2017-2018 WVLHS Network Code of Conduct

(Keep this form for your records.)

I. PURPOSE

The purpose of this Network Code of Conduct is to provide guidelines for ensuring the responsible and secure use of the School's network and computing systems, for safeguarding against unauthorized access and/or abuse, while making the systems accessible for authorized users.

II. SCOPE

This Code applies to all authorized users working at the School's facilities, working offsite at remote locations, and working from home. The policy also includes authorized vendors and customers having access to all or part of the School's network.

III. RESPONSIBILITY

- The users of the network are responsible for understanding and adhering to this policy and all applicable local, state, federal and international laws.
- It is the responsibility of the IT Coordinator to review and update this Code annually.
- It is the responsibility of each authorized user to read and be familiar with this Code.

IV. PROCEDURE

Section A. General Computing Policy

Whereas, all computing hardware and software belonging to the School are to be managed by the Information Technology Coordinator, all installations and configurations of hardware and software are to be authorized and managed by the Information Technology Coordinator. All computing output is the property of the school.

Once an authorized user receives a user ID and password to access the network and computer systems on that network, they are solely responsible for all actions taken while using that user ID and password. Security on the School's network is a shared concern and shared responsibility of all network users. Therefore:

- Sharing your password with any other person is prohibited. In the event that you intentionally share your password with another person, you will be held responsible for the actions of that other person.
- Loading of personal software without the approval of the Information Technology Coordinator is also prohibited.
- Unauthorized downloads including screensavers to desktops are also prohibited.
- Use of unlicensed copies of software is also prohibited.
- Attempts to evade or change resource security and permissions are prohibited.
- Any unauthorized, deliberate action, which damages or disrupts a computing system, alters its performance, or causes a system malfunction, is prohibited regardless of system location or time duration.

Section B. Electronic Mail Policy

Whenever sending electronic mail, your name and user ID are included in each mail message. You are responsible for all electronic mail originating from your user ID. Therefore:

- Forgery, or attempted forgery, of electronic mail messages is prohibited.
- Attempting to read, delete, copy, or modify the electronic mail of other users is prohibited.
- Attempting to send harassing, obscene, and/or threatening email to other users is prohibited.
- Sending abusive statements, patently unwanted materials, i.e. electronic "chain letters" or "junk mail" or "spam" to others is prohibited.

Section C. Network Security

As a user of the network, you may be allowed to access other networks and/or use the computer systems attached to those networks. Therefore:

- Use of systems and/or networks to attempt to gain unauthorized access to remote systems is prohibited.
- Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote system/local, is prohibited.
- Decryption of system or user passwords is prohibited.
- The copying of operating system files is prohibited.
- The copying of copyrighted materials, such as third-party software, without the express permission of the owner or the proper license, is prohibited.
- Intentional attempting to "crash" network systems or programs is prohibited.
- Attempting to secure a higher level of privilege or security authorization on network systems is prohibited.
- The willful introduction of computer viruses or other disruptive/destructive programs into the School's network or into external networks is prohibited.
- Using the network systems to send confidential School documents, or to communicate confidential School information to unauthorized persons is prohibited.

Section D. Personal Use

As an authorized user of the School's computing resources, you are allowed to use the Internet, email, hardware and software for personal use. Personal use should not disrupt your academic duties and responsibilities nor interfere with your scheduled class assignments. Personal use does not imply School acceptance of illegal, immoral, and unethical practices or actions on School property.

All network activities, including web access, email, Internet browsing, chat rooms, newsgroups, downloads, and other items are continuously monitored for abuse, disruptive influences, illegal functions, viruses, and wrongful usage, to prevent troublesome attacks on the School's network.

Section E. Enforcement

Any attempt to violate the provisions of this policy will result in disciplinary action in the form of temporary disablement of user accounts, and notification to the School Administrator, regardless of the success or failure of the attempt.

The users of the network are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. Should this occur, the School will comply fully with the authorities to provide any information necessary for the litigation process.

V. DOCUMENTATION

I have read and understand the Wisconsin Valley Lutheran High School Network Code of Conduct regarding Network Computing, and will abide its terms and conditions as an authorized user. I also understand that violations of the provisions of this policy will result in disciplinary action, up to or including termination of enrollment. I agree that it is my responsibility to address any questions on network systems usage and security to the School's Information Technology Coordinator.