The Bryn Mawr School

Acceptable Use Policy 2019-2020

Lower, Middle and Upper School Students and Parents/Legal Guardians

PURPOSE

This policy defines the activities that are permissible when using any Bryn Mawr School computer and communications systems. This policy aims to ensure the prudent and appropriate use of Bryn Mawr’s computing network and resources.

SCOPE

This policy applies to all Lower, Middle, and Upper school students and their parents/legal guardians when using computers, internet access, or online services provided by Bryn Mawr. It is a privilege to have access to the Bryn Mawr network and computing resources. This policy is applicable whether or not it is during school hours, and whether or not the usage occurs on the Bryn Mawr School campus.

POLICY

User IDs and Passwords

Personal User IDs and Accounts — Responsibility – Each User must be responsible for all uses and contents of her account and activity performed with their personal User IDs. They must not permit others to perform any activity with their User IDs, and they must not perform any activity with IDs belonging to other Users. Access Code Sharing - Bryn Mawr School computer accounts, User IDs, network Passwords, and other access codes must not be used by anyone other than the person to whom they were originally issued. Encryption On Portable Computers, Mobile Devices, And Smart Phones - Users should not store clear-text authentication credentials on portable computers, mobile devices or smart phones. These credentials should never be stored anywhere on these devices unless they are in encrypted form. Typing Passwords When Others Are Watching - Users must never type their Passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access. Suspected Password Disclosure - Each User must immediately change his or her Password if the Password is suspected of being disclosed, or known to have been disclosed to an
Unauthorized party. **Password Proximity to Access Devices** - Users must never write down or otherwise record a readable Password and store it near the access device to which it pertains. **Passwords in Communications Software** - Users must not store Passwords in Internet browsers or related data communications software at any time.

### Electronic Messaging

**Reasonable Personal Use of Computer and Communications Systems** - Bryn Mawr School allows computer Users to make limited personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards of ethical and polite conduct. **Electronic Mail Contracts** - All Users must include a notice at the end of each electronic mail message indicating that the message does not bind Bryn Mawr School to any contract, position, or course of action unless the User is specifically authorized to enter into contracts on behalf of Bryn Mawr School, or otherwise authorized to legally represent Bryn Mawr School. **Offensive Electronic Mail Messages** - Users must not respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, Users must report the communications to the correct department. **Sending Unsolicited Electronic Mail** - Users must not send uninvited or unsolicited electronic mail to a large number of recipients. This includes commercial advertisements, charitable solicitations, questionnaires/surveys, chain letters, and political statements. **Identity Misrepresentation** - Users must not misrepresent, obscure, suppress, or replace their own or another person’s identity on any Bryn Mawr School electronic communications.

### Internet and Intranet

**Internet Information Modifications** - Users connecting to Bryn Mawr School systems through the Internet can only modify their personal information. **Internet Software Downloads** - End-users may download and use any software from the Internet on Bryn Mawr School computers as long as it is for educational purposes only. **Internet Discussion Groups** - Users must not post to controversial discussion groups on the Internet or to any other controversial online public forums when using their Bryn Mawr School User IDs. Users may use their Bryn Mawr School User IDs when posting to school related discussion groups. **Personal Internet Message Disclaimers** - Whenever a User posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message should be accompanied by words clearly indicating that the comments do not necessarily represent the official position of Bryn Mawr School. **Internet Product and Service Representations** - Users must not advertise, promote, present, or otherwise make statements about Bryn Mawr School products and services in Internet forums such as mailing lists, news groups, or chat sessions.
without the prior approval of the Communications Office. **Public Electronic Forums** - Users use Bryn Mawr School information systems to participate in Internet discussion groups, chat rooms, or other public electronic forums. **Appropriate Communications** – Communications must be made in ways that are kind and respectful. Publishing or re-publishing statements or materials that defame, harass, abuse, stalk, threaten, or infringe on the rights of others. This includes material that contain vulgar, obscene, profane, or otherwise objectionable language or images.

