VALIANT CROSS
ACADEMY

INTERNET SAFETY & TECHNOLOGY POLICY AND PROCEDURES

INTRODUCTION

This policy has been adopted in compliance with the Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and is the policy of Valiant Cross Academy ("VCA" or the "School") to provide technology resources, including Internet access, to its students and employees in order to more fully support the School's vision and core purpose and to meet educational and instructional goals set by the School. It is the intention of VCA that all technology resources will be used in accordance with any and all School policies and procedures as well as applicable local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. This policy applies to all technology resources, regardless of purchase date, location, or funding source. All users, in the process of logging onto the School's network, will agree to abide by all school policies. Students and staff must have the appropriate Acceptable Use Policy on file with the school prior to use. Visitors to the School must have the permission of School staff in order to access the Internet. Such permission may not be shared or transferred. This Internet Safety Policy will be displayed on the School's website and be made available upon request. Any questions about this policy, its interpretation, or specific circumstances shall be directed to the Head of School before proceeding. Violators of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action. The administrators of the School will be responsible for establishing specific practices to enforce this policy.

TECHNOLOGY PROTECTION MEASURES

Filtering and Blocking

The Children's Internet Protection Act ensures the School will make a reasonable effort to filter and block access to "visual depictions" that are obscene, contain child pornography, are harmful to minors, or that VCA determines is "inappropriate for minors." A software solution or combination of software solutions will filter all incoming Internet sites based on both URL (website name) and IP address. URLs and IP addresses may be added to the filtered list in cases where the filtering system may not have accurately identified inappropriate sites as defined above or as VCA and/or its employees determine may be inappropriate in nature, may create a disruption to School, or may place excessive demand on bandwidth. All users are required to report any sites that contain inappropriate materials or materials harmful to minors. Students must report this information to their teacher. Teachers or staff members must report the information to the Technology Coordinator. This includes any email, text, audio segment, picture, image, graphic image file, or other visual depiction that:

- Taken as a whole, appeals to an interest in nudity, sex, or excretion.
- Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political, or scientific value to minors. Adult staff members may request a review of filtered sites. Adults, who are engaged in legitimate research or need access to blocked sites for other lawful purposes, may request a temporary release of specific sites at specific workstations to complete their work. Such requests should be directed to the Technology Coordinator.

Monitoring

It is the responsibility of all teachers and employees to properly inform students/staff under their charge of this policy and to see that the policy is strictly enforced. Students using the Internet and World Wide Web will be under the direct supervision of the instructor. In addition, the School will use software to monitor Internet activity on campus no matter the ownership of the device, and 24 hours per day if the device is owned by the district. Teachers will be provided a list of students in their classes and their current status regarding use of the Internet. Teachers who will be presenting Internet sites to students as part of the instructional process must preview the sites, they plan to incorporate to ensure their safety and suitability. If students are to independently access the Internet on

a computer, the teacher must ensure that they have a signed the Student Acceptable Use Policy on file. In addition, any student under the age of 18 must also have a signed Parent Permission Form on file. During instructional time, teachers must give students specific permission to independently access the Internet and monitor their activity while they are online. The School provides additional software solutions to monitor student actions and behavior while accessing the Internet.

Communicating Electronically

VCA permits students to engage in electronic communications on a limited basis for educational purposes under the direct supervision of their teacher. All such communications are subject to School rules, the Student Acceptable Use Policy, any applicable laws, and the following safety and security measures. Student email communication conducted via School-provided accounts allows communication between teachers, students, and other School officials, however, all external email to and from students is blocked unless placed on a "whitelist" for sending/receiving. In compliance with the Children's Internet Protection Act, electronic communications (including but not limited to e-mail, chat and instant messaging) may not be used for: Unsafe practices such as:

- Contacting strangers or communicating with unknown individuals or organizations;
- Posting or forwarding other users' personal communication without the author's consent;
- Sending mass emails without the consent of the Principal or Technology Coordinator;
- Sending or attempting to send anonymous messages;
- Disclosing, using, or disseminating personal information without authorization regarding minors including, but not limited to the following: home and/or school address work, home, school, or cellular phone numbers, full names, social security numbers, etc.;
- Harmful, malicious or unlawful practices such as: spreading viruses, spamming, hacking of any type, copyright infringement, engaging in any other unlawful activities; or
- Commercial practices such as selling or advertising products or services or purchasing products or services.

Posting to the Web

All users wishing to post pages or information on the School's website must obtain prior permission and comply with rules and policies of VCA. Students may not use technology resources operated by the School to post information or graphics to personal web pages on the Internet. Student-created websites as part of an instructional activity are acceptable.

VCA prohibits posting of the following to School websites:

- Pictures of employees without their written consent;
- Pictures and other personally identifiable information without the permission in writing from the parent/guardian of the student involved;
- Pictures of students along with their full names. (Only first name and last initial of students may be used.);
- Personal information of any kind including but not limited to:
    - home and/or school address,
    - work address,
    - home and/or school phone numbers,
    - full name, and
    - social security number.
- Materials that infringe on any copyright held by others without permission and acknowledgement; and
- Any obscene, harassing or threatening materials.

