the following hyperlink, http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemt_d_agreement.pdf and made a part of this agreement as if stated fully herein.

T. The Authorized Representative shall also, if the data shared by the KCBOE includes data protected by 7 C.F.R. 245.6 (i.e., free or reduced price lunch eligibility data which is the student poverty indicator for most education programs), abide by the restrictions of disclosure and confidentiality requirements contained in 7 C.F.R. 245.6 (f) applicable to the KCBOE.

Section 4. Permission to Use Data.

The KCBOE acknowledges that by entering this agreement it is approving, in writing, of the Authorized Representative's use of these confidential data within the scope of purposes outlined in this agreement.

Section 5. Transfer Protocol.

The KCBOE and the Authorized Representative shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. The Authorized Representative shall confirm the transfer of confidential data and notify the KCBOE as soon as practicable of any discrepancies between the actual data transferred and the data described in this agreement. The same protocol shall apply to any transfer of confidential data from the Authorized Representative to the KCBOE.

Section 6. Breach of Data Confidentiality and Remedies.

The Authorized Representative acknowledges that the breach of this agreement or its part may result in irreparable and continuing damage to the KCBOE for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by the Authorized Representative, the KCBOE, in addition to any other rights and remedies available to the KCBOE at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that the Authorized Representative has violated paragraph 34 C.F.R. 99.31(a)(3), the KCBOE may not allow the Authorized Representative access to personally identifiable information from education records for at least five (5) years. If the Authorized Representative breaches the confidentiality requirements of 7 C.F.R. 245.6 relative to any confidential free or reduced price lunch eligibility data, then the Authorized Representative shall be responsible for any consequences or penalties which result from such breach.

Section 7. Amendment and Assignability.

The terms and conditions of this agreement may only be amended by mutual written consent of both the KCBOE and the Authorized Representative and the Authorized Representative shall not assign its respective rights or obligations under this agreement without the KCBOE's prior written consent. The rights and obligations of each party under this agreement shall inure to the benefit of and shall be binding upon each party and any respective successors and assigns.

Section 8. Choice of Law and Forum.

All questions as to the execution, validity, interpretation, and performance of this agreement shall be governed by the laws of the Commonwealth of Kentucky. The selected forum to hear any causes of action arising from this agreement, or any actions thereunder, is the Kenton Circuit Court, Covington, Kentucky.

Section 9. Waiver.

The failure by one party to require performance of any provision shall not affect that party's right to require performance at any time thereafter, nor shall a waiver of any breach or default of this agreement constitute a waiver of any subsequent breach or default or a waiver of the provision itself. No modification, amendment, waiver or release of any provision of this agreement or of any right, obligation, claim or cause of action arising from this agreement shall be valid or binding for any purpose unless in writing and duly executed by the party against whom they are asserted.

Section 10. Severability.

Any provision of this agreement that is declared invalid by a court of competent jurisdiction or by operation of law, shall not affect the validity or enforceability of any other provision of this agreement.

Section 11. Authority to Enter the Agreement.

The KCBOE and the Authorized Representative represent and warrant, by the signatures of their duly appointed representatives, that they are legally entitled to enter into this agreement.

Section 12. Data Custodians.

The individuals who are the designated data custodians for the Authorized Representative with respect to this confidential data release and use agreement are listed in Exhibit E with their contact information.

Section 13. Term and Termination.

The term of this agreement shall be *the same as the term of any Master Agreement between the KCBOE and the Authorized Representative / for (length of time or insert a date here)* unless terminated earlier by either party upon thirty (30) days written notice. Either party may terminate this agreement with thirty (30) days written notice.

Section 14. Effective Date of This Agreement.

This agreement will become effective once the KCBOE and the Authorized Representative have both signed.

APPROVED:

Name
Title
Kenton County Board of Education

Date

Authorized Representative's Authorized Agent / Date
Agent's Title _____
Agent's Name (Typed) _____
Authorized Representative Entity's Name

Memorandum of Understanding (MOU)

Description of Exhibits

To authorize the release and use of confidential data under the FERPA Audit and Evaluation Exception

Exhibits referenced in the Memorandum of Understanding must be completed and incorporated into the final MOU. Exhibits include:

- Exhibit A - Specifics of data being requested
 - Section I - the initial data request that describes the audit/evaluation and data being requested
 - Section II- describes the need for Personally Identifiable Information (PII)
 - Section III - required if requesting Free and Reduced Lunch information
- Exhibit B – Authorized Representative Confidentiality Agreements (one for each data custodian)
- Exhibit C – Authorized Representative data security policy
- Exhibit D - Data destruction plan at completion of audit/evaluation
- Exhibit E - Identification of data custodians

Please refer to The U.S. Department of Education, Family Policy Compliance Office's [Guidance for Reasonable Methods and Written Agreements](#) for additional information on requirements for data sharing under the Family Educational Rights and Privacy Act (FERPA).

Exhibit A:

Contact Information

Research Entity Legal Name _____

Primary Data Custodian Name _____, Title _____

Phone _____

Email _____

Secondary Data Custodian Name _____, Title _____

Phone _____

Email _____

Section I- to be completed by all requestors:

Purpose, Scope and Duration *Use of data received under this MOU is limited to purpose and scope defined.*

**Completely describe
the purpose and
scope of the
audit/evaluation.**

Click here to enter text.

