TECHNOLOGY ACCEPTABLE USE POLICY

Worcester Preparatory School (Worcester) offers Internet and network access to its students, faculty, and staff. Access to the school network and the Internet service is a privilege not a right. The intent of this policy is to ensure that users utilize this access in a manner consistent with the mission of Worcester. Parents and guardians are asked to review this policy and discuss it with their children.

Internet use provides valuable opportunities for research, curriculum support, and career development. The primary purpose of the Worcester Internet service is to support the educational objectives of the school. Worcester's Internet service is not a public forum. Worcester reserves the right to place limits on materials posted or accessed through Worcester's Internet service. While Worcester's intent is to make Internet access available to further educational goals and objectives, users may find ways to access other materials as well. Filtering software is in use, but no filtering system is capable of blocking 100% of the inappropriate material available online. Worcester believes that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.
To use Worcester's Internet service and network, users must take full responsibility for their actions. Worcester shall not be liable for the actions of anyone accessing the Internet through this or any other Internet connection. Users assume full responsibility for any costs, liabilities, or damages arising from the way users choose to use their access to Worcester's Internet service or network.

Network Usage Guidelines
All use of the Worcester network must be consistent with the purpose as stated above. This policy does not attempt to articulate behaviors by users of this network. In any specific situation Worcester relies upon each individual's judgment of appropriate conduct. To assist in such judgment, the following general guidelines are offered.
Users are expected to abide by the generally accepted rules of network etiquette, which include, but are not limited to:

- Do not reveal personal information about oneself or any others such as last names, addresses, phone numbers, photos, etc. that could identify the user or other individuals. You must immediately disclose to a teacher or administrator any message you receive arrangements to meet with anyone that he/she has met on Worcester's Internet or network.
- Do not use the network in such a way as to disrupt its use by others.
- Refrain from making defamatory remarks, sexual or racial slurs, and from using obscene or profane language.
- Do not use the network to harass, offend, or bully. Bullying or harassment that offends others is unacceptable. Action that results in serious emotional distress or places someone in fear of bodily injury or death is a criminal offense.
- Internet IDs and passwords are provided for each user's personal use only. Passwords should not be revealed or shared with anyone. Users must not use another person's password. If you suspect that someone has discovered your password, you should change it immediately. The account owner is responsible for all activity under that account. It is imperative that all users keep their passwords secret so that no one else can use their account
- Any use for, or in support of, illegal purposes or activities is prohibited. This includes, but is not limited to gaining unauthorized access to other systems (computer hacking), arranging for the sale or purchase of drugs or alcohol, participating in criminal activity of any kind, threatening others, transferring obscene material or attempting to do any of the above.
- Any use for commercial or non-school related purposes is prohibited. Users may not create web pages or other ways to advertise or sell products or services or to promote political, religious or other non-school related causes. Users may not offer, provide, or purchase products or services through the Worcester network. This does not include school-approved activities.
- Users should assume that all materials available on the Internet are protected by copyright. Users shall not copy and forward, copy and download, or copy and upload any copyrighted material without prior approval of the supervising teacher or an administrator. Any material obtained from

the Internet and included in one's own work must be cited and credited by name or by electronic address or path on the Internet Information obtained through email or news sources must also be credited as to sources. Worcester and its network make no guarantees, implied or otherwise, regarding the factual reliability of data collected through the Internet

- Not all material accessible through the Internet is of educational value. Students are expected to refrain from seeking, accessing, or downloading material that is not relevant to their assignments or coursework. No students may upload or download material to or from Internet sites without permission from his/her teacher. Students must not access chat rooms. Games must not be played, accessed or downloaded unless they are approved by a teacher or administrator. The Worcester network will take reasonable precautions to filter out controversial materials. However, it is impossible to monitor all materials and controversial information.
- Users shall neither download nor install any commercial software, shareware, or freeware onto network drives or disks without prior permission from a teacher or school administrator. Users shall not change settings on the browser or any other application.
- Users shall not upload, download, or distribute pornographic, obscene, sexually explicit or threatening material of any nature. Users shall not upload, download, or distribute visual and/or audio depictions that are obscene, child pornography, or (in the case of use by minors) harmful to minors.
- Users shall not receive or transmit information pertaining to dangerous instruments such as bombs or other explosive devices, automatic weapons or other weaponry.
- Users must not attempt to get unauthorized access to any file servers on Worcester's network, outside file servers, or go beyond the user's authorized access. This includes logging in through another person's account accessing another person's files, or attempting to do either. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Users must not vandalize school computers by causing physical damage, reconfiguring the computer system, attempting to disrupt the computer system, or destroying data by spreading computer viruses by any other means.
- Users shall make every effort to safeguard the Worcester network from computer viruses. Users should never download files from the Internet, accept email attachments from outsiders, or use disks from non-Worcester sources, without first scanning the material with Worcester-approved virus checking software. If you suspect that a virus has been introduced into the Worcester network, notify the Technology Department immediately.

Ownership Information

The Worcester network is owned and maintained by the school. Worcester reserves the absolute right in its discretion, to delete, wipe, shred, or otherwise dispose of any information or other aspects of the electronic systems, from time to time, whether as a part of its information retention policy, routine maintenance, or otherwise. By using the Worcester network, users consent to all monitoring, access and disclosure by Worcester and acknowledge Worcester’s right to dispose of information in its discretion.

Longevity of Information Storage

Users should be aware that email or other electronic content may not be fully deleted from the Worcester network even if that information is "deleted" from an individual device. Records of electronic communications and electronically created documents may remain on the Worcester network. As a practical matter, Users should never create any electronic communication or document that they would not want to be retained for posterity or monitored, accessed, and/or disclosed by Worcester.

Privacy

Users should not have an expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on Worcester's network or stored by the user. Network storage areas are treated like school lockers and may be inspected at any time. Worcester reserves the right to examine all data stored on removable drives involved in the user's use of Worcester's

network. Internet messages are public communication and are not private. All communications including text and images may be disclosed to law enforcement or other third parties without prior consent of the sender or the receivers. School administrators may review communications to maintain integrity system-wide and ensure that users are using the system in a responsible manner. Worcester reserves the right to monitor the online activities of all users. Electronic mail messages are backed up and may be inspected by appropriate school administrators. Worcester reserves the right to inspect electronic mail and computer-generated logs regarding web sites visited by users that the school deems necessary and appropriate to ensure proper use of resources and to conduct routine network maintenance.

Violations
Worcester reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from the school, for violations of this policy. Additionally, all regulations in the Worcester Handbook for Students & Parents apply to use of Worcester's network. Worcester will advise appropriate law enforcement agencies of illegal activities conducted through the school's network and will cooperate fully with local, state and/or federal officials in any investigation related to any illegal activities conducted through the Worcester's Network.

General Guidelines for Mobile Device Use
It is Worcester's goal to promote educational excellence for the 21st Century Learner by facilitating resource sharing, innovation, research, creativity, communication, increased productivity, mobile learning, and differentiated instruction. Individual use of mobile devices is a way to empower students to maximize their full potential and to prepare them for college and the workplace. Use of mobile technologies is a privilege that carries responsibility and behavioral expectations, including but not limited to those already stated in the Handbook for Students & Parents and the Technology Acceptable Use Policy. It is understood that all members of the Worcester community will use all available technological devices and the school's network in a responsible, ethical and legal manner.

The term mobile device in this policy denotes mobile phones, laptops, iPod touches, tablets such as an iPad or Android OS device or any mobile device that can access the Worcester Network. Students and their parents or guardians must read and sign the Acceptable Use Policy before students are given permission to bring mobile devices to school. The Acceptable Use Policy also applies to students during school excursions, camps and extra-curricular activities. It is the responsibility of students who bring mobile devices to school to abide by the guidelines outlined in this document. Permission to have a mobile device at school while under the school's supervision is contingent on parent/guardian permission in the form of a signed copy of this policy. In the event a mobile device is brought to school without a signed agreement by the parent, the student (by the fact of bringing the device onto campus) implies agreement to accept the rules governing mobile devices.

Responsibility for digital devices rests with the student and Worcester accepts no financial responsibility for damage, loss or theft. Students in Grades 6-12 must keep digital devices, except those required for classroom use, locked in their lockers. Students in Grades 3-5 who use iPads in their classrooms must leave them in their classrooms during lunch, special periods, etc. (Teachers will keep classroom doors locked in order to secure items in classrooms.)

Cell phone/smart phones must be turned off. Students in Grades 6-12 must keep phones locked in lockers. Students in the Lower School who bring phones to school must turn them off and keep them in their backpacks. (Teachers will lock doors during lunch, special periods, etc.) Digital phones may not be used during the school day.
Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients is strictly prohibited. This includes but not limited to use of email, messaging, Twitter, Facebook, and other social media and communication technologies.
Use of cameras and microphones are strictly prohibited in the classrooms and hallways unless permission is granted by a teacher. Students must use good judgment; students agree that cameras will not be used to

take inappropriate, illicit or sexually explicit photographs or videos, nor will they be used to embarrass anyone in any way.

Any use of cameras in restrooms or the locker room, regardless of intent, is strictly prohibited. Students may not engage in personal attacks, harass another person, or post private information about another person.

Students using mobile devices to bully other students will face disciplinary action. (It is a criminal offence to use a device or phone to menace, harass or offend another person.
File Storage on the network, Internet DropBox, or other storage area from personal mobile devices is limited to schoolwork only. Anything not directly related to schoolwork may be removed by the Technology Department or a school administrator.

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal Information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission. If users see a message, comment, image, or anything else online that makes them concerned for their personal safety or the safety of others, this must be brought to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.