VCA does permit the posting of faculty/staff listings with their school contact information (phone extension, e-mail address, etc.). In addition, webmasters may link to other websites provided the content on the linked site(s) meet the safety and professional standards set out in School policies and the linking page contains a disclaimer for the downstream website content and links.

Downloading from the Internet

Students may not download files of any type without the specific permission of their supervising teacher and within the context of the supervising teacher's coursework requirements. Under no circumstances will students be permitted to download graphic, video, or audio files in any format that violate the letter or intention of this or any other School policy. No user may download any files which violate copyright laws.

Limitations of Liability

VCA and its employees make no guarantee that the functions or the services provided by or through the School's network will be error-free or without defect. VCA will not be responsible for any damage suffered by the user, including but not limited to loss of data or interruptions of service. VCA will not be responsible for any financial obligations arising from the unauthorized or inappropriate use of School technology.

Notice of Right to Change

This policy may be changed as deemed necessary to continue to ensure the safety of students and compliance with any and all laws and regulations through action by Head of School or his designee.

Additional Restrictions

This policy is intended to work in concert with other VCA policies, procedures, and guidelines in order to ensure the safe, ethical, and educational use of all technology within the School.

COMPUTER AND INTERNET ACCEPTABLE USE POLICY FOR FACULTY AND STAFF

The term "computer," as used in this document is intended to have a broad interpretation. "Computer" as used herein, means the computer itself along with all of the accessories and peripherals used in connection with the computer such as, but not limited to, the servers, backup drivers, backup disk, network servers, communication servers, modems, Internet access software, CD drives, printers, software, stored data, computer hardware, e-mail and any and all data and programs used on the computers. The term "computer" also includes any digital device such as a tablet, phone, iPod, or any other device that serves in this function or performs functions or activities which would typically occur on a traditional computing device.

Use of computers should be in support of education, research, or business applications consistent with the purposes of VCA. Employees are to adhere to these acceptable use guidelines:

1. Employees' passwords will not be revealed to anyone other than the network administrator(s) or other personnel as determined by School administrators. Under no circumstance is an employee to reveal to a student the passwords of employees or other students.

2. The illegal installation or use of copyrighted software for use on School-owned computers is prohibited. The School must possess appropriate license(s) before copyrighted software may be installed or used.

3. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; or misrepresent other users on the computer or network.

4. Any use of computer for commercial or for-profit purposes is prohibited.

5. Extensive use of computers for personal activities is prohibited.

6. Antisocial behaviors (harassment, discriminatory remarks, etc.) are prohibited on the computer.

7. The computer will not be used to access internet sites or run programs that are offensive, illegal or otherwise not suitable or proper for use in the School.

8. Malicious use of the computer to develop programs that harass other users or infiltrate a computer and/or damage the software components of the computer is prohibited.

9. Use of computers to intentionally access or process files dangerous to the integrity of individual computers (i.e., viruses) is prohibited.

10. From time to time, VCA designees will make determinations as to whether specific uses of computers are consistent with use guidelines.

11. VCA personnel or designees reserve the right to remove user files without any notice.

12. VCA reserves the right to amend this Use

Policy.

13. VCA employees may be subject to disciplinary action for violation of the Use Guidelines. VCA will not provide legal assistance to any employee whom, in the process of violating the use guidelines, breaches local, state, or federal law.

14. All communications and information stored on computers and related cloud services, owned or operated by VCA, shall be considered property of the VCA.

STUDENTS' ACCEPTABLE USE PRACTICES FOR TECHNOLOGY AND WEB PUBLISHING

The term "technology," as used in this document, is intended to have a broad interpretation. "Technology" as used herein, means the computer itself along with all of the accessories and peripherals used in connection with the computer such as, but not limited to, the servers, backup drivers, backup disk, network servers, communication servers, modems, Internet access software, CD drives, printers, software, stored data, computer hardware, e-mail and any and all data and programs used on the computers. The term “computer” also includes any digital device such as a tablet, phone, iPod, or any other device that serves in this function or performs functions or activities which would typically occur on a traditional computing device.

All use of technology must be consistent with the mission of VCA. All users of the School’s technology resources will conduct themselves in accordance with any and all VCA guidelines, policies and procedures as well as applicable local, state, and federal laws governing the usage of technology and its component parts. Additionally, it is implied that students will use the School’s technology resources so as not to waste them, abuse them, interfere with or cause harm to other individuals, institutions, or companies. Administrators, the Technology Coordinator, and their designees will make determinations as to whether specific uses of technology are consistent with acceptable use policies. Students are responsible for their behavior while using School technology and shall comply with VCA standards.

STUDENT RULES FOR GENERAL USE

1. Students shall not use technology in violation of applicable local, state or federal laws and regulations.

2. Students shall adhere to all copyright regulations. The illegal installation or use of copyrighted software is prohibited and subject to criminal prosecution. The illegal installation of School-owned software on personal computers is also subject to criminal prosecution. The School must possess appropriate license(s) before copyrighted software may be installed or used. It is the responsibility of the user to determine that a license is available prior to attempting any software or data installation.