**Describe how the
results will be used.**

Click here to enter text.

Duration of Audit/Evaluation

Start Date: _____

End Date: _____

Data Being Requested

**Provide specific data
elements needed to
complete audit/
evaluation**

Click here to enter text.

Years included in Audit Evaluation:

☐ 2014-15

☐ 2013-14

☐ 2012-13

☐ 2011-12

☐ 2010-11

☐ 2009-10

☐ 2008-09

☐ Other: _____

Level of detail/aggregation: ☐ Student/Individual ☐ School ☐ District ☐ State

If requesting Personally Identifiable Information (PII), check Student/Individual box. For aggregate level select School, District, or State.

Please complete Section II if requesting PII detail.

Section II- Complete if Personally Identifiable Information (PII) is being requested:

**Justify your request
for
student/individual
level data**

*Explain why
audit/evaluation could not
be completed by using
aggregate-level data
without PII*

Click here to enter text.

Special requirements for requests for Personally Identifiable Information (PII)

- *Student-Level/Individual detail from education records can only be used to meet the purpose or purposes of the audit/evaluation as stated in this MOU for duration as defined.*
- *Requestor agrees to conduct the audit/evaluation in a manner that does not permit the personal identification of parents, students, individuals by anyone other than designated data custodians.*
- *Authorized Representative agrees to destroy all PII from education records and confidential data from other records.*
- *If Free & Reduced Lunch Status is needed on PII data, complete Section III.*

III- Complete if free or reduced -price lunch eligibility data is required for PII records.

Prototype Agreement:

Disclosure of Free and Reduced Price Information

A. Purpose and Scope

Kenton County Board of Education, KCBOE, and _____ acknowledge and agree that children's free and reduced price meal and free milk eligibility information obtained under provisions of Richard B. Russell National School Lunch Act (42 USC 1751 et. seq.) (NSLA) or Child Nutrition Act of 1966 (42 USC 1771 et. seq.) (CNA) and the regulations implementing these Acts is confidential information. This Agreement is intended to ensure that any information disclosed by the KCBOE to the _____ about children eligible for free and reduced price meals or free milk will be used only for purposes specified in this Agreement and that the KCBOE and _____ recognize that there are penalties for unauthorized disclosures of this eligibility information.

B. Authority

Section 9(b)(6)(A) of the NSLA (42 USC 1758(b)(6)(A)) authorizes the limited disclosure of children's free and reduced price meal or free milk eligibility information to specific programs or individuals, without prior parent/guardian consent. Except that, the parent/guardian must be provided the opportunity to decline to share eligibility information prior to the disclosure for identifying children eligible for benefits under or enrolling children in the State Medicaid Program and the State children's health insurance program. Additionally, the statute specifies that for any disclosures not authorized by the statute, the consent of children's parents/guardians must be obtained prior to the disclosure.

The requesting agency certifies that it is currently authorized to administer the following program(s) and that information requested will only be used by the program(s) indicated.

Check all that Apply	Program	Information Authorized
☐	<i>Medicaid or the State children's health insurance program (SCHIP), administered by a State or local agency authorized under titles XIX or XXI of the Social Security Act.</i> Specify Program: _____	All eligibility information unless parents elect not to have information disclosed.
☐	<i>State health program other than Medicaid/SCHIP, administered by a State agency or local education agency.</i> Specify Program: _____	Eligibility status only; consent not required
☐	<i>Federal health program other than Medicaid/SCHIP</i> Specify Program: _____	No eligibility information unless parental consent is obtained.
☐	<i>Local health program</i> Specify Program: _____	No eligibility information unless parental consent is obtained.
☐	<i>Child Nutrition Program under the National School Lunch Act or Child Nutrition Act</i> Specify Program: _____	All eligibility information; consent not required.
☐	<i>Federal education program</i> Specify Program: _____	Eligibility status only; consent not required.
☐	<i>State education program administered by a State agency or local education agency</i> Specify Program: _____	Eligibility status only; consent not required.

Note: Section 9(b)(6)(A) specifies that certain programs may receive children's eligibility status only, without parental consent. Parental consent must be obtained to disclose any additional eligibility information. Section 9(b)(6)(D)(ii) specifies that for State Medicaid or SCHIP, parents must be notified and given opportunity to elect not to have information disclosed. Social security numbers may only be disclosed if households are given notice of the disclosure and the uses to be made of their social security numbers as required by Sec. 7 of the Privacy Act.

C. Responsibilities

Kenton County Board of Education will:

When required, secure parents/guardians consent prior to any disclosure not authorized by the National School Lunch Act or any regulations under that Act, unless prior consent is secured by the receiving agency and made available to the determining agency;

For State Medicaid and SCHIP, notify parents/guardians of potential disclosures and provide opportunity for parents/guardians to elect not to have information disclosed;

Disclose eligibility information only to persons directly connected to the administration or enforcement of programs authorized access under the National School Lunch Act or regulations under the Act or to programs or services for which parents/guardians gave consent.

_____ will:

Ensure that only persons designated as data custodians and listed on Exhibit E who are directly connected with the administration or enforcement of the _____ (program) and whose job responsibilities require use of the eligibility information will have access to children's eligibility information.

