

SUBJECT: DISTRICT WELLNESS POLICY

The Lake Shore Central School District is committed to providing a school environment that enhances the learning and development of lifelong wellness practices.

The District's Wellness Committee is charged with the oversight of this policy and will report to the Board of Education.

Our primary goal of nutrition education is to influence students' eating behaviors, build nutrition knowledge and skills that help children make lifelong healthy eating and positive physical activity choices. To make a difference, Lake Shore Central School will provide nutrition education that is appropriate for students' ages; and provides opportunities for students to practice skills and have fun. Healthy eating and physical activities are essential for students to achieve their full academic and physical potential, mental growth, lifelong health and well-being.

To accomplish these goals the Board of Education:

Nutrition

- a) Acknowledges that the school food service program shall operate in accordance with the National School Lunch Act and the Child Nutrition Act of 1996 as amended and applicable laws and regulations of the state;
- b) Recognize that schools shall offer appealing, varied and nutritious food choices that are consistent with the federal government's recommended intakes within energy needs by adopting a balanced eating pattern, such as the USDA Food Guide;
- c) Provides students and staff with adequate space to eat meals in pleasant surroundings and shall have adequate time to eat and relax. Safe drinking water and convenient access to facilities for hand washing and oral hygiene shall be available;
- d) Provides appropriately scheduled meal periods. Lunch should be scheduled as near to the middle of the school day as possible and should not be scheduled during tutoring, club or organizational meetings;
- e) Recognizes that classroom teaching will include but is not limited to, the new food pyramid, a dietary guide and the F.I.T.T. principle;
- f) Recognizes that education, marketing and promotion links outside the classroom will include but is not limited to; news media, food service programs and the community education flyer;
- g) Recognizes that the fundraising activities will include but is not limited to; senior fruit sale and chicken bar-b-ques and these activities are encouraged to follow the District Wellness and Nutrition Standards.

(Continued)

SUBJECT: DISTRICT WELLNESS POLICY (Cont'd.)Physical Activity

- a) Recognizes that physical education requirements for graduation will include; two (2) full units of physical education, a 1/4 (one-quarter) credit per semester for 8 (eight) semesters;
- b) The District will identify and seek to progressively remedy any deficits in meeting state mandates for physical education as specified in the Commissioner of Education's regulations. When practical students will spend at least 50 (fifty) percent of physical education class time participating in moderate to vigorous physical activity;
- c) Acknowledges that adaptive physical education programming is provided for students with individual education plans;
- d) Recognizes that the ratio for physical education classes District wide is on average 1(one) to 24 (twenty four) students;
- e) Acknowledges that the physical education curriculum District wide is developed around the New York State Physical Education and Health Standards;
- f) Recognizes that physical activity outside of the required physical education classes include but are not limited to; interscholastic sports and various athletic intramurals;
- g) Encourages walking or biking to school and in fact recognizes the elementary programs that endorse a National Walk to School Week.

Other School-Based Activities

- a) Encourages community access to District facilities for physical activity including but not limited to the Fitness Center, Community Education and Community Pool;
- b) Encourages community involvement with the Community Fitness Run, Family Support Center and various wellness events.

The Superintendent/designee will ensure compliance with established District-wide nutrition and physical activity wellness policies.

The Superintendent/or designee will develop a summary report every three years on District-wide compliance with the District's established nutrition and physical activity wellness policies, based on input from schools within the District.

The Lake Shore Central School District Wellness Policy will be publicized through the School District Website at www.lakeshore.wnyric.org, the Eagle Express, menus and various other media.

(Continued)

2008

5661
3 of 3

Non-Instructional/Business
Operations

SUBJECT: DISTRICT WELLNESS POLICY (Cont'd.)

Child Nutrition and WIC Reauthorization Act of 2004, Public Law Section 108-265 Section 204

Richard B. Russell National School Lunch Act, 42 USC Section 1751 et seq.

Child Nutrition Act of 1966, 42 USC Section 1771 et seq.

7 CFR Section 210.10

http://www.access.gpo.gov/nara/cfr/waisidx_05/7cfr210_05.html

Adopted: 8/19/08

SUBJECT: RECORDS MANAGEMENT

A Records Management Officer shall be designated by the Superintendent, subject to the approval of the Board of Education. Such Records Management Officer shall coordinate the development of and oversee a program for the orderly and efficient management of records, including the legal disposition or destruction of obsolete records, and be given the authority and responsibility to work with other local officials at all levels in the development and maintenance of the records management program.

In addition, a Records Advisory Board may be created to assist in establishing and supporting the records management program. The District's legal counsel, the fiscal officer, and the Superintendent/designee may comprise the Advisory Board.

Retention and Disposition of Records

The Records Management Officer shall retain records for such a period and dispose of them in the manner described in Records Retention and Disposition Schedule ED-1, established pursuant to Part 185, Title VIII of the Official Compilation of Codes, Rules and Regulations of the State of New York and Article 57-A of the Arts and Cultural Affairs Law.

Special Approvals for Disposition of Records Not Included in Schedule/Records Damaged by Natural or Manmade Disasters

Records not listed on a records retention and disposition schedule shall not be disposed of without the approval of the Commissioner of Education.

Records that have been damaged by natural or manmade disaster and constitute a human health or safety risk also require the Commissioner's prior approval before disposition.

Replacing Original Records with Microforms or Electronic Images

Digital images of public records may be stored on electronic media, and such electronic records may replace paper originals or micrographic copies of these records. To ensure accessibility and intelligibility for the life of these records, the School District shall follow the procedures prescribed by the Commissioner of Education.

Retention and Preservation of Electronic Records

The District shall ensure that records retention requirements are incorporated into any plan and process for design, redesign, or substantial enhancement of an information system that stores electronic records.

