Concord School District Policy #817 *

Internet Use – Staff

1. **Preamble**

   The purpose of this policy is to serve as a statement on the appropriate and acceptable use of the School District computer network (the Network), including the District's connection to the Internet, by District staff.

2. **Definitions**

   The Network consists of all computers of any type, monitors, printers, permanent and portable computer peripheral devices, personal digital assistants, alphanumeric pagers and cellular phones, digital photocopiers and, in general, any hardware, software, media or other devices that are owned or leased by the District. Any computers of any type, monitors, printers, permanent and portable computer peripheral devices, personal digital assistants, alphanumeric pagers and cellular phones, digital photocopiers and, in general, any hardware, software media or other devices that are not owned by the District but that have been permitted to be attached to the Network shall be considered part of the Network and shall be governed by this policy.

3. **Access privileges**

   The use of the Network is an integral part of the District's work. There are and will be varying degrees of access to the Network that are and will be allowed to different users.

   Inappropriate use will result in restriction or cancellation of access privileges and such other actions as the District's administration deems appropriate for violations of the District's or school building's policies or procedures. Other actions may include verbal warnings, written warnings, work suspensions with or without pay and termination of employment.

4. **Educational purposes**

   The purpose of the Network is to serve as a resource for improving, extending and enriching teaching and learning in the District. Any use by staff that interferes with the staff person's duties or the duties of another staff member shall not be permitted. Users are responsible for ensuring that their activities adhere to these uses and generally accepted educational standards.

   Inappropriate use includes all those activities prohibited to the user based on their allowed degree of access and any activity that violates the District's or school building's policies or procedures.

   Uses of the Network that are not considered acceptable for education purposes are generally those that are unlawful or offensive, which include but are not limited to:

   - Destruction or damage to equipment, software or data belonging to the District or to others;

- Disruption or unauthorized use of accounts, access codes or identification numbers;
- Use of computer resources to defraud, harass, bully, defame or threaten others;
- Use of computer resources in such a way as to intentionally or unintentionally impede the computing activities of others;
- Use of computer resources that violate copyright, trademark or license agreements;
- Use of computer resources to violate another's privacy;
- Transmission of unsolicited advertising, promotional materials or other forms of solicitation, including placing hyperlinks to non-District related websites;
- Use of computer resources for commercial purposes;
- Inappropriate mass mailings;
- Tampering with software protections or restrictions placed on equipment or files;
- Attempting to circumvent local or Network security restrictions;
- Altering or attempting to alter system software or hardware configurations;
- Installing unauthorized software programs onto the District's computers or Network, and/or using such programs on the District's computers or Network;
- Use of computer resources outside of the Network to cause material and substantial interference with education and discipline within a school;
- Ignoring or disobeying policies and procedures established for specific network systems; and,
- Use of computer resources to access adult-oriented sites that contain descriptions or depictions of a pornographic or obscene nature, or that permit access to gambling facilities over the Internet.

The above list is not intended to be a comprehensive list, but rather to provide examples of inappropriate use of the Network. The District may choose to employ filtering software and/or devices that may block certain sites, or that may notify appropriate administrators and/or staff that inappropriate use is taking place within a building. Any such notification shall be investigated in accordance with Part 5 of this policy.

5. Investigation

a. All investigations that relate to student conduct (Policy #540), and/or sexual harassment (Policies #414 and #521), and/or bullying (Policy #539) shall also be investigated as required under those policies. Disciplinary actions may include those outlined under the above policies if investigations find that violations of the policy or policies in question occurred.

b. Investigating administrators shall be the building Principal or, if designated, the Assistant Principal, in his or her respective building. The Business Administrator shall be the investigator for the central office, maintenance and transportation facilities. The

Assistant Superintendent shall serve as a backup for the building Principals unable to conduct an investigation in their buildings. The Superintendent shall be responsible for investigations involving administrators under this policy, and the President of the Board shall be responsible for investigations involving the Superintendent. All administrators may use internal technical expertise as needed and may be authorized to use external technical expertise if deemed necessary.

6. Responsibilities

All users assume full liability – legal, financial and otherwise – for their actions when using the Network. All users of the Network will be held fully responsible for the use of their account. Any inappropriate activities performed through the account will be considered to be the actions of the account holder. Users should report any inappropriate activity observed to the building Principal or a responsible administrator immediately. The responsibility of the user is to familiarize himself/herself with and abide by the rules of the District's Internet Use – Staff policy.

7. Privacy

The Network is maintained and managed by the system administrator in such a way as to ensure its availability and reliability in performing its educational mission. Users have no reasonable expectation of privacy concerning any materials transferred over or stored with the Network, even if protected by password. The District reserves the right to monitor, access, change, delete, review and/or retrieve any and all information transferred to or stored on the Network, even if such information has been deleted but is still available on the Network and/or on District-owned media storage such as, but not limited to, diskettes, CD-ROMs, tapes, zip disks, or other types of data storage. Users will be expected to surrender any and all passwords needed to access this information if requested.

8. Retention of records

All electronic information shall be retained in accordance with the District's Records Retention Policy.

Adopted October 4, 2004. Revised August 6, 2018
* Also Policies #433 and #652
Corresponds to NHSBA Policies GBEF, EHAA, JICL