Use children's free and reduced price eligibility information for the following specific purpose(s):

Describe:

Click here to enter text.

Inform all persons that have access to children's free and reduced price meal eligibility information that the information is confidential, that children's eligibility information must only be used for purposes specified above, and the penalties for unauthorized disclosures.

Protect the confidentiality of children's free and reduced price meal or free milk eligibility information as follows:

Click here to enter text.

Specifically describe how the information will be protected from unauthorized uses and further disclosures.

Click here to enter text.

D. Effective Dates

This agreement shall be effective during the dates of duration for the audit/evaluation.

E. Penalties

Any person who publishes, divulges, discloses, or makes known in any manner, or to any extent not authorized by Federal law (Section 9(b)(6)(C) of the National School Lunch Act; 42 USC 1758(b)(6)(C)) or regulation, any information about a child's eligibility for free and reduced price meals or free milk shall be fined not more than a \$1,000 or imprisonment of not more than 1 year or both.

F. Signatures

The parties acknowledge that children's free and reduced price meal and free milk eligibility information may be used only for the specific purposes stated above; that unauthorized use of free and reduced price meal and free milk information or further disclosure to other persons or programs is prohibited and a violation of Federal law which may result in civil and criminal penalties.

Requesting Agency/Program Administrator

Typed or Printed Name: _____

Title: _____ Phone: _____

Signature: _____ Date: _____

Determining Agency Administrator

Printed Name: _____

Title: _____ Phone: _____

Signature: _____ Date: _____

**Any attachments will become part of this agreement.*

**Exhibit B: KENTON COUNTY BOARD OF EDUCATION
CONTRACTOR'S EMPLOYEE OR CONTRACTOR NONDISCLOSURE STATEMENT**

Contractor _____

Contractor's employee or contractor name _____ Title: _____

Address _____ Phone _____

I understand that the performance of my duties as an employee or contractor, of a contractor for the Kenton County Board of Education (KCBOE), may involve a need to access and review confidential information (information designated as confidential by FERPA, NSLA, CNA, KRS 61.931(6), or other federal or state law); and, that I am required to maintain the confidentiality of this information and prevent any re-disclosure prohibited under the law as stated below. By signing this document I agree to the following:

- I will not permit access to confidential information to persons not authorized by the KCBOE and its contractor.
- I will maintain the confidentiality of the data or information.
- I will not access data of persons related or known to me for personal reasons.
- I will not reveal any individually identifiable information furnished, acquired, retrieved, or assembled by me or others for any purpose other than statistical purposes specified in the KCBOE survey, project, or proposed research.
- I will report, immediately and within twenty-four (24) hours, any known reasonably believed instances of missing data, data that has been inappropriately shared, or data taken off site
 - to my immediate supervisor, Associate Commissioner, and
 - to the Division of Human Resources if I am a KCBOE employee or
 - to the KCBOE Office for whom I perform work under the contract if I am a KCBOE contractor or an employee of a KCBOE contractor
- I understand that procedures must be in place for monitoring and protecting confidential information.
- I understand and acknowledge that FERPA-protected information obtained under provisions of Family Educational Rights and Privacy Act of 1974 (FERPA) as a KCBOE contractor's employee or contractor of KCBOE is confidential information.
- I understand that FERPA protects information in students' education records that are maintained by an educational agency or institution or by a party acting for the agency or institution, and includes, but is not limited to the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- I understand that any unauthorized disclosure of confidential information is illegal as provided in FERPA and in the implementing of federal regulations found in 34 CFR, Part 99. The penalty for unlawful disclosure is a fine of not more than \$250,000 (under 18 U.S.C. 3571) or imprisonment for not more than five years (under 18 U.S.C. 3559), or both.
- I understand and acknowledge that children's free and reduced price meal and free milk eligibility information or information from the family's application for eligibility, obtained under provisions

of the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, is confidential information.

- I understand that any unauthorized disclosure of confidential free and reduced price lunch information or information from an application for this benefit is illegal as provided in the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq)(NSLA) or Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.)(CNA) and the regulations implementing these Acts, specifically 7 C.F.R 245.6. The penalty for unlawful disclosure is a fine of not more than \$1,000.00 (under 7 C.F.R. 245.6) or imprisonment for up to one year (under 7 C.F.R. 245.6), or both.
- I understand that KRS 61.931 also defines "personal information" to include:
 - an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;(b) A Social Security number;
 - A taxpayer identification number that incorporates a Social Security number;
 - A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - A passport number or other identification number issued by the United States government; or
 - Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.
- I understand that other federal and state privacy laws protect confidential data not otherwise detailed above and I acknowledge my duty to maintain confidentiality of that data as well.
- I understand that any personal characteristics that could make the person's identity traceable, including membership in a group such as ethnicity or program area, are protected.
- In addition, I understand that any data sets or output reports that I may generate using confidential data are to be protected. I will not distribute to any unauthorized person any data sets or reports that I have access to or may generate using confidential data. I understand that I am responsible for any computer transactions performed as a result of access authorized by use of sign on/password(s).

Contractor's employee or contractor signature

Date

Contractor's authorized agent signature

Date

Contractor's authorized agent name (typed)

Exhibit C:

Please describe the measures you take to ensure the protection of PII released to you. If you have a policy, please attach or copy/paste here as Exhibit C.