**Personal Internet Service Provider Accounts** - Users who wish to make a statement in a public Internet forum about any topic that does not involve Bryn Mawr School educational, or Bryn Mawr School educational interests, must use their own personal Internet service provider accounts to submit such statements. **Access to Social Networking Sites Prohibited** - Users may access Social Networking sites using Bryn Mawr School computers or personal computers connected to Bryn Mawr School networks. Access to Social Networking Sites should be for educational purposes. **Bryn Mawr School Information Not Posted on Social Networking Sites** – Posting or online use of The Bryn Mawr School proprietary information is prohibited. **After Hours Web Shopping and Auction Educational** - To ensure that network bandwidth is not consumed for personal purposes, Bryn Mawr School prohibits personal web shopping and personal involvement in any on-line auctions during regular educational hours. **Personal Use of Internet** - Use of Bryn Mawr School information systems to access the Internet is limited for personal purposes. **Internet Connection Approval** - Users must not establish any external network connections that could permit non-Bryn Mawr School Users to gain access to Bryn Mawr School systems and information, unless prior approval of the Information Systems Department has first been obtained. **Large Internet Downloads** - Internet Users may use video streaming facilities, audio streaming facilities, or download large graphics files as long as it does not overburden the network. **Machines Connected Only to Internal LAN or Intranet** - Users must use caution when connecting to any external network, especially with public external networks. **Sensitive Information Not Accessed from Public Terminals** - Students must not use public web terminals to access sensitive Bryn Mawr School information. **Unencrypted Personal Identifiers Sent Via Internet Prohibited** - Users must never transmit any personally identifiable information (such as social security numbers and birth dates) unencrypted over the Internet. This prohibition includes email, instant messaging, chat rooms, and other communication systems.

**Internal Systems**

**Involvement with Computer Viruses** - Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Bryn Mawr School computer or network. **Computer Viruses** - Any User who suspects infection by a virus must immediately shut-down the involved computer, disconnect from all networks, and contact the Technology Department. **Software Scanning** - Users must not use any externally-provided software from a person or organization other than a known and trusted supplier unless approved by the Technology Department. **Hacking Activities** - Users must not use Bryn Mawr School
information systems to engage in hacking activities that include, but are not limited to: (a) gaining unauthorized access to any other information systems, (b) damaging, altering, or disrupting the operations of any other information systems, and (c) capturing or otherwise obtaining Passwords, encryption keys, or any other access control mechanism that could permit unauthorized access. **Testing Information System Controls** - Users must not test, or attempt to compromise internal controls unless this activity is specifically approved for IT security purposes. **Encryption Usage Aside from That in Browsers** - Aside from the encryption that is built into Internet browsers, Users may employ encryption of any sort when using computer systems or networks as long as these encryption systems have first been established and approved by the Technology Department. **Incidental Personal Use of Computer Communications Systems** - Bryn Mawr School information systems are provided for, and must be used only for educational purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for educational purposes, (b) does not interfere with User productivity, and (c) does not preempt any educational activity. **Prohibition Against All Forms of Adult Content** - All forms of adult content are prohibited on Bryn Mawr School computers, mobile devices, smartphones, and networks. This includes content obtained via web sites, email attachments, CD-ROMs, and file sharing networks. **Program Resource Consumption** - Computer Users must not run or write any computer program or process that is likely to consume significant system resources or otherwise interfere with Bryn Mawr School educational activities unless authorized by the Technology Department. **Software Duplication** - Users must not copy software provided by Bryn Mawr School to any storage media, transfer such software to another computer, or disclose such software to outside parties without written permission from the Technology Department. **Unauthorized Software and Data Copies** - Bryn Mawr School strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet Users or other system Users make unauthorized copies of software, the Users are doing so on their own behalf, since all such copying is strictly forbidden by Bryn Mawr School.

**Equipment**

**User Installation of Software** - Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization from the Technology Department. **Sharing A Personal Computer with Other People Prohibited** - Users must not share their personal computer, smartphone, tablet or other mobile device if it is used for Bryn Mawr School educational activities, with any other person. **Unattended Active Sessions** - If the computer system to which they are connected or which they are using contains sensitive information, Users must not leave their personal computer, workstation, or terminal unattended without locking their computer. **Student Computer Responsibility** - Middle and Upper School students are required to bring their laptop to school each day, in good working order, charged, and with a power adapter and any other necessary accessories. If a student’s computer becomes infected, she must seek immediate help from Bryn Mawr’s Technology Department. If the Technology Department cannot fix the issue immediately, then the student must go to their...
warranty for assistance. Games On Organization Computer Systems - Games may not be stored or used on any Bryn Mawr School computer systems unless used for educational purposes.

