Computer and Network Resources Responsible Use Policy

Academy Technology Services (ATS) supports Milton student, faculty and staff access to the School's computer and network resources. To ensure that these resources are available to all members of the community, and to protect the School's computer and network systems, all users must agree to and comply with the terms of the Milton Academy Computer and Network Resources Responsible Use Policy. This policy is grounded in the fundamental "Complete Integrity" principle, listed in the Standards section of the *Handbook*, and reflects the School's commitment to the open expression of ideas and respect for the ideas and creations of others.

The School's computer and network resources exist to support educational goals and related activities. All use of computer and network resources must be consistent with these goals and must conform to standards that the School sets for student behavior. Use of network resources, computers, and other devices, whether School-owned or student-owned, may be monitored by the School's faculty and staff, and there should be no expectation of privacy. Student email accounts, hard drives, network and Google Drive storage, Internet activity and system logs may be searched at any time at the School's discretion.

Community Standards

1. It is expected that all users will communicate in ways that respect others, regardless of medium. This includes written and video modalities. All users represent Milton Academy, both on- and off-campus, and must be mindful of how their words and actions may impact others.
2. As we embark on a period of remote learning, users are reminded to be mindful of conduct and expressions communicated through video communication and collaboration tools. Faculty, staff and students must adhere to community and behavioral standards as though interactions were occurring in person.

Security

1. Passwords for computer and network resources are private to each individual; they uniquely identify a person as well as identify a person to others. You are responsible for all use made of your Google and Schoology accounts, network storage or Internet access. You may not allow anyone to use your identity to access any computer or network resource and you must diligently guard your password(s). Using another person's password, or attempting to discover it, is an integrity violation and may be regarded as theft. Should you discover someone's password accidentally, you must notify the person immediately so that it may be changed.
2. Masquerading as another person, concealing your identity, or sending anonymous messages violates the School's expectation of honest and open communication. You may not take steps to hide or misrepresent your identity when using School accounts, computers, networks or services.

In any situation that threatens system security, stability, integrity or performance, ATS system administrators will take necessary action to defend computer and network resources. These defense measures may include terminating or suspending computer processes, deleting files or disabling user accounts without advance notice. A threatening situation may or may not involve deliberate user misconduct. ATS will notify affected users as soon as possible.

Network Connectivity

1. Any computer connected to the School's network must be running a School-supported version of the operating system. Supported operating systems include Chrome OS, Windows 10 or higher, and MacOS

10.10 or higher.

2. Disconnecting or moving School-owned computing equipment (including devices, monitors, wireless access points, and cables) interferes with the ability of others to use this equipment, and is prohibited unless done so in agreement with ATS. When working on School-owned computers, you may not delete, modify or add to installed software or hardware, preference files or other configurations.
3. You may not knowingly or carelessly perform any act that interferes with the normal operation or performance of computers, printers, terminals, servers, peripherals or networks.
4. Students are not allowed to attach any switch, hub or router to the School's wired or wireless networks, unless the device was obtained from ATS.

   Unmanaged wireless access points pose a security threat to the network as a whole and you are not permitted to run a wireless access point, be it stand-alone or integrated within your computer.

   You may use only the Internet Protocol (IP) address assigned to your computer or device by the School's DHCP server. Under no conditions may you manually assign your computer's or device's IP address.
5. Network services may not be run on personal computers without the explicit approval of ATS. This includes, but is not limited to, Web servers, DHCP servers, FTP servers, and external peer-to-peer file-sharing services. Under no circumstances may you use network monitoring or packet-capture software.

Use of Milton's Network

1. The use, storage or sharing of illegally copied or stolen software or digital materials (e.g., MP3, video, text and image files) is theft, violates copyright and other intellectual property laws, and is prohibited. The School takes violations of intellectual property law seriously. We must all respect the laws that govern and protect creators of intellectual content.
2. The School employs proxy and Web filtering to restrict access to World Wide Web sites whose content may be inappropriate for this academic community. Examples of inappropriate content include sites promoting pornography, violence, drugs, smoking, gambling and hate. Access to the Web is monitored, and students should have no expectation of privacy in their online activities. Students accessing the Internet through the School's wired or wireless networks may not attempt to bypass or thwart security, filtering, or proxy services operated by the School, including, but not limited to the use of anonymous VPNs. Students who, for academic reasons, need to access restricted Web sites may submit a request to ATS through the page block screen.
3. You may not use computer or network resources to send harassing, bullying, offensive, or obscene content. Remember that you are responsible for the effect that your message may have on another person. Any messages, photos or other media distributed or posted in a digital format will be treated as if they were permanent and public. Many campus organizations sponsor open discussions in Schoology. These pages must be used in accordance with the guidelines published here.
4. The School's computer and network resources may not be used for commercial or illegal activity or to gain unauthorized access to any computer or network system.
5. You are responsible for any material that is stored on your computer or School-issued accounts (e.g., Gmail, M-drive and Google Drive).
6. You must respect and preserve the privacy of others at Milton.

Any abuse of the above policies and regulations may result in the suspension of privileges and/or disciplinary action.