Network and Technology Acceptable Use Agreement

Students have access to the Brentwood School network, a comprehensive technological tool that provides them with vast resources intended to expand their educational horizons. The network includes a variety of computer programs, databases, and Internet searching capability. Access to these resources includes material that has no educational value in a school setting. These guidelines are provided to apprise students of their responsibilities when logging onto the network. If a student violates any of these provisions, access may be limited or denied. Please read the terms and conditions listed below and make certain you understand them.

RESPONSIBILITY

Access to the Brentwood School network is a privilege, not a right.

Students must behave responsibly while using school computers and should remember that network communication is not private.

Students, faculty, and staff will not use technology to record another member of the community without the person's consent.

Parents should understand that they are ultimately responsible for their child's actions and should take time to read this policy and discuss it with their child/ren.

Students are responsible for immediately reporting security or network vulnerabilities they encounter (including viruses, hackers, and spyware).

RIGHTS AND PRIVILEGES

Network services are provided for educational communication, research, and other activities. Access to the Brentwood School network will be provided to students who act in a considerate and responsible manner.

A network account will include a user name and private password, which must not be shared with others except as requested by school administration. In some cases, the system administrator may issue a limited "class" account to groups of students, which may be used temporarily for specific purposes.

Each student or "class" with network access will be assigned storage space on the corresponding file servers, which may be treated like school lockers. Students should have no expectation of privacy in any information stored in their assigned storage space.

Network security is designed to allow access to these spaces only by the assigned user; however, network administrators may review files and communications to maintain system integrity and to ensure that users are using the system responsibly.

Users should not expect that emails, messages, files, information or anything else stored on the network will be private. This includes personal email, content posted on social networking sites and other data stored or transmitted using the school's resources. Our staff may monitor such items at any time with or without notice, for any reason.

RESTRICTIONS

The following activities are not permitted while using the school's technology or network resources:

- Violating a copyright or otherwise using another person's intellectual property without prior approval or proper citation; using another person's password; accessing another person's folders, work, or files
- Families are not permitted to use the school's logo, trademarks, official photographs, or any other intellectual property or proprietary materials in any way without the written consent of the Director of Communications
- Accessing, uploading, downloading, transmitting, displaying, or distributing obscene or sexually explicit material; transmitting obscene, abusive, or sexually explicit language
- Damaging computers, computer systems, or computer networks; vandalizing, damaging, or disabling the property of another person or organization; debilitating or disabling computers, systems, or networks through the intentional misuse or overuse of electronic distribution or the spreading of computer "viruses" through the inappropriate use of files
- Violating any local, state, or federal law
- Sending an abusive, cruel, threatening, obscene, sexually explicit, anonymous message or photo/image to another member of our school community (whether from the school's network or using a personal device and/or personal resource)
- Engaging in harassing or intimidating public or private messages or cyberbullying (i.e. being cruel to others through electronic means by sending or posting harmful materials using the internet or other electronic means)
- Email shall not be used, or access provided for use, for commercial and related purposes, or to communicate inappropriate materials or messages contrary to

school policy as defined in Family Handbooks. This email policy prohibits the transmittal of copyrighted or proprietary information without the appropriate authorization of the owner

- Falsifying permission, authorization or identification documents
- Intentionally impersonating another person for an illegal or improper purpose
- Using the network to disrupt the use of the net-work by other users
- For students, revealing your personal address or telephone number or for parents and students, revealing the address or telephone number of any member of the school community
- Any action that would damage, impair or disrupt the function of the school's network, computer systems, software, data, or files
- Operation of any unauthorized server or service that makes high demands on the network

DISCLAIMERS

Brentwood School makes no warranties of any kind, either expressed or implied, for the access being provided.

The staff and the school are not responsible for any damages, including without limitation loss of data resulting from delays or interruption of service, loss of data stored on Brentwood School resources, or for damage to personal property used to access Brentwood School resources.

Brentwood School will not be responsible for the accuracy, nature, or quality of information stored on Brentwood School resources or gathered through school-provided access.

Brentwood School does not filter or censor Middle or Upper School students' use of the Internet, and students are personally responsible for their own use.

SANCTIONS

Violation of this policy will be subject to disciplinary action, which may include loss of access to electronic resources, suspension, or expulsion.

Users will be financially responsible for damages resulting from improper use of the Brentwood School network and technology.

When appropriate, law enforcement agencies may be involved.

SOCIAL NETWORKING GUIDELINES

Brentwood School strongly encourages members of the community to follow the guidelines below when blogging and/or participating in social media platforms:

- Pay attention to each site's "terms of use" and privacy policies
- Adhere to any minimum age requirements of social networking sites. Social networking platforms stipulate minimum age requirements (usually 13 years) for their members.
- Always consider your digital footprint—any information distributed using digital technologies (including pictures, text messages, email, etc.) could be available to others to access and use without your knowledge or permission
- Seek approval from other parents before posting photos or video of students and use discretion when selecting those images
- Do not use full names of Brentwood School students. Our naming protocol is First Name, Last Initial.
- For parents/guardians, refrain from "friending" students as some personal content may be inappropriate for their viewing
- Monitor your child's use of blogs and other social networking sites to ensure that they follow Internet safety best practices

SOCIAL NETWORKING AT BRENTWOOD SCHOOL

Brentwood School parents, students, administration, faculty, and staff are encouraged to use school-provided tools for communication and networking. Brentwood School administration, faculty, and staff are strongly discouraged from "friending" parents of current or prospective students due to the inherent conflicts of interest that may arise. They may not initiate or accept social media "friend" requests from current students (of any age) or former students under the age of 18. Administration, faculty, and staff are encouraged to use professional discretion when "friending" alumni 18 years of age and older. When doing so, they must recognize that many former students have online connections with current students including younger siblings and underclassmen friends, and that the information shared between recent alumni is likely to be seen by current students as well.