Regulation 5671R **Non-Instructional/Business Operations**

INFORMATION SECURITY

This regulation accompanies Board po4licy 5671 *Information Security* and is designed to assure that confidential information stored by the district (electronically or otherwise) is properly available for authorized access and is effectively protected from unauthorized access. The steps indicated here are intended to prevent and respond to possible identity theft as well as other illicit uses of such information.

Protected information includes information that is legally protected by law as well as "personal, private, or sensitive information" (PPSI) of students, staff, and others.

Classification of Information

Determinations of what information is protected will be according to laws and consistent with other Board policies that address such information.* The Superintendent will designate administrative officials who, in collaboration with the Director of Technology, will make and oversee such determinations within their respective domains of responsibility. Such domains include but are not limited to educational records, special education records, student health records, student/family personal and financial information, employee/volunteer/outside consultant information, and any other records containing personal, private, or sensitive information (PPSI).

With the Director of Technology, the designated officials will be responsible for maintaining the currency and accuracy of protected records in their domains.

Access

The designated officials will also be responsible for determining who is and who is not authorized to access protected information. Authorized access will be consistent with laws, pursuant to Board policy 5671, and on a need-to-know basis.

The Director of Technology will maintain the electronic database which contains protected information. Officials will collaborate with the Director of Technology in establishing and maintaining the structure and details of that database with respect to access and restriction and in keeping it current.

Technology

Protected information held by the District will be maintained in an electronic database whose software is designed to assure the security of such information by permitting authorized access while prohibiting unauthorized access. Authorized access will require user name and password identification.

The Director of Technology will oversee the database and, in collaboration with other District officials, will maintain its currency by updating any changes in authorization that may occur.

Where mobile computing devices (MCDs—laptops, tablets, smart phones, etc.) are able to access the District server and protected information remotely, the Director of Technology will be

responsible for determining the level of security each device needs and for providing appropriate encryption.

Email

Pursuant to policy 5671, district personnel are expected to understand the seriousness of safeguarding protected information and to apply extreme caution in the use of email (or other channels) that may contain protected information. Prior to sending any such information by email, staff members should take steps to assure that the recipient is, in fact, authorized to receive it. These expectations apply to email sent through the District's server as well as through any personal email channels.

Staff members must understand that the privacy of any email cannot be guaranteed. Any time a staff member knows or suspects that unauthorized access to an email containing protected information may have occurred, he/she shall report it immediately to his supervisor and the Director of Technology.

Information Breach

Any District employee or other person who suspects that an information security breach has occurred will immediately notify his/her supervisor and the Director of Technology and will provide the information on which his/her suspicion is based.

In addition, the Director of Technology, in collaboration with other staff and officials where appropriate, will monitor the electronic database for any signs of a breach and will report any suspected breach to the Superintendent. Where appropriate, the Superintendent will conduct further investigation to determine whether or not a breach has occurred, how it occurred, which information may have been compromised, and the extent of compromise. The Superintendent, in consultation with the Director of Technology and others, will direct whatever actions may need to be taken to restore and assure high levels of security to the system.

In the event of a breach, the Superintendent will follow the criteria set forth in Section 208 of the Information Security Breach and Notification Act (State Technology Law) to determine whether or not to initiate the notification procedure. Once initiated, notification will proceed in accordance with all the terms of Section 208 of the law.

Copies of the law detailing the procedures to be followed will be kept on file in the offices of the Superintendent and the Director of Technology. It is also available online at http://law.onecle.com/newyork/state-technology/STT0208_208.html.

Staff Awareness

Staff awareness of the expectations and procedures related to the storage and use of protected information will be promoted through multiple channels including but not limited to guidelines, notifications, reminders, etc. issued by the Director of Technology and others, as well as through training incorporated in professional development sessions. Staff members who are new to the District will receive complete information regarding the expectations and procedures associated with the use and safeguarding of protected information.

In collaboration with other District officials, the Director of Technology will oversee and maintain the currency of information conveyed to staff. Such information will be designed to address the criteria set forth in policy 5671, specifically:

- What kinds of information are protected (student educational records, PPSI, etc.) and the utmost seriousness of maintaining the security of protected information
- Who has authorized access to such information and who does not
- Guidance in the use of desktops, laptops, MCDs and relevant software
- How to exercise care when engaging with protected material through email; pitfalls to avoid
- How and to whom to report suspected information breaches
- How to guard against non-electronic breaches of protected information

***Related Policies**

The Board policies listed below are directly or indirectly related to the issue of information security:

- 5660: School Food Service Program
- 5672 Employee Personal Identifying Information
- 5675 Student Grading Information Systems
- 7240: Student Records: Access and Challenge
- 7241: Student Directory Information
- 7243: Confidentiality of Personally Identifiable Data on Classified Students
- 7244: Military Recruiters' Access To High School Students And Directory Information
- 7620: IEP Distribution

New Regulation: 09-06-13
Revised: 10-22-18