VIGO COUNTY SCHOOL CORPORATION
TERRE HAUTE, INDIANA

File: __GBLA-R___

I. COMPUTER OPERATIONS

Access (physical, virtual or otherwise) to VCSC data, the Network Operations Center (NOC), Data Centers, wiring closets, and associated equipment is restricted to authorized operational and maintenance personnel. Every precaution should be taken to prevent unauthorized access to the VCSC internal network, data, and systems. Access to computer data, shared within all VCSC computer systems, is restricted to appropriately authorized personnel. The Information Technology Department (IT) is responsible for maintaining security procedures. Unauthorized access to the computing and network resources of the School Corporation may be considered misconduct, may result in disciplinary action, and could be a violation of law. Violations will be reported to the immediate Supervisor, the Technology Director, and/or the Human Resources Director.

A. Security and Access

To maintain proper security and safety, the following policies apply:

1. Access to data centers, networking equipment, and systems with secure data is restricted to those persons needed to operate, supervise, or provide maintenance to the area and its equipment. A system to restrict access will be maintained.

2. Levels of access and authorization for VCSC equipment, systems, and data will be controlled with proper user accounts and passwords. Passwords will not be shared and accounts will be used only by the assigned user. Practices to ensure the construction of strong passwords and their security will be applied by the IT Department. Passwords for accounts that access School Corporation financial data will be changed every thirty (30) days. Passwords for accounts that access student data will be changed every ninety (90) days. Passwords for accounts that include, but are not limited to e-mail, file sharing, student folders, course management systems, web site editing, databases, etc, will be changed on a schedule to be determined by the IT Department. To further limit the risk of unauthorized access, accounts that are suspended or no longer required will be deleted regularly.

3. The IT Department will develop governing procedures for computer operations.

4. The IT Department will be responsible for developing and maintaining systems and procedures for workstation security.

5. Access to data and secure areas will be determined by the Administrator of the department, area, or program involved. Final authority regarding access will be determined by the Superintendent or his/her designee.

II. APPLICATIONS

A. Operation of a committee structure to review appropriate software for inclusion on any VCSC computer system will be the responsibility of the Director of Technology.

B. Personal Hardware and Software

1. In general, no personally-owned hardware or software is allowed to be connected to or installed on VCSC computers or the VCSC internal network. All equipment and software of any kind that is connected to or installed on VCSC computers or networks must be VCSC hardware or software. To reduce problems with equipment and software failure, damage to data files, and the introduction of malware onto the VCSC network, use of equipment or software that has not been reviewed and approved by the IT Department is not permitted. The IT Department must approve in writing any connection of personally-owned hardware or installation of personally-owned software on VCSC computers or systems.

2. To protect School Corporation data and prevent malware transmission, electronic storage media belonging to the School Corporation must not be used in personal home computers. Access to School Corporation data from external locations should be via VPN or other secure access. The IT Department will purge unauthorized software or remove unauthorized equipment and report it to the appropriate Supervisor and the Technology Director. To further aid in the management of unauthorized software installations, monitoring and blocking software will be installed.

C. Guest Network Access

1. The School Corporation's network is intended for the use of authorized users only. This also applies to the School Corporation's Guest WiFi networks. Authorized users may include students, staff, and others with a legitimate purpose for access as determined by the Superintendent or his/her designee. The School Corporation's wireless Guest networks provide limited access with fixed bandwidth and may be filtered for CIPA (Children's Internet Protection Act) compliance. Users of this network are subject to all School Corporation policies, and any state and federal laws related to such use. Use of the Guest networks indicates an agreement to comply with all terms and policies of the School Corporation. Technical support is not provided for general guest access. The School Corporation is not responsible for access or use

of the Guest network and does not guarantee the suitability or capability of it for any purpose.

Adoption Date: August 5, 1996; Revised March 9, 2009; Revised: August 21, 2017