3. Students shall consider computer storage no differently than school lockers. In other words, authorized personnel may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on computers will always be private. VCA employees retain the right to inspect School-owned computer storage areas for any reason at any time without notice, without consent, and without a search warrant. Network administrators or their designees reserve the right to remove users' files without any notice.

4. Students shall use their accounts only as authorized by their teacher(s).

5. Students shall set unique passwords on all password-protected programs. Passwords to system resources are set automatically upon enrollment. Should a student's password become compromised, he or she should notify their Principal or other school authorities. Student passwords can be reset if compromised.

6. Students shall protect their login I.D. from others.

7. Students will be held responsible for activity on their account.

8. Students shall use only their authorized network account. Attempts to login as any other individual are prohibited.

9. Students shall not intentionally view, seek, obtain, or modify information, other data, or passwords belonging to other users.

10. Students shall not trespass in other users' folders or

files.

11. Students shall close programs and log out of unattended computers.

12. Students shall not use technology for any non-educational, commercial, or “for- profit” purposes.

13. Students shall not use technology or other means to disrupt the computer use of others.

14. Students shall not use technology maliciously to develop programs or process files (e.g. viruses or hacking) that harass other users, infiltrate computers, and/or damage the software components on or off school campus.

15. Students shall not use technology for illegal, offensive, or antisocial behaviors (harassment, discriminatory remarks, etc.).

16. Students shall notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

17. Students shall not waste or monopolize network resources (i.e. non-instructional use of gaming software, audio, video, locally or across the Internet.)

18. Students shall not modify technology devices or software in any way without the express permission of school administrators.

19. Students shall not attempt to disable or circumvent security measures including Internet filtering software.

20. Students shall not commit the School or employees of the School to any unauthorized financial obligation through the use of technology. Any resulting financial burden will remain with the user originating such obligations.

21. Students shall not intentionally harm, destroy, disable, or remove parts from computers or other technology devices. In such cases, students or their families may be held financially responsible for the repair, replacement, or reconfiguration of affected equipment.

INTERNET USE AND ELECTRONIC COMMUNICATIONS

Access to the Internet is provided for the purpose of supporting the curriculum. All students must have a signed acceptable use policy form on file, a signed parent/guardian permission form, and during the school day, the permission of their supervising faculty member in order to use the Internet. Students are restricted from establishing, accessing, or using web-based email accounts, chat, social media accounts, or messaging apps and accounts without the permission of a supervising faculty member. In addition, any such use must support the curriculum and may not be used for personal communication. Communications on the Internet are public in nature; therefore, general school rules for behavior and communications apply for all students using the Internet. In addition, students must refrain from inappropriate behavior that violates any laws or compromises their safety or that of others. Inappropriate behavior includes, but is not limited to the following:

- sending or willfully soliciting information including but not limited to hoaxes, chain letters, jokes, etc.;

- giving out personal information regarding oneself, others, or the school such as names, addresses, social security numbers, or phone numbers unless directed to do so by supervising faculty members;

- sending or willfully soliciting e-mail containing offensive, obscene, insulting, or harassing language or graphics;

- sending or intentionally receiving e-mail for political or personal gain;

- sending or intentionally receiving files dangerous to the integrity of the network;

- forging or attempting to forge email messages;

- sending or attempting to send anonymous email messages;

- attempting to read, delete, copy, or modify e-mail of other users;

- viewing any material that may not have been filtered, but would be classified as inappropriate for the school environment whether on the Internet or sent as an e-mail attachment or instant message; or

- making appointments to meet unknown individuals contacted via electronic communications.

DISCLAIMER AND OWNERSHIP

All email content is implicitly understood to be representative of the author's individual point of view and not that of VCA. All email generated using school-owned equipment or a school- assigned email account remains the property of VCA and may be reviewed and deleted as needed to ensure network integrity, confidentiality, and student safety.

WEB PUBLISHING

Students may be granted permission by School faculty to post to web pages, social media, or other sites which represent VCA for educational purposes. Students shall not provide information about VCA to parties that claim to represent VCA for web publication purposes on external servers. When posting materials to the web pages, social media, or other sites which represent VCA, students must adhere to the established design requirements. Authorized School personnel or designees reserve the right to remove unacceptable files or links from any official VCA website without notice. In addition, the School's website may not be used for: making profits, commercial purposes, or political gain; linking to external websites considered inappropriate by VCA standards as identified in the School Internet Safety Policy; posting student or employee photographs, names, or intellectual property without written consent from parent/guardian and/or individual; or posting inaccurate, derogatory, malicious, or threatening information or messages.

**Penalties for students who violate the Acceptable Use Practices will be commensurate with those outlined in the VCA disciplinary policy. Any student identified as a security risk or as having a history of such may have their access to technology resources restricted.

**VCA reserves the right to amend these Acceptable Use Practices as needed to comply with legal requirements and best practices.