Brunswick School

COURAGE ♦ HONOR ♦ TRUTH

ACCEPTABLE USE POLICY FOR ELECTRONIC RESOURCES

1. Introduction

Brunswick School provides access to electronic resources, including the Internet, Intranet, email and network computing to authorized users (students, faculty and staff) for educational, research and administrative purposes. These resources are provided to promote educational excellence by facilitating communication, resource sharing and innovation. This acceptable use policy governs the use of all such electronic resources by our community.

The use of Brunswick's I.T. resources is a privilege, not a right, granted to users primarily for the enhancement of curricular-related learning or job functions. Users may have limited access to Brunswick's email, network and Internet for minimal personal use. Brunswick's email, voicemail or electronic equipment, including Internet access, should not be used for communications that are inconsistent with the mission of the school or what it stands for.

Violations of this policy will result in revocation of this privilege. Depending upon the severity of the infraction, users will face disciplinary action up to and including dismissal, civil litigation, and/or criminal prosecution for misuse of these resources.

Brunswick School does not attempt to articulate all possible violations of this policy. In general, users are expected to use Brunswick's electronic resources and networks in a responsible, ethical, and professional manner.

2. Authorization

Brunswick School's I.T Department allocates unique usernames and passwords to each authorized user to access internal computing and communication resources. The user is personally responsible and accountable for all activities carried out under his/her username. The password associated with a personal username must not be divulged to another person, except to members of I.T. staff who may require it for troubleshooting purposes. No one may use, or attempt to use, computing resources allocated to another person, except when authorized by the provider of those resources.

All users must correctly identify themselves on the school's email and computing network at all times. A user must not masquerade as another, withhold his/her identity or tamper with audit trails. A user should take all reasonable precautions to protect their resources. Passwords should be changed frequently and adhere to strong encryption standards.

3. Privacy

It should be noted that authorized Brunswick I.T. staff have the ability to access all user files, including email stored on central servers and data on individual computers as well as on the network that they manage.

Brunswick School reserves the right to review, audit, intercept, access, and disclose any and all data stored on Brunswick School computers, servers, and email systems, as security considerations warrant, with or without notice, during or after working hours. The use of a password by a user does not restrict Brunswick's legal right to access electronic communications.

While Brunswick does not routinely monitor or censor electronic communications, users of its electronic resources should have no expectation of privacy in their email, data files or on their Internet usage. Accordingly, all users must ensure that their electronic communications are appropriate, lawful, and in compliance with the provisions of this policy. As a condition of use of these resources, users agree to Brunswick School's review and disclosure of email and Internet records, if a security situation so warrants.

4. Definition of Acceptable and Unacceptable Usage

In general, unacceptable use of Brunswick computer, network and communication resources may be summarized as:

- Access, propagation, retention or printing of material that is offensive, obscene, indecent or poses a safety risk.
- Intellectual property rights infringement, including copyright, trademark, patent or designs.
- Unsolicited advertising or "spamming".
- Attempts to break into or damage computer systems or data held thereon.
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorized.

The following activities, while not exclusive, are specific examples of unacceptable uses that will be considered violations of this policy:

- Engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in our local jurisdiction.
- Communications that ridicule, disparage, or criticize a person, a group of people, or an organization based upon race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs are strictly prohibited.
- Send, receive, or display communications that demean, threaten, insult, harass, disparage or defame anyone, or diminish workplace productivity and/or professionalism.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including the installation or distribution of "pirated" software that is not appropriately licensed for use by Brunswick School.
- Unauthorized copying of copyrighted material through digitization and distribution, such as photographs from magazines, books, or other sources, incl. copyrighted music.
- Accessing data, a server or an account for any purpose other than conducting school business, even if you have authorized access, is prohibited.

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- **Executing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. For purposes of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.**
- Introduction of malicious programs into the network or servers - e.g., viruses, worms, Trojan horses, e-mail bombs, etc.
- Port scanning or security scanning of our network assets is expressly prohibited.
- Any form of network monitoring which will intercept data not intended for the user.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on our network.
- Interfering with or denying service to any user for any purpose.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via the Internet/Intranet/Extranet.
- Solicit, endorse, or proselytize others for commercial ventures, outside organizations, or religious, social, or political causes.
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Recreational activities generating heavy network traffic, such as streaming music or video, shopping or visiting sport sites during work hours, especially activities that interfere with others' legitimate use of I.T. services, or which incur a financial cost to the school in terms of provisioning additional bandwidth.
- Frivolous or excessive personal use of Brunswick owned electronic equipment.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use or transmission of academic mailing lists for non-academic purposes.
- Downloading or installing software applications of any kind, including games, on school owned hardware, without express permission of the I.T. Dept.
- Using the school's 3-D Printers to "print" any weapon, such as a knife or gun, is expressly forbidden, as is printing of offensive/obscene material on the school's networked printers
- Posting anonymous messages or attributing one's messages to another individual.
- Disseminating confidential information of Brunswick School's or personal contact information of employees of Brunswick School without their consent.

Note: Faculty and students may only communicate with each other online via the school's email system or Google Classroom. No other digital modes of communication are permissible, including social media sites like Facebook, Twitter and Instagram, or texting on mobile devices.

It should also be noted that individuals may be held responsible for the retention of explicit or offensive attachments that they have received via email that they have read.

Acceptable uses include: Personal email and reasonable recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others. However, such use must be regarded as a privilege and not as a right and may be withdrawn if abused or the user may be subject to a disciplinary procedure.

Commercial work for external entities, using Brunswick's computing and communication resources requires explicit permission from the Head of School; such use may be liable to a charge.

5. Licenses and Copyrights

Brunswick's computing systems, the data saved on them, and any additions and modifications to them developed by the school's employees, shall remain the school's exclusive property. Any hardware, software and documentation owned by Brunswick School may not be sold, transferred, reproduced or used for purposes not reasonably related to Brunswick's mission. Licenses and copyrights exist for all software used by Brunswick School. Employees and students are prohibited from violating any licensing agreements or copyrights.

6. Coverage

Users should remember that this policy is not exhaustive and inevitably new social and technical developments will lead to further uses that are not fully covered. In case of any doubt, users should address questions concerning what is acceptable to the Head of School or Director of I.T.