Portable Computers, And Smart Phones Out of Sight - When stored in a motor vehicle or in another unattended public place, Users must lock portable computing devices. Downloaded Software On Mobile Devices & Smart Phones - Software may be downloaded on mobile devices and smart phones that are used for Bryn Mawr School purposes. Physical Protection of Wireless Handheld Devices and Network Interface Cards - Wireless handheld devices, and any other device containing wireless network interface cards (NICs), must be physically protected by the User from loss, theft, and tampering. To maintain access control on Bryn Mawr School's internal network, any loss, theft, or tampering of these devices must be immediately reported to the Technology Department. Powering Down Network-Connected Workstations at Night - All machines, desktops, or non-portable devices connected to the Bryn Mawr School internal network must be powered down and shut off during non-working hours.

Securing Information

Sensitive Information Retention and Destruction - Critical data is backed up on site nightly. Critical data is also backed up at Barracuda to insure that the latest critical data will be readily available even if the physical plant of Bryn Mawr is unavailable. Only personnel that has been given permission, can destroy records that have sensitive information. Portable Computer Backups - Students are required to back up their computer files which might include using an online backup system such as Google Drive or Dropbox and/or external hard drive.

VIOLATIONS

Bryn Mawr reserves the right to take other action in response to actions or omissions that Bryn Mawr believes in good faith violate this policy and/or are potentially unlawful. If a violation of this policy occurs or is reasonably likely to occur, Bryn Mawr may, in its sole discretion, delete the unacceptable file, record, or message and/or terminate use of the Bryn Mawr network and other computing resources. Any information obtained by monitoring, reviewing, or recording may be subject to review by law enforcement organizations in connection with investigation or prosecution of possible criminal activity on or associated with Bryn Mawr’s resources. Bryn Mawr will comply with all effective court orders and subpoenas involving requests for such information.

DEFINITIONS

For definitions and examples of data classifications, please refer to the Bryn Mawr School Information Classification Guide. Information Asset – Any Bryn Mawr School data in any form, and the equipment used to manage, process, or store Bryn Mawr School data, that is used in the course of executing educational. This includes, but is not limited to, corporate, customer data. Password – An arbitrary string of characters chosen by a User that is used to
authenticate the User when he attempts to log on, in order to prevent unauthorized access to his account. **User** - Any Bryn Mawr School student authorized to access any Bryn Mawr School electronic information resource.

**PARENT/GUARDIAN RESPONSIBILITIES**

The parent/guardian must sign this policy in order for the student in his or her care to be provided access to Bryn Mawr’s network and equipment. The parent/guardian must understand the terms and conditions of this policy and that there are disciplinary and other consequences if the student misuses the Bryn Mawr network or online services, or otherwise violates this policy. The parent/guardian remains responsible for his or her student’s use of Bryn Mawr computers, network, software, hardware, peripherals, systems, and services. The parent/guardian consents to the use by the student of Bryn Mawr’s online resources. A copy of these online resources utilized by Bryn Mawr can be found at [http://www.brynmawrschool.org/technology](http://www.brynmawrschool.org/technology). In order for the student to use certain online programs and services made available through Bryn Mawr’s network, the parent/guardian must understand that certain personally identifiable information must be provided to the provider of such online program or service, including for example, the student’s name and school email address. Under federal law, providers of these online programs and services must provide parental notification obtain parental/guardian consent before collecting personally identifiable information from students under the age of thirteen. Bryn Mawr is permitted under law to facilitate the provision of this notice and the gathering of this consent to the collection of personally identifiable information from students in lieu of the provider providing such notice and seeking such consent directly from each parent or guardian. Please note therefore that acceptance of this policy will also constitute notice to and consent by you to the collection and use by these providers of the personally identifiable information made available by your name, email address, and user name, for registration and utilization purposes in connection with use of the online resources.

**AGREEMENT**

**For parents/guardians:**

I have read and discussed the Bryn Mawr School Student Acceptable Use of Assets Policy with my daughter. I understand that violations of this policy may result in revocation of network privileges and in disciplinary action up to and including dismissal. Acknowledging that some materials on the Internet may be objectionable, I accept the policy in both letter and spirit, and grant permission for my daughter to have access to online services as well as networked Bryn Mawr computer services. I exonerate and hold Bryn Mawr harmless from all liability should my daughter encounter any material that she, I or the school may find objectionable. I understand that violations of any of these policies may result in revocation of network privileges and in disciplinary action up to and including expulsion.