Internet Acceptable Use and Safety Policy

a. **General**

Internet access and e-mail provided by NVCS are intended for educational use, instruction, research and the facilitation of communication, collaboration, and other school related purposes. Users are subject to the same standards expected in a classroom and/or professional workplace.

b. **Monitoring and Privacy**

Users have no right to privacy while using the school's internet systems. The school monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on school-provided devices, such as files, e-mails, cookies, and Internet history.

New Ventures reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law. The school will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the school's internet system.

c. **Prohibited Uses of the School's Internet Systems**

Users may not engage in any of the activities prohibited by this policy when using or accessing the school's internet systems.

If a user is uncertain whether behavior is prohibited, he or she should contact a teacher, supervisor or other appropriate school personnel. NVCS reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for the school, students, employees, network or computer resources, or (2) expend school resources on content the school determines lacks legitimate educational content or purpose, or (3) the school determines are inappropriate.

Below is a non-exhaustive list of examples of prohibited behavior:

1. **Causing harm to others, damage to their property or school property, such as:**

- Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, material posted online, or professional social media sites;
- Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent to school administration;
- Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
- Sending, posting, or otherwise distributing chain letters or engaging in spamming;
- Damaging computer equipment, files, or data in any way, including spreading computer viruses, vandalizing data, software or equipment, damaging or disabling others' electronic property, or engaging in conduct that could interfere or cause a danger of disruption to the school's educational or business environment;
- Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws. Any music, photographs and/or video should only be downloaded for school, and not personal purposes. If a work specifies how that work may be used, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright or trademark owner; or
- Engaging in plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

2. **Gaining or attempting to gain unauthorized access to the school's Internet Systems, or to any third party's computer system, such as:**

- Malicious tampering, phishing or hacking activities;
- Intentionally seeking information about passwords belonging to other users;
- Disclosing a user's password to other individuals. However, students may share their password with their parents.
- Modifying passwords belonging to other users;
- Attempting to log in through another person's account;
- Attempting to gain access to material that is blocked or filtered by the school;
- Accessing, copying, or modifying another user's files without authorization;
- Disguising a user's identity;
- Using the password or identifier of an account that does not belong to the user; or
- Engaging in uses that jeopardize access into others' accounts or other computer networks.

3. **Using the school's Internet Systems for commercial purposes, such as:**

- Using the Internet for personal financial gain;
- Conducting for-profit business activities, personal advertising, or other non-school business communications; or
- Using the school's Internet Systems on behalf of any elected official, candidate, candidates, slate of candidates or a political organization or committee.

4. **Engaging in criminal or other unlawful activities.**

d. **Filtering**

In accordance to Children's Internet Protection Act ("CIPA"), the school blocks or filters content over the Internet that the school considers inappropriate for minors. This includes pornography, obscene material, and other material that may be harmful to minors. The school may also block or filter other content deemed to be inappropriate, lacking educational or work-related content or that pose a threat to the network. The school may, in its discretion, disable such filtering for certain users for bona-fide research or other lawful educational or business purposes.

Users shall not use any website, application, or methods to bypass filtering of the network or perform any other unlawful activities.

e. **Protection of Personally Identifiable & Confidential Information**

The Family Educational Rights and Privacy Act ("FERPA") prohibits school officials from disclosing personally identifiable information ("PII") from education records of students and families to third parties without parental consent. However, several exceptions to this general rule may apply.

f. **Student Internet Safety**

1. **School Responsibilities:**

- New Ventures will provide curriculum about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.
- The school will work to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- As appropriate, the school will provide students, staff and parents with guidelines and instructions for student safety while using the Internet.

2. **Students Using the School's Internet Systems**

- Students must not reveal personal information about themselves or other persons on social networking sites, in chat rooms, in emails or other direct electronic communications, or any other forum over the Internet. For example, students must not reveal their home address, or telephone or cell phone number. Students must not display photographs of themselves, or the images of others.
- Students should not meet in person anyone they have met only on the Internet. Students must promptly disclose to their teacher or other school employee any message or other activity they receive that is inappropriate or makes them feel uncomfortable.
- Students should not allow school's computers to save their passwords.

3. **Parents**:

- Although students generally will be supervised when using the school's Internet System during the school day, it is not practicable for the school to monitor and enforce a wide

range of social values in student use of the Internet. Parents are primarily responsible for transmitting their particular set of family values to their children, and discussing with their children what material is and is not acceptable for their children to access.

- Parents are exclusively responsible for monitoring their children's use of the Internet when the school's Internet Systems are accessed from home or a non-school location.

g. **Violations of this Policy**

New Ventures Charter School reserves the right to terminate any user's access to the school's Internet Systems at any time.

If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline Code. If a student's access to the school's Internet System is revoked, the student may not be penalized academically, and the school will ensure that the student continues to have a meaningful opportunity to participate in the educational program.

All users must promptly disclose to their teacher, or principal any information they receive that is inappropriate or makes them feel uncomfortable.

a. **Limitation of Liability**

The school makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the school's network are to be borne by the user. The school also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the school or employees.

I have read and agree to comply with the New Ventures Internet Use and Safety Policy.

_____ _____

Student Name Student Signature

_____ _____

Parent Name Parent Signature

Date _____ Date _____