SUBJECT: DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS

In accordance with the Federal Trade Commission's (FTC) "Disposal Rule," and in an effort to protect the privacy of consumer information, reduce the risk of fraud and identity theft, and guard against unauthorized access to or use of the information, the School District will take appropriate measures to properly dispose of sensitive information (i.e., personal identifiers) contained in or derived from consumer reports and records. Any employer who uses or possesses consumer information for a business purpose is subject to the Disposal Rule. According to the FTC, the standard for proper disposal of information derived from a consumer report is flexible, and allows the District to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

The term "*consumer report*" shall include information obtained from a consumer reporting company that is used - or expected to be used - in establishing a consumer's eligibility for employment or insurance, among other purposes. The term "*employment purposes*" when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

The FTC Disposal Rule defines "*consumer information*" as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data."

Information Covered by the Disposal Rule

The FTC has not included a rigid definition of the kinds of information that would be considered to identify particular individuals. In accordance with FTC guidance, there are a variety of personal identifiers beyond simply a person's name that would bring information within the scope of the Disposal Rule, including, but not limited to, a social security number, driver's license number, phone number, physical address, and email address. Depending upon the circumstances, data elements that are not inherently identifying can, in combination, identify particular individuals.

"Proper" Disposal

The FTC Disposal Rule defines "*dispose*," "*disposing*," or "*disposal*," as:

- a) "The discarding or abandonment of consumer information," or
- b) "The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored."

(Continued)

**SUBJECT: DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS
(Cont'd.)**

The District will utilize disposal practices that are reasonable and appropriate to prevent the unauthorized access to - or use of - information contained in or derived from consumer reports and records. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with District disposal include the following examples. These examples are not exclusive or exhaustive methods for complying with the Disposal Rule.

- a) Burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
- b) Destroying or erasing electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
- c) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with the Disposal Rule. In this context, due diligence could include:
 1. Reviewing an independent audit of the disposal company's operations and/or its compliance with the Disposal Rule;
 2. Obtaining information about the disposal company from several references or other reliable sources;
 3. Requiring that the disposal company be certified by a recognized trade association or similar third party;
 4. Reviewing and evaluating the disposal company's information security policies or procedures;
 5. Taking other appropriate measures to determine the competency and integrity of the potential disposal company; or
 6. Requiring that the disposal company have a certificate of registration from the New York Department of State issued on or after October 1, 2008.
- d) For persons (as defined in accordance with the Fair Credit Reporting Act) or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to the Disposal Rule, monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples a) and b) above.

(Continued)

**SUBJECT: DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS
(Cont'd.)**

Implementation of Practices and Procedures

The Board delegates to the Superintendent/designee(s) the authority and responsibility to review current practices regarding the disposal of consumer information; and to implement such further reasonable and appropriate procedures, including staff training as necessary, to ensure compliance with the FTC's Disposal Rule.

The Fair Credit Reporting Act, 15 USC Section 1681 et seq.
The Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159
Federal Trade Commission Disposal of Consumer Report Information and Records
16 CFR Part 682
General Business Law Article 39-G

Adopted: 8/19/08

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The School District values the protection of private information of individuals in accordance with applicable law and regulations. Further, the District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's *private information* in compliance with the Information Security Breach and Notification Act and Board policy.

- a) "*Private information*" shall mean ****personal information** in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:
1. Social security number;
 2. Driver's license number or non-driver identification card number; or
 3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"*Private information*" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

****"Personal information"** shall mean any information concerning a person which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

- b) "*Breach of the security of the system,*" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Examples of Determining Factors

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the District may consider the following factors, among others:

- a) Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- b) Indications that the information has been downloaded or copied; or

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

- c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Notification Requirements

- a) For any computerized data owned or licensed by the School District that includes private information, the District shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The District shall consult with the State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.
- b) For any computerized data maintained by the District that includes private information which the District does not own, the District shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

Methods of Notification

The required notice shall be directly provided to the affected persons by one of the following methods:

- a) Written notice;
- b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the District when notifying affected persons in electronic form. However, in no case shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;
- c) Telephone notification, provided that a log of each such notification is kept by the District when notifying affected persons by phone; or

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

- d) Substitute notice, if the District demonstrates to the State Attorney General that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice shall consist of **all** of the following:
1. Email notice when the District has an email address for the subject persons;
 2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and
 3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying District and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the District shall notify the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents.

In the event that more than 5,000 New York State residents are to be notified at one time, the District shall also notify consumer reporting agencies, as defined pursuant to State Technology Law Section 208, as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to school districts required to make a notification in accordance with Section 208(2) of the State Technology Law, regarding notification of breach of security of the system for any computerized data owned or licensed by the District that includes private information.

State Technology Law Sections 202 and 208

Adopted: 8/19/08

SUBJECT: EMPLOYEE PERSONAL IDENTIFYING INFORMATION

In accordance with Section 203-d of the New York State Labor Law, the District shall restrict the use and access to employee personal identifying information. As enumerated in law, "personal identifying information" shall include social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or driver's license number.

The District shall not unless otherwise required by law:

- a) Publicly post or display an employee's social security number;
- b) Visibly print a social security number on any identification badge or card, including any time card;
- c) Place a social security number in files with unrestricted access; or
- d) Communicate an employee's personal identifying information to the general public.

A social security number shall not be used as an identification number for purposes of any occupational licensing.

District staff shall have access to this policy, informing them of their rights and responsibilities in accordance with Labor Law Section 203-d. District procedures for safeguarding employee "personal identifying information" shall be evaluated; and employees who have access to such information as part of their job responsibilities shall be advised as to the restrictions on release of such information in accordance with law.

Labor Law Section 203-d

Adopted: 9/15/09
Revised: 1/18/11