Click here to enter text.

Exhibit D:

Please use the space provided to describe the methods used to destroy all confidential data at the completion of your work. Please specify the date of destruction. If you have a policy that describes it can be attached as Exhibit D.

Click here to enter text.

Exhibit E: In alphabetical order by last name, provide information for those persons designated as data custodians. This should include anyone with access to confidential data. A designated primary and secondary data custodian are required and a minimum of four is requested. Attach if more space is needed. A signed nondisclosure agreement labeled as Exhibit B is required for each data custodian.

Primary Data Custodian

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Secondary Data Custodian

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

All Other Data Custodians

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Last Name, First Name: _____
Phone: _____
Email: _____
Employer: _____

Appendix D

Sample Security Breach Notification Letter

Date

Dear Recipient Name:

We are contacting you because we have learned of a serious data security incident that occurred on *(specific or approximate date)* OR between *(date, year and date, year)* that involved some of your personal information.

The breach involved *(provide a brief general description of the breach and include how many records or people it may have affected)*. The information breached contained *(customer names, mailing addresses, credit card numbers, and/or Social Security numbers, etc.)*. Other information *(bank account PIN, security codes, etc.)* was not released.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information. We have advised the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred, however, we have not notified them about the presence of your specific information in the data breach.*

*(Optional paragraph if offering credit protection service.**)*

To protect you we have retained *(name of identity theft company)*, a specialist in identity theft protection, to provide you with ____year(s) of *(description of services)* services, free of charge. You can enroll in the program by following the directions below. **Please keep this letter; you will need the personal access code it contains in order to register for services.**

As a first preventive step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338) or online at <https://www.ftccomplaintassistant.gov/>

As a second step, you also may want to contact the three U.S. credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

You also may want to consider placing a security freeze on your credit files. A freeze prevents an authorized person from using your personal identifying information to open new accounts or borrow money in your name.

You will need to contact the three U.S. credit reporting agencies to place the security freeze. The fee is \$10 for each credit reporting agency. The agencies may waive the fee if you can prove that identity theft has occurred. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To obtain a security freeze, contact the following

agencies: Equifax: 1-888-298-0045; web:

www.freeze.equifax.com

TransUnion: 1-800-680-7289; web: www.transunion.com (search for security freeze) Experian: 1-888-EXPERIAN; www.experian.com/freeze.com

For more information, see the website for the Oregon Department of Consumer and Business Services at www.dfcs.oregon.gov/id_theft.html and click on "How to Obtain a Security Freeze."

If you have further questions or concerns, you may contact us at this special telephone number: 000- 000-0000. You can also check our website at www.ourwebsite.org for updated information.

Sincerely,

* Reporting to credit agencies is required only for breaches affecting 1,000 or more persons.

** Not required under ORS 646A.600-646A.628.

Appendix E

FAC-001
Effective Date: 01/01/2015

Determined Breach Notification Form

Section 1

Complete and submit within 72 hours of determination or notification.

Determined

- ☐ Finance Cabinet Secretary
- ☐ Auditor of Public Accounts (APA)
- ☐ Kentucky State Police (KSP)
- ☐ Attorney General (AG)
- ☐ Commissioner of Department of Library and Archives, if breach determined
- ☐ Chief Information Officer of Commonwealth Office of Technology
- ☐ If Department of Local Government under KRS 61.931(1)(b) or (c) also contact:
 - ☐ Commissioner of Department of Local Government
 - ☐ If Public School District listed in KRS 61.931(1)(d) also contact:
 - ☐ Commissioner of Kentucky Department of Education
 - ☐ If Educational entity listed under KRS 61.931(1)(e) also contact:
 - ☐ President of Council on Postsecondary Education

Agency Name: _____

Agency Contact: _____

Agency Contact Email: _____

Agency Contact Phone Number: _____

Date of Notification to Agencies: _____

Time of Notification: _____

Date Breach Determined: _____

Section 2

Complete this portion after the conclusion of the investigation regarding whether the Security Breach has resulted in or is likely to result in the misuse of personal information. Provide notice to agencies within 48 hours of completing investigation.

Personal Information Breached: ☐ Yes ☐ No

If Yes, Explain: _____

Total Number of Individuals Impacted: _____

Date Individuals Notified: _____

Type of Notices Sent Out (select all that apply and provide explanations):

☐ Web Posting:

☐ Email:

☐ Local or Regional Media:

☐ Telephone:

☐ Letter:

☐ Other:

Did You Notify Consumer Credit Reporting Agencies? ☐ Yes ☐ No

If Yes, Date: _____

Any Other Breach Compliance Requirements Apply such as Federal? ☐ Yes ☐ No

If Yes, Explain: _____

Third Party Breach: ☐ Yes ☐ No

If Yes, Third Party Name: _____

If Third Party Involved, When Did They Notify the Agency: _____

If a delay then please attach the delay notification record along with supporting documentation. Was there a delay due to:

- ☐ Law enforcement investigation. Reference to KRS 61.933 (3)(a)
- ☐ An agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established and will delay the breach determination. Delay will need to be approved in writing from the Office of the Attorney General. Reference to KRS 61.933 (3)(b)

□

Section 3

Complete and submit at the conclusion of the investigation and any notice and resolution process.

