Year: 2018 **Policy Number: 3110** **Section**: □ Community Relations x Administration □ Business Procedures □ Community Operations □ Personnel □ Students □ Instruction	HealthSciences CHARTER SCHOOL

SUBJECT: Computer, Network, and Information Systems Access, Control, Use, and Network Security

Policy Statement

The Health Sciences Charter School ("HSCS" or "the school") computers, networks and other technological resources support the educational and administrative functions of the school system. Due to employees and students depending on these systems to assist with teaching and learning and because sensitive and confidential information may be stored on these systems, system integrity and security is of utmost importance. This policy is intended to ensure that personal information is dealt with correctly and securely to meet all legal requirements for maintaining the privacy and security of protected student data, teacher data, and other protected school data under applicable state and federal laws, as well as to educate its' staff on such obligations and mandates.

Network and Information Security

The school system information technology systems are valuable assets that must be protected. To this end, school technology personnel shall evaluate each information technology asset and assign protective controls that are commensurate with the established value of such assets. Appropriate security measures must be in place to protect all information technology assets from accidental or unauthorized use, theft, modification or destruction and to prevent the unauthorized disclosure of restricted information. Network security measures must include an information technology system disaster recovery process. Audits of security measures must be conducted annually.

The use of the HSCS network is restricted to school-owned equipment. Personal or outside equipment can only be used on the HSCS network with the express permission of an Administrator (who must provide the access code to the school's wireless system). All personnel shall ensure the protection and security of information technology assets that are under their control.

Security Awareness

The schools' IT administrator (either in-house or from the outside firm contracted with) shall provide employees with information to enhance awareness regarding technology security threats and to educate them about appropriate safeguards, network security and information security. A general training will be done upon an employee starting their employment with the school and follow-ups will be done as deemed necessary.

Virus Protection

Virus detection programs and practices must be implemented throughout the school system. The Principal or designee is responsible for ensuring that the school system network includes current software to prevent the introduction or propagation of computer viruses.

User ID and Password

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of HSCS's resources. All users (for these purposes, students are excluded in the definition of users as the access they have to school systems is limited and does not pose a significant threat to the systems) with access to the school's systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

All users of information technology systems must be properly identified and authenticated before being allowed to access such systems. The combination of unique user identification and a valid password is the minimum requirement for granting access to information technology systems.

Users will be required to reset network passwords every ninety (90) days. Users will receive an electronic reminder notice indicating it is time to change their passwords; each user will then have three subsequent logons with their old password where they will continue to be prompted to change their password. At that time, if the password has not been changed, the user will be locked out of the network and will need to see the network administrator to have their password reset. Users should create a unique password every time; incremental passwords should be avoided.

To provide the utmost security, "strong" passwords shall be created by users consisting of a minimum of eight (8) characters. A "strong" password shall contain a combination of:
1) at least one uppercase and one lowercase letter;
2) at least one numeric; and
3) at least one punctuation character.

Avoid weak passwords such as:

- Using part or all of your username;
- Names or other information about family members, friends or pets that could be found on social media;
- Personal information about yourself or family members that can easily be obtained online, such as a birth date;
- Date, phone number, street name;
- Any sequences such as "abcde", "12345", or even in reverse order;
- Actual dictionary words in any language, including those with a number or character in front or back, or substituting a number for a letter, such as "0" in place of "o".

Passwords must not be disclosed, shared or communicated with any third parties. The password is the private knowledge of the user and must not be shared. Employees shall ensure that they make use of technology and related services only as required in the performance of their job and/or academic function. Users are responsible for all transactions occurring during the use of their user ID and/or password.

Any breach of security or compromise of safeguards must be reported immediately to the Principal or network administrator.

IT Systems/Data Backups

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practices.

The following steps will help ensure the schools' information and data is backed up and restored securely in the most efficient manner possible:

1) The school's IT administrator is responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the school's Disaster Recovery Procedures and data retention procedures;
2) All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery;
3) All data, operating systems/domain infrastructure data and supporting system configuration files must be systematically backed up, including patches, fixes and updates which may be required in the event of system re-installation and/or configuration;
4) All backup media must be encrypted and appropriately labeled with date/s and codes/markings, which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster;
5) A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup job;
6) Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed;
7) Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised;
8) All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media; and
9) Regular tests must be carried out to establish the effectiveness of the school's backup and restore procedures by restoring data/software from backup copies and analyzing the results.

User Responsibilities

IT Users also have a responsibility to ensure school data is securely maintained and is available for backup:

1) IT Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorized software which require the 'caching' of files locally in order to function). Instead, users must save data (files) on their allocated areas - this could be a mapped drive or network shared folder the User has access to. Data (files) which are stored "locally" will NOT be backed up and will therefore be at risk of exposure, damage, corruption or loss;
2) If the school network becomes unavailable for whatever reason and data or work is at risk of being lost, users may save the data (files) locally (i.e. on the computer being used) or on media storage such as a data stick (USB storage). Once the network becomes available again, data (files) should be immediately transferred to the network in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored; and
3) USB data sticks should only be used to store data for temporary purposes. All sensitive, business and personal identifiable information should be removed from the USB data stick and moved to an appropriate data network location as soon as possible. If a USB must be used offsite and has data from the school on it, the USB must be password protected and encrypted to ensure the integrity and security of the data.

Supporting Procedures:
Related Laws, Regulations & Acts:
Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Adopted: 3/12/2015 Revised: 6/9/2021