Spencerport Central School District
Policy Regulation

REGULATIONS
Staff Use of Computerized Information Resources
Regulation #5260R

The Spencerport School District's Computer Systems (hereafter referred to as, "SC-CS") is provided for staff to enhance the educational programs of the Spencerport School District, to further Spencerport School District goals and objectives; and to conduct research and communicate with others. SC-CS is defined as Spencerport School District computerized system consisting of software, hardware, computer networks (wired and wireless), electronic communication systems, email, on-line services, Internet, portable computing devices, portable media and removable media and software subscriptions.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the SC-CS. The standards of acceptable use as well as prohibited conduct by staff accessing the SC-CS, as outlined in Spencerport School District policy and regulation, are not intended to be all-inclusive. The staff member who commits an act of misconduct which is not specifically addressed in Spencerport School District policy and/or regulation may also be subject to disciplinary action, including loss of access to the SC-CS as well as the imposition of discipline under the law and/or the applicable collective bargaining agreement. Legal action may also be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the SC-CS.

Staff are encouraged to utilize electronic communications in their roles as employees of Spencerport School District. Staff are also encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. Such usage shall be limited to school related issues or activities. Communications over the SC-CS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The Spencerport School District policies and accompanying regulations on staff and student use of computerized information resources establish guidelines for staff to follow in instruction and in working with students on acceptable student use of the SC-CS, including access to external computer networks.

Definitions:

- **Portable computing devices (PCDs)** – including, but not limited to, smart phones (i.e., iPhones, Android devices), computers, laptops, tablets (e.g., iPad), RIM Blackberrys, MP3 players, text pagers, and/or other similar devices.
- **Portable/removable media –** includes but is not limited to CDs, DVDs, external hard drives, floppy disks and universal serial bus (USB) drives (also known as memory sticks, jump drives and thumb disks).
- **User** – Anyone with authorized access to the SC-CS and information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid Spencerport School District access accounts.
- **Firewall** – Software, or a combination of hardware and software, that implements security policy governing traffic between two or more networks or network segments, used to protect internal networks, servers, and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a laptop computer, and must be configured properly to enable protection.
- **Screen Locking –** Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.
- **Screen Timeout** – An automated mechanism hide data on a visual display while the computer continues to operate after a specified time period.
- **Restricted Information** – information includes but is not limited to protected health information (PHI), personal identification information, confidential student records, and any other information whose access is prohibited by laws.
- **Cloud** – Storage and data services that are hosted by a 3rd party and are utilized for district computational needs.

Security

- PCDs, computer media, and removable components must be stored in designated areas, and must not be left unattended without ensuring that the designated area is securely locked.
- Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.
- Mandatory system configurations, settings, and software for Spencerport School District-owned equipment must not be modified without prior authorization by Technology Operations. PCD operating systems must be maintained with appropriate vendor security patches and updates.

Privacy Rights

The SC-CS, staff data files, email, the Internet, and all electronic information systems, SC-CS Cloud storage and all other storage areas shall remain Spencerport School District property, subject to Spencerport School District control and inspection. The staff member designated by the District Superintendent may access all such files and communications to insure system integrity and that users are complying with requirements of Spencerport School District policy and accompanying regulations. Staff should NOT expect that information stored on the SC-CS will be private. Use of Spencerport School District systems constitutes consent to monitoring by Spencerport School District.

Data Security

Restricted Spencerport School District data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all restricted Spencerport School District data stored on portable computing devices must be secured in the following way:

- Spencerport School District data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols, approved encryption techniques, and a password is utilized.
- If restricted data is transferred/synchronized either via wire (LAN/WAN or Public Internet) or wireless connections (including to and from web sites, server databases, or email servers), it must be transmitted in an encrypted format using the Spencerport School District centralized, secured server or the SC-CS approved Cloud vendor.
- Use of the included synchronization software from the portable computing devices manufacturer is permitted when the data sources are not considered restricted under the Spencerport School District policy.
- Portable computing devices must not be equipped with remote system or application administrator privileges unless authorized. Portable computing devices equipped with remote system administrator capabilities must be assigned higher levels of security in accordance with the increased risk of an IT security breach or loss of device.
- All remote access to Spencerport School District Information systems must be either through a Virtual Private Network (VPN) or via other district provided access mechanism.
- Restricted information stored on removable media must also be stored on the SC-CS cloud so notification obligations can be carried out expediently in the event of an inappropriate disclosure.
- There are procedures for the return of Spencerport School District-owned portable computing devices (PCDs) when the user's employment or contract terminates, or the user's assignment no longer requires the device. Please contact the Technology Operations Help Desk for support.
- If removable media with SC-CS data on it is misplaced, the user must contact their Program Director/Supervisor immediately so necessary steps can be taken to limit damage and liability of an inappropriate disclosure.
- Provisions of this policy and regulation apply equally to non-Spencerport School District provided equipment during the time the equipment accesses or uses Spencerport School District information or networks including but not limited to the SC-CS Bring Your Own Device (BYOD) network.
- The provisions of this policy and regulation apply to users when accessing Spencerport School District information and computer systems from remote locations.
- Spencerport School District provided equipment shall be secured to prevent non-district employees access to Spencerport School District information.

Prohibitions

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of acceptable staff behavior, activities which shall be prohibited by staff members using the SC-CS include, but are not limited to, the following:

1. Using the SC-CS which in any way results in unauthorized charges or expense to the Spencerport School District.
2. Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.
3. Using unauthorized software on Spencerport School District-owned equipment.
4. Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member without express permission from that person or the Director of Technology Operations.
5. Violating copyright law or trade secrets.
6. Employing the SC-CS for commercial purposes, product advertisement or political lobbying.
7. Disclosing an individual password or any personal account information to others or using others' passwords unless in extenuating circumstances with the building administrator's approval.
8. Sharing confidential information on students and employees.
9. Sending or displaying offensive, vulgar, abusive, unlawful, or sexual messages or pictures.
10. Using obscene language.
11. Harassing, insulting or attacking others.
12. Engaging in practices that threaten the SC-CS (e.g., loading files that may introduce a virus, engaging in distributed denial of service attacks).
13. Violating regulations prescribed by the network provider.
14. Use of the SC-CS for other than school related work or activities.
15. Assisting a student to violate Spencerport School District policy and/or regulation, student code of conduct, or failing to report knowledge of any student or staff violations of Spencerport School District policy and regulation.
16. Use which violates any other aspect of Spencerport School District policy and/or regulations, as well as local, state or federal laws or regulations.
17. Using the system for hacking, forgery, or vandalism.
18. Using the system for any bullying, intimidation, discrimination or bias.
19. Sexually harassing or bullying anyone.
20. Sending illegal, immoral and/or unethical messages.
21. Employees shall not use unauthorized encryption software on Spencerport School District equipment. Email must include an author; neither anonymity nor impersonations are permitted.
22. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.
23. Any user of the SC-CS that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

24. Spencerport School District makes no warranty as to the accuracy, appropriateness, or quality of information accessed on the Internet.

Sanctions

Inventory and security audits will be conducted on any aspect of the SC-CS on a routine and random basis. The staff member who had been designated by the District Superintendent will report inappropriate behavior to the District Superintendent who will take appropriate action if needed. Any other reports of inappropriate behavior, violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the SC-CS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

Notification

Annually all staff will be emailed a copy of Spencerport School District policies on staff use of computerized information resources and the regulations established in connection with those policies. Additionally, copies of these documents will be made available on the District's intranet and Internet web pages.