

Scope of Coverage for all Technology Policies:

Policies, guidelines, and rules described in this guide refer to all computing devices (including but not limited to computers, handhelds or PDAs, MP3 players, portable memory storage devices, calculators with interfacing capability, cell phones, digital cameras, etc.), technology infrastructure, associated peripheral devices and/or software.

- Owned or leased by Chