

## February 2026 Policy - First Reading Packet

Policy Number	Title of Policy	Explanation	Adopted BOCES Update	Revised by SH	Keep Current Policy	Deleted	Date of Vote
<a href="#">3311</a>	<b>Notification of Disclosure of Employee Disciplinary Records</b>	<p><b>Required policy.</b> This new policy was developed in response to the addition of subdivision 6 to Section 87 of the Public Officers Law, enacted as Chapter 302 of the Laws of 2024, which mandates that New York public agencies, including K-12 school districts, notify employees when their disciplinary records are requested under the Freedom of Information Law (FOIL). The amendment requires K-12 school districts to develop a policy regarding the required notification but does not establish specific procedures for issuing the notification. Districts should use their best judgement as to the most appropriate form of notification. While the text is silent on this issue, the Committee on Open Government states that the notification should be in writing so that the district has evidence of compliance and that notice by either regular mail or email is sufficient. Districts should make reasonable efforts to notify former employees and document their efforts to do so. Given that collective bargaining agreements often include provisions on employee record handling, any policy changes that impact notification could be viewed as altering these agreements. Consequently, districts may need to work with union representatives in implementing this policy.</p> <p><b>Policy Committee recommends adopting with customization</b></p>					
<a href="#">5850</a>	<b>Data Networks and Security Access</b>	<p>Revised in response to a review of the updated NYS IT Governance Document (2024). The policy was re-written to provide current guidance on topics such as firewalls, passwords, patch management, and IT Contingency planning. Additionally, the policy was renumbered from 5674 for better placement in the manual, placing it within the Technology section of the manual.</p> <p><b>Policy Committee recommends adopting as is.</b></p>					

## **SUBJECT: NOTIFICATION OF DISCLOSURE OF EMPLOYEE DISCIPLINARY RECORDS**

### **Overview**

In accordance with New York State Public Officers Law, this policy establishes a process to notify district employees when the District is responding to a request for their disciplinary records.

### Scope

This policy applies to all current and former employees of the District whose disciplinary records may be subject to public disclosure under the Freedom of Information Law (FOIL).

### **What Constitutes an Employee Disciplinary Record**

For purposes of this policy, disciplinary records are any record created in furtherance of a disciplinary proceeding. ~~, including, but not limited to:~~

- ~~a) The complaints, allegations, and charges against an employee;~~
- ~~b) The name of the employee complained of or charged;~~
- ~~c) The transcript of any disciplinary trial or hearing, including any exhibits introduced at such trial or hearing;~~
- ~~d) The disposition of any disciplinary proceeding; and~~
- ~~e) The final written opinion or memorandum supporting the disposition and discipline imposed including the District's complete factual findings and its analysis of the conduct and appropriate discipline of the covered employee.~~

### **Notification Upon Release of Disciplinary Records**

When the District releases an employee's disciplinary records in response to a FOIL request, it will ~~promptly~~ provide written notification to the affected employee, unless the request is from the employee for their own records.

For current employees, this notification will be sent to the employee's work email address or, if unavailable, their home address on file with human resources.

For former employees, this notification will be sent to the employee's last known home address on file with human resources. The District will make every reasonable effort to notify former employees, and will document the steps taken to do so.

(Continued)

Community Relations

**SUBJECT: NOTIFICATION OF DISCLOSURE OF EMPLOYEE DISCIPLINARY RECORDS  
(Cont'd.)**Content of Notification

The notification will include a brief **and general** description of the released records. This notification is for informational purposes only and does not require employee consent. Its purpose is to ensure employees are aware of the disclosure.

Public Officers Law Section 87

NOTE: Refer also to Policy #3310 -- Public Access to Records

Adopted:

Non-Instructional/Business  
Operations**SUBJECT: DATA NETWORKS AND SECURITY ACCESS**

The District values the protection of private information of individuals in accordance with applicable law, regulations, and best practice. Accordingly, District officials and Information Technology (IT) staff will plan, implement, and monitor IT security mechanisms, procedures, and technologies necessary to prevent improper or illegal disclosure, modification, or denial of sensitive information in the District Computer System (DCS). Similarly, such IT mechanisms and procedures will also be implemented in order to safeguard District technology resources, including computer hardware and software. District network administrators may review District computers to maintain system integrity and to ensure that individuals are using the system responsibly. Users should not expect that anything stored on school computers or networks will be private.

