PRIVACY POLICY

PURPOSE:

The North Kingstown School District acknowledges the need to protect private information provided by parents and others to the School District, whether that information is electronically provided or otherwise. This policy was created to provide information on our collection and use of personal information, and to establish guidelines to protect the privacy of all information.

PHILOSOPHY:

The School District is committed to protecting your privacy. It is a serious responsibility of the School District to protect personal information about individuals. While no computing environment is 100% secure, the School District will take all reasonable precautions to protect the user's information.

POLICY STATEMENT:

This Privacy Statement applies to electronic information as well as information provided by other traditional means. This policy applies to any data collection and usage on School District sites and services; it does not apply to any third party websites linked to any NKSD websites.

POLICY

I. COLLECTION OF DATA

The NKSD website contains paper and electronic forms submitted to schools by parents (for example: field trip permission forms.) The School District collects personal information, such as student's and parent/guardian name, e-mail address, home or work address and telephone numbers, as well as demographic information, age, gender, and specific preferences of information dissemination.

The School District may collect information about user's visit to the NKSD website, including the pages viewed, the links clicked upon and other actions taken within the website. The School District may also collect certain standard information that a browser sends to every website visited, such as an IP address, browser type and language, access times and referring Web site addresses.

II. USE OF DATA

A. Security of Your Personal Information

The School District is committed to protecting the security of all personal information. A variety of security technologies and procedures are used to help protect personal information from unauthorized access, use, or disclosure. For example, the personal information provided on computer systems are stored on systems with limited access, and are located in controlled facilities. When highly confidential information is transmitted over the Internet, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) or other protocol.

B. Internal Uses

The School District uses the information collected in order to help complete transactions, to communicate back to parents/guardians and others, to update the community on service and benefits, and to personalize the NKSD web sites.

Access to personally identifiable information is only given to School District employees who need to know particular information in order to provide specific services. Employees are obligated to protect that information and limit its uses to those described in this policy.

C. Disclosure To Third Parties

The release of personal information to a third party will follow the specific instructions parents/guardians give to the School District. If no instructions are given, the School District will follow state and federal law for release of information.

The School District will not sell, rent, or lease any personally identifiable information to anyone. The School District will not share any of personally identifiable information with third parties except in the limited circumstances described below, or with express permission (and to employees as described above), or to comply with applicable law. These third parties will be limited by law or by contract from using the information for secondary purposes beyond the purposes for which the information is shared.

The School District only discloses information that in good faith or a search warrant, is appropriate to cooperate with investigations of fraud or other illegal activity, or to conduct investigations of violations of School Committee Acceptable Use Statement. (Policy IJNDB-R)

Information will be disclosed in response to a civil or criminal subpoena, warrant, court order, levy, attachment, order of a court-appointed receiver or other comparable legal process.

Information will be disclosed to an agent or legal representative if there is a holder of a power of attorney, or an appointed guardian.

Information will only be shared with third parties, in compliance with the Federal Family Educational Rights and Privacy Act of 1974 (FERPA), Health Information Privacy Protection Act (HIPPA) and when required by the Rhode Island Access to Public Records Act or other federal, state or local ordinance.

Under no circumstances will the School District allow third parties in attendance at meetings where private medical information about a student in the District is discussed, unless otherwise authorized by law.

D. Retention and Disposal of Data

The School District retains the private information of individuals only as long as there is an active need to do so. The Technology Director or designee of the School District will review the names, e-mails and other private information stored in the District's technology system on a yearly basis and will delete information related to students who are no longer attending school in North Kingstown. The disposal of electronic data will follow the same guidelines as the National Institute of Standards and Technology.

E. Email

Any electronic mail message (e-mail) sent to the School District will contain your return e-mail address. Any personally identifying information contained in e-mail may be used in responding to a request. E-mail is not considered a secure means of transmitting information. Information sent via e-mail should only be as detailed as to process a request. If e-mail is sent to a NKSD address, it will be forwarded to those individuals (employees, school board members) necessary to address that e-mail.

F. Email Lists

The information collected when a subscriber joins to one of our email lists is used solely to administer these lists and is not shared, disclosed or sold to other organizations. Users who no longer wish to receive school notifications may opt-out of receiving these communications by sending an e-mail to the administration of the school listserv.

III. BIOMETRIC DATA

The School District utilizes encrypted biometric data in the form of fingerprint scans to administer the District's lunch program. Biometrics are used in verifying a claimed identity or identifying an unknown individual from numeric templates created when enrolling individuals in a data base. Parents and others should note that the type of biometric encryption utilized by the School District does not allow the reversal of the technology to identify an individual student. The following restrictions and guidelines are applicable:

A. Use of Biometric Data

The use of Biometric Data in the possession of the School District is restricted only to those District employees who need to know that information for specific services. The School District will not share Biometric Data with third parties except as strictly authorized by law in the limited circumstances described in paragraph II C entitled "Disclosure To Third Parties".

B. Security of Biometric Data

The School District recognizes the serious responsibility to protect Biometric data of students. The following measures are taken to protect Biometric Data from unauthorized access:

- The accounts are encrypted to prevent hacking.
- The biometric numbers are not stored on the internet.
- The biometric numbers are stored at the North Kingstown Technology Building with an alarm tied to the North Kingstown police, three locked doors and the building is video monitored. The District uses the industry's leading firewall to protect the network from unauthorized access.
- The point of sale scanners are locked at each cafeteria and turned off when not in use to prevent unauthorized access.
- Biometrics store numbers, not fingerprints hindering access to account numbers and printing out a fingerprint.

C. Disposal of Biometric Data

All biometric data related to a student shall be destroyed immediately upon parental request, the graduation of that student, or upon receiving notice that a student is not longer attending North Kingstown School District.

D. Written Permission

The School District must obtain written permission from a parent/guardian for a child to be scanned and participate in the Biometrics program. A permission form will be sent to all parents or guardians prior to any child using the biometrics program. The permission form will contain the specifics of the program including when, how and what information will be collected, used and disposed of; the restrictions on the use of the data by School District personnel and third parties; along with a request that parents/guardians who agree to participate must sign a permission statement. The form will clearly explain that biometric data will be destroyed after students either withdraw from the program, leave the school or graduate. If a student is 18 years of age, the form will be signed by the student.

The Federal Family Educational Rights and Privacy Act of 1974 (FERPA) may well apply to protect the privacy of biometric data, and the School District will protect the privacy of such data as described in this policy, and will release such data only as required by law.

All provisions of this policy restricting the collection, use, access, security, retention and disposal of private information by the School District shall apply with equal force to the use of biometric data.

First Read: 12-14-2009
Second Read: 1-26-2010
Adopted: 1-26-2010