Actions Taken to Resolve Breach:

Actions Taken to Prevent Additional Security Breaches in Future, if any:

A General Description of what Actions are Taken as a Matter of Course to Protect Personal Data from Security Breaches:

Any Quantifiable Financial Impact to the Agency Reporting the Security Breach:

Reference:

KRS 61.931 to 61.934 - <http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575>

KRS 42.726 - <http://www.lrc.ky.gov/Statutes/statute.aspx?id=43580>

Appendix F

FAC-F002
Effective Date: 01/01/2015

Delay Notification Record

All documentation in reference to the delay should be attached to the notification record.

Agency Name: _____

3rd Party Name, if applicable: _____

Agencies are to use this form to record information:

- ☐ If a law enforcement investigation has delayed the notification process for a breach determination.
Reference to KRS 61.933 (3)(a)

Date Law Enforcement Notified Agency: _____

Law Enforcement Agency: _____

- ☐ If an agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established and will delay the breach determination. Delay will need to be approved in writing from the Office of the Attorney General.
Reference to KRS 61.933 (3)(b)

Date Submitted to Office of Attorney General: _____

Date Approved by the Office of Attorney General: _____

The agency will submit form FAC-001 as required by KRS 61.933 if law enforcement has not contacted it within seventy-two (72) hours of a determined breach.

Data Security and Breach Notification Best Practice Guide

Kentucky Department of Education (KDE)

V2.2 September 2015



Kentucky Department of Education
300 Sower Blvd.
Frankfort, KY 40601
(502) 564-2020

Special Note:

This guide is a living document and subject to change. Districts will be alerted to major changes, which could occur at any time. Otherwise, updates to this document will be available each August.

Version Control

Version	Date	Author	Change Description
2.0	4/22/2015	R. Hackworth	Adapted from 2006 HB 341 Data Security Study
2.1	4/24/2015	R. Hackworth	Added "version control." Added "Resources" section with webcast archive & COT document links at end of document. Changed links for HBs 5 and 232 docs to highlighted versions used during noted webcast.
2.2	7/20/2015	R. Hackworth	Added data breach notification distribution list
2.3	1/6/2023	R. Hackworth	Links updated

Overview

In 2006, the Kentucky General Assembly passed House Bill 341, which mandated the Kentucky Department of Education (KDE) to conduct a study of the requirements for data security and a notification process when a data breach occurs.

The intent of the study requested by the legislature was to provide some general guidelines and recommendations to KDE and school districts related to some basic measures that can be considered to protect and prevent the access to restricted personal information by any person that does not have the proper access rights, authority or the “need to know” (a.k.a., an unauthorized person) and to provide some considerations and protocols in regards to notifying any affected individual should this type of information be made available in paper or electronic form to any unauthorized person.

Since that legislation, the threat and occurrence of data breaches has only increased. The House Bill 341 data security study has remained an effective cornerstone of guidance, and new legislation has added clarity, definition, and direction. But, as technology and how we use it in the schools has changed, so must that original guidance. This document, while incorporating the still-relevant guidance of the HB 341 study, will supersede it.

One thing that has not changed, however, is KDE’s role. Since the Kentucky Educational Technology System (KETS) began in the early 1990s, districts have possessed the authority and responsibility to ensure their own security, whether it be part of the network, data system or even paper documents on a desk. KIDS does not have the staff or desire to begin inspecting, approving, disapproving, or monitoring each district’s reasons or detailed actions in implementing or not implementing suggested best practices. However KIDS staff will be a resource for any questions or suggestions for additions/edits a district has throughout the years in regards to the reg and the best practice guideline. Any district wanting anything beyond that (e.g., an annual inspection, confirmation, thumbs up of their data security, a professional opinion on which data security recommendations should or shouldn’t be implemented within their district, etc) will be pointed to resources outside of KDE (see “Remediation, below) that can best help them with the types of task/services.

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, et seq.) went into effect. This legislation is more commonly known as “House Bill 5.” This Act concerns the protection of personal information and applies to every state agency, including KDE, every public school district, and every vendor with which we have contracts. While this document incorporates best practice that we are all encouraged to follow, it also incorporates the “have to” actions from KRS 61.931, et seq. (HB 5).

In addition to the legal requirements, this document makes recommendations based on research and experience (best practice). However, there is no guarantee that implementing all of the recommendations will remove 100% of the risk of a data breach. Each district is encouraged to implement the recommendations that it believes are the most helpful given its perception of risk and fiscal capabilities.

This next section provides a summary of the requirements, prior to and following a suspected or confirmed data breach, from KRS 61.931, et seq. (HB 5). The remaining sections either provide more detail for these requirements or provide recommendations.

Data Breach Act “Have to” Section

Please be advised that this is a summary. A thorough understanding of KRS 61.931, et seq. (HB 5), along with its [included definitions](#), will be very helpful and is recommended.

Immediately

- [Procedures and practices to safeguard against security breaches](#) must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.
- For any contracts involving personal information that are entered into or amended after January 1st, 2015, specific language requiring protection of the data must be included.