In order to achieve the objectives of this policy, the Board of Education entrusts the Superintendent, or his/her designee, to:

- a) Maintain ~~Inventory~~ inventories of computer hardware, software, and data, to include:
  1. Computer hardware - physical description, person assigned to, physical location, and relevant purchase or lease information;
  2. Software - description of item, locations installed, and pertinent licensing information;
  3. Data - ~~and classification based on district data classification scheme, and location where data resides. personal, private, and sensitive information on the DCS to protect the confidentiality, integrity, and availability of information~~
- b) Regularly update inventories;
- c) Install and maintain antivirus software on all district devices. Antivirus software should be set to update definitions daily and to scan for threats throughout the day. Hardware should be set to force scans of all newly connected devices;
- d) Ensure that software patches and updates are installed in a timely fashion to address potential weaknesses in out-of-date software;
- e) Develop procedures for promptly disabling accounts of former employees and for ensuring that former employees cannot access district systems and accounts;
- bf) Develop password standards for all users ~~including, but not limited to, how to create passwords and how often passwords should be changed by users to ensure security of the DCS~~ that adhere to current industry standards for password security;

(Continued)

Non-Instructional/Business  
Operations**SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)**

- ~~f) Periodically grant, change, and terminate review user access rights to the overall networked computer system and to specific software applications and to ensure that users are given access based on, and necessary for, only to those resources necessary for their job duties;~~
- ~~e) Ensure that the "audit trail" function is enabled within the District's network operating system, which will allow the District to determine on a constant basis who is accessing the DCS, and establish procedures for periodically reviewing such audit trails;~~
- h) Establish policies for remote access, which should include eligibility requirements, District expectations, and provisions to monitor and control remote access;
- i) Utilize a firewall configured to allow only communication types necessary for system operation and to explicitly deny all other communications. Such firewall logs should be monitored for potential security and resource issues, including for intrusion detection;
- ~~d) Develop procedures to control physical access to computer facilities, data rooms, systems, networks, and data, ensuring adequate physical security commensurate with the risks of physical damage or access; to only authorized individuals; these procedures may include ensuring that server rooms remain locked at all times and the recording of arrival and departure dates and times of employees and visitors to and from the server room;~~
- ~~e) Establish procedures for tagging new purchases as they occur, relocating assets, updating the inventory list, performing periodic physical inventories, and investigating any differences in an effort to prevent unauthorized and/or malicious access to these assets;~~
- ~~f) Periodically grant, change, and terminate review user access rights to the overall networked computer system and to specific software applications and to ensure that users are given access based on, and necessary for, only to those resources necessary for their job duties;~~
- ~~g) Limit user access to the vendor master file, which contains a list of vendors from which District employees are permitted to purchase goods and services, to only the individual who is responsible for making changes to such list, and ensure that all former employees' access rights to the vendor master list are promptly removed;~~
- ~~h) Determine how, and to whom, remote access should be granted, obtain written agreements with remote access users to establish the District's needs and expectations, as appropriate, and monitor and control such remote access;~~
- ~~i) Verify that laptop computer systems assigned to teachers and administrators use full-disk encryption software to protect against loss of sensitive data;~~

(Continued)

Non-Instructional/Business  
Operations

**SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)**

- ~~j) Deploy software to servers and workstations to identify and eradicate malicious software attacks such as viruses and malware;~~
- k) Develop an ~~disaster recovery~~ IT contingency plan appropriate for the size and complexity of District IT operations to ensure continuous critical IT services in the event of any sudden, catastrophic event, including, but not limited to fire, computer virus or deliberate or inadvertent employee action.

Adopted: 4/19/16

Revised: