

Appendix 4

INTERNET USAGE POLICY

The use of technology is a privilege and an important part of the School's overall curriculum. The School will, from time to time, make determinations on whether specific uses of technology are consistent with School policies for students and employees of the School but does not warrant that the technology resources will meet any specific requirements of the student or other users, or that it will be error free or uninterrupted. The School always reserves the right to monitor and log technology use, to monitor file server space utilization by users, and examine specific network usage (as may be deemed necessary) for maintenance, safety or security of the technology resources, or the safety of the user.

It is the policy of the School to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity and damage to school resources; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1)(B).

I. ACCESS TO INAPPROPRIATE MATERIAL

To the extent practicable, technology protection measures (or "Internet filters") are used to block or filter Internet access to, or other forms of electronic communications containing, inappropriate information. Filtering, or blocking, is applied to visual depictions of material deemed obscene, child pornography, or to any material deemed harmful to minors, as defined by the Children's Internet Protection Act. The filter serves to block minors from accessing inappropriate material on the Internet and the World Wide Web.

The technology protection measures may be disabled only for bona fide research or other lawful purposes. Disabling technology protection shall only be performed by a member of the Operator's Information Technology Team or its designated representatives.

Additionally, it shall be the responsibility of all members of the staff to supervise and monitor usage of the online computer network and access to the Internet and ensure that the same is in accordance with this policy. By using the filter program as well as staff monitoring student use, the School is attempting to provide a safe and secure medium by which students can use the Internet, World Wide Web, electronic mail, chat rooms, and other forms of direct electronic communications.

To the extent reasonable, steps are taken to promote the safety and security of users of the School's online computer network. Other inappropriate network usage that the School intends to eliminate includes:

- Unauthorized access, including so-called 'hacking' and other unlawful activities; and
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

By signing the Parent/Student Contract Page at the end of the Parent/Student Handbook, the parent and student agree:

- To abide by all School policies relating to the use of technology;
- To release all School employees from any and all claims of any nature arising from the use or inability to use the technology;

Appendix 4

- That the use of technology is a privilege; and
- That use of the technology will be monitored and there is no expectation of privacy whatsoever in any use of the technology.

The parent/student further agrees and understands that the user may have his/her privileges revoked or other disciplinary actions taken against him/her for actions and/or misuse such as, but not limited to, the following:

- Altering system technology, including but not limited to, software or hardware;
- Placing unauthorized information, computer viruses or harmful programs on or through the computer system in either public or private files or messages;
- Obtaining, viewing, downloading, transmitting, disseminating or otherwise gaining access to or disclosing materials the School believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable;
- Using technology resources for commercial, political, or other unauthorized purposes since the School technology resources are intended only for educational use;
- Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users;
- Disrupting technology through abuse of the technology, including but not limited to, hardware or software;
- Malicious uses of technology through hate mail, harassment, profanity, vulgar statements, or discriminating remarks;
- Interfering with others' use of technology;
- Installation of software without consent of the School;
- Allowing anyone else to use an account other than the account holder; and
- Other unlawful or inappropriate behavior.

The user also acknowledges and agrees that he/she is solely responsible for the use of his/her accounts, passwords, and/or access privileges, and that misuse of such may result in appropriate disciplinary actions (including but not limited to suspension or expulsion), loss of access privileges, and/or appropriate legal action.

The user must also know and further agrees that:

- Should the user transfer a file, shareware, or software that infects the technology resources with a virus and causes damage, the user will be liable for any and all repair costs;
- The user will be liable to pay the cost or fee of any file, shareware, or software transferred or downloaded, whether intentional or accidental;
- Should the user intentionally destroy information or equipment that causes damage to technology resources, the user(s) will be liable for any and all costs; and
- Violation of this Internet Safety Policy is also a violation of the School Code of Conduct and may result in any in other scholastic disciplinary action, other than those specifically set forth above, including but not limited to suspension or expulsion.

II. DEFINITIONS

For purposes of this Policy:

A "minor" is anyone under the age of 18.

"Harmful to minors" means any picture, image, graphic image file or other visual depiction that: (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity or sex; (b) depicts,

Appendix 4

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 (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

“Technology Protection Measure” means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in Section 1460 of Title 18 of the United States Code;
2. Child Pornography, as that term is defined in Section 1226 of Title 18 of the United States Code; or
3. “Harmful to minors.”

“Sexual act” and “sexual contact” have the meanings given such terms in Section 2246 of Title 18 of the United States Code.