Within 72 Hours of Suspected or Confirmed Breach

0. [Send notification](#), via the [FAC-001 form](#), to the CommonwealthBreachNotification@ky.gov distribution list. It will be forwarded to the following agencies as required by KRS 61.933:
 - a. Attorney General’s Office
 - b. Auditor of Public Accounts
 - c. Finance and Administration Cabinet
 - d. Kentucky State Police
 - e. Kentucky Department of Library and Archives
 - f. Commonwealth Office of Technology

Please also Cc the Department of Education’s Chief Information Security officer when sending the FAC-001 form. This will ensure the Department of Education also receives the form, as required. If there is an ongoing investigation involving law enforcement which causes a delay of information being disclosed, use the [FAC-002 form](#) to provide the notification required by KRS 61.933.

1. Begin conducting a “reasonable and prompt” investigation to determine “whether the security breach has resulted in or is likely to result in the misuse of personal information.”

Within 48 Hours of Completion of the Investigation

Notify the above staff contacts if the investigation finds that the misuse of personal information has occurred or is likely to occur. The length of the investigation is not set, and will vary with each instance.

Within 35 Days of Suspected or Confirmed Breach

- Notify all individuals impacted by the breach [in a manner required by KRS 61.931](#), et seq. including information required by the Act. If breach impacts more than 1,000 individuals, nationwide consumer reporting agencies must also be notified. KDE recommends notifying affected individuals as soon as possible and not waiting until the 35th day.
- If the investigation determines that misuse of personal information has not occurred or is not likely to occur, notification of the impacted individuals is not required, but records of the decision and evidence must be kept. Notification of the agency contacts, above, is still required noting that misuse of personal information has NOT occurred.

Data at Risk

Unlike the private sector or most other parts of government, a very high percentage of the data elements collected and used in P-12 schools are not considered confidential and are usually made directly accessible to any public citizen either instantly through a variety of electronic means (e.g., Web sites at schools, district offices, the Kentucky Department of Education and the U.S. Education Department) or very quickly in response to open records requests that must be provided in paper or e-mail form. Also, most of the data collected at the state and federal level are in summative form and therefore do not contain individually identifiable or confidential data.

This means that access to the majority of the truly private P-12 data is controlled by district staff, who control the permissions to these areas, systems and services. Most reside physically (e.g., on paper within cabinets, on electronic files inside a fileserver or workstation) within the district though as cloud services increase in popularity, more and more sensitive or confidential data exists outside of the district boundaries, though still under district control.

There is a category of P-12 data that is considered very personal and restricted and is becoming more and more sought after by identity thieves – the social security numbers of students. Even more than the SSNs of adults, the SSNs of children are valuable because children usually do not engage in behavior that might result in a credit check. This means the identity thief can use or sell these SSNs for years before ever having any attention drawn to them.

Most of the time, if there is an exposure of this type of restricted personal data, such as a student's medical records or a teacher's SSN, it happens accidentally (e.g., confidential personal data is printed to an unintended printer in a building, e-mailed to the wrong person or group or placed on an incorrect Web site). Also, the number of people who accidentally see confidential data that they should not be viewing tends to be limited to a small group; most of which disregard or destroy what they have seen because they do not realize that it is restricted personal data.

Yet, there are times where there are intentional attempts (e.g., a laptop or cabinet drawer containing paper files is stolen from a school, someone is just curious about a fellow employee's personal information) to access restricted personal information by unauthorized people who do not have a true need to know.

Whether the exposure happens accidentally or intentionally, the same prevention steps and notification protocols should be considered for all restricted personal data, no matter the media form (i.e. paper or electronic) that that data is stored on. In fact, most organizations already have well-established procedures for confidential personal data that is on paper form, which also can be considered for the same type of restricted data that is available and stored in electronic form.

The bottom line is that pre-emptive measures to protect and prevent the access by unauthorized people should be taken by each P-12 organization that controls and manages restricted personal information. However, if an individual's restricted personal information possibly has been seen by an unauthorized person, no matter how small or large the level of knowledgeable exposure, there is an obligation to let the affected individual know as quickly as possible that restricted personal data may have been compromised and disclosed to unauthorized people. If possible, that affected person should be informed what specific restricted data has been exposed, how long it has been exposed, who it has been exposed to and how the exposure occurred. This must be done no matter how embarrassing this announcement may be to the organization that is responsible for that restricted data becoming accidentally exposed or a victim of its data system being successfully accessed through criminal activity.

The Three Major Areas of Consideration of Personal Data Security Management

This study was originally conducted by Kentucky Department of Education with research derived from information received from Gartner, NOREX and various state departments around the nation. Gartner provides independent research and analysis to private and public organizations over a wide range of technology subjects. Norex is a consortium of public and private companies that share their policies, lessons learned and processes with the other association members to consider for use in their organizations. Finally, a large number of states already have established legislation and policies that we can learn from without trying to reinvent the wheel. Therefore, we considered and consolidated information gathered from all these sources into a concise report that focuses on three major areas:

- Protection and Prevention
- Preparation for Notification
- Notification

1. Protection and Prevention

Organizations must implement an effective incident response program that includes pre-incident preparation; detection and analysis; containment; mitigation and recovery; and post-incident activities. Proper preparation (e.g. staff education, a healthy data diet) and awareness of legal and ethical issues are crucial.

The level of acceptable risk should be articulated, and security procedures should be balanced with available funding for information and data security, access and safeguards. In the event that more secure measures are needed, these measures should be identified for implementation and allocation of resources.

The cornerstone of improving data security is basic awareness among all staff. To promote awareness of data security best practices, the Kentucky Department of Education's Data Governance team has produced a series of three short videos focused on protecting personal information. While everyone is welcome to view and use these videos, please keep in mind they were developed specifically for KDE use and may not perfectly match every district's needs.

1. [What is PII?](#)
2. [Data Access and Sharing](#)
3. [Was that a Data Breach?](#)

Additional information about data privacy and security from KDE, the U.S. Education Department, PTAC, and others can be found [on the KDE website here](#).

An organization should protect the confidentiality of personal information whether it pertains to customers, employees, parents or students. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices:

- **Do the Basics** – Keep and promote awareness of basic, but extremely important, security and privacy policies related to
 - using strong passwords or passphrases and changing them often,
 - keeping a password, PIN or passcode on all devices, including laptops, tablets and smartphones,
 - whenever staff depart:
 - changing security entry codes/locks for buildings/rooms containing sensitive information
 - removing old or unused user accounts from all systems
 - ongoing employee training and communications.

This should help reduce the number of incidences or magnitude of exposure of very sensitive data, while at the same time increasing the speed of proper notification and protocol should this exposure occur.
- **Keep Accurate and Updated Data Inventories** - Inventory all of your records systems (e.g., electronic and paper storage media) to identify those containing any type of personal information. This will help you decide what level of protection is necessary for each system, and what priority it has in your educational processes.
- **Have a Healthy Data Diet** - Collect the minimum amount of personal information necessary to accomplish your educational purposes, and retain it for the minimum time necessary.
- **Classify Data** - Classify information in each paper and electronic records system according to sensitivity and the level of risk if that information was accidentally or intentionally accessed by anyone without a need to know. A simple rule of thumb that can be used to quickly identify the data that has the highest levels of sensitivity and confidentiality in an organization would be to reflect on whether the data could be posted on a public website or viewed by anyone making an open records request.
- **Intruder Detection** - Use appropriate physical and technological safeguards, such as video surveillance or alarms on buildings or rooms, to protect personal information, particularly higher-risk information, in paper as well as electronic records.
- **Vendor Management** - Require service providers and educational partners who handle personal information on behalf of your organization to follow your security policies and procedures as well as state and federal laws (such as HBs 5, 232 and COPPA). KDE has developed the following verbiage, which, if used by any district, must be customized, for inclusion in contracts:
 - [DRAFT RFP Attachment - Data Security and Breach Protocols](#)
 - [DRAFT RFP Attachment - FERPA and Affidavit of Non-Disclosure](#)
- **Encryption** - Wherever it makes sense, such as devices used to host or access high-risk information, use data encryption in combination with host protection and access control. Pay particular attention to protecting higher-risk personal information on laptops and other portable computers and mobile storage devices (e.g. smartphones, CDs, thumb drives).
- **Records Retention** - Dispose of records and equipment containing personal information in a secure manner.
- **Document Your Security** - Have a security plan and review it at least annually or whenever there is a material change in educational practices, delivery mechanism, where the data is stored and how it accessed that may reasonably implicate the security of sensitive personal information.

2. Preparation for Notification of Affected Individuals

- **Leading the Charge** - Designate an individual, such as the CIO, as responsible for coordinating your internal investigation and notification procedures for the paper and electronic restricted personal data for which you are responsible.
- **Data Breach Policy** - Outline investigation and notification procedures to be followed if the school district determines or is notified of a security breach of personal information, including notice to the individual whose personal information was breached or to the parents of an individual under eighteen (18) years of age whose personal information was breached, documentation of the event, and a process for the parents or individual to request a debriefing session regarding the breach.
 - Consider suggestions from law enforcement with expertise in investigating crimes that use technology (e.g., hackers breaking into file servers) and nontechnology (e.g., burglars breaking into buildings) means for intentionally accessing unauthorized restricted personal information for inclusion in your incident response plan.
 - Consider suggestions from your legal staff during planning. They have the greatest knowledge and expertise on what data does and does not meet the requirements of the open records law. This means they can be very valuable in helping you identify the most restricted personal data in your organization. They also can help you craft the wording for your written or verbal notifications that must be provided when an exposure occurs. They can point you to the most appropriate law enforcement official to contact should criminal activity be the reason the data became exposed or if the exposed data is possibly being used for criminal purposes (e.g., identity theft, fraud).
 - Adopt written procedures, in accordance with data breach legislation, for notification of individuals whose unencrypted notice-triggering personal information have been, or are reasonably believed to have been, acquired by an unauthorized person. Notification can take many forms that include a face-to-face meeting, a phone call, posting on a Web site or sending a paper notice to each affected person's home. The number of people that need to be contacted will usually influence the form of notification that is chosen and how quickly each person can be reasonably notified
- **Training** - Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your data breach policy/incident response plan. It is also important to make sure everyone is familiar with key terms such as "confidential," "PII," and what, exactly, defines a breach.
- **Remediation** - In addition to the notification of state agencies, each district, just like KDE, is expected to be able to remediate the issue which allowed the breach to occur. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information. Multiple options are available.
 - Many IT auditing firms can offer forensic/recovery/notification services in addition to pre-incident vulnerability auditing for potential weaknesses. Districts are encouraged to inquire with their existing auditors for these services.
 - Check the transparency.ky.gov for the current state contract holder for security services, including vulnerability assessment and forensic investigations.
 - The Commonwealth Office of Technology also offers [various security services](#) available to all state agencies and public-school districts.

- The United States Cybersecurity & Infrastructure Security Agency (CISA) offers a free or facilitated [Cyber Resilience Review](#) “to evaluate an organization’s operational resilience and cybersecurity practices.”
- **Whom to Call** - Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities. Keep important numbers handy.
- **Documentation** – As soon as a potential breach occurs, it is important to document the issues found and response actions taken on an incident.

Reflect and Review - Review your incident response plan at least annually or whenever there is a significant change in your educational practices or how the data can be accessed electronically or in paper form. It is also important, after a security incident, to reflect on what worked well, and perhaps not so well, and then make changes to your process.

3. Notification

As of January 1st, 2015, Kentucky began to require notification of suspected or confirmed data breaches. With the passage of KRS 61.931, ET SEQ. (HB 5), Kentucky public agencies and public schools are required to notify both the individual victims of a breach and various state officials.

House Bill 5 addresses the safety and security of personal information held by public agencies and requires public agencies and nonaffiliated third parties to implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.

- [House Bill 5 document with Highlighting](#)

House Bill 232 has two sections. Section 1 requires consumer notification when a private party data breach reveals personally identifiable information. Section 2 requires cloud computing service providers contracting with educational institutions to maintain security of student data.

- [House Bill 232 document with Highlighting](#)

In addition to this legislation, districts are encouraged to review the following links, which provide helpful information regarding contractual arrangements with cloud service providers:

- [Gartner insights: 3 important questions to ask your potential cloud provider](#)
- [Infoworld – Gartner: Seven cloud-computing security risks](#)
- [Gartner: Cloud Exit Strategies](#)

Required Data Breach Notification Forms

As noted in House Bill 5, the following forms, developed by the Commonwealth Office of Technology, are to be used to notify all required agencies in the event of a breach or a suspected breach of data.

- [Data Breach Notification Form FAC-001](#)

- [Delay of Notification Form FAC-002](#)

The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm. To ensure giving timely and helpful notice to affected individuals, the following practices are required by Kentucky's data breach legislation:

Contents of Notification

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;
2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;
3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and
4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
 - The major consumer credit reporting agencies;
 - The Federal Trade Commission; and
 - The Office of the Kentucky Attorney General.

Timing of Notification

- According to the data breach legislation passed in 2014 and that went into effect January 1st, 2015, each agency and public school has a total of 35 days from the time of their formal notification of agency contacts to "notify all individuals impacted by the security breach." Details about the type of notification, which can impact the cost, can be found in the legislation.

Contact Law Enforcement

- If your assessment leads you to reasonably believe that an unauthorized person through criminal activity versus by accident acquired restricted personal information, then a notification to law enforcement, such that would begin an investigation, should occur as well. This is over and above the notification required by KRS 61.931, ET SEQ. (HB 5).

Cost Considerations When Implementing Personal Data Security

Please note that none of the other states and private organizations identify the total cost to fully implement all three major areas mentioned above. But if cost was mentioned, it was a cap amount that had to be spent in notifying people of a potential compromise of their personal data. A cap is something that should be considered by the department and school districts.

KDE and every public school district will need to weigh the risk of a data security breach versus the cost to implement these recommendations. Some of the suggested items listed under Protection and Prevention can be very expensive to implement (e.g., encryption, intrusion detection systems), so some owners of data systems will implement these, and others will take their chances and will do the best they can with the methods they are now using. This will cause the costs to fully implement all the recommendations mentioned above to fluctuate greatly between all the different paper and electronic data systems in school districts and KDE. This makes it very difficult to estimate overall cost to implement statewide at this time. It is, however, fair to ask each organization to prepare for and implement these three major areas the best they can, while at the same time placing a cap on what must be spent toward actual notification.

Additional Resources

[April 23, 2015 HB5 Kentucky K-12 Data Breach Webcast Archive - Direct link](#)

[April 23, 2015 HB5 Kentucky K-12 Data Breach Webcast Archive - Short link](#)

Additional Commonwealth Office of Technology Resources

COT has the following enterprise policies in place that may assist meeting requirements for [KRS 61.931, et seq. \(HB 5\)](#) for "Reasonable security and breach investigation procedures and practices..." Districts are encouraged to review these documents and use them as examples, but customization will be required. These documents are written for COT and agencies in the Executive Cabinet of state government. Several of the processes within, such as contacting the Commonwealth Service Desk after an incident, will not be applicable for school districts.

- [CIO-090 - Information Security Incident Response Policy](#)
Identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs.
- [CIO-091 - Enterprise Information Security Program](#)
Aligns the Commonwealth's Enterprise Information Security Program with the security framework of the current National Institute of Security Standards (NIST) Special Publication 800-53.
- [CIO-092 - Media Protection Policy](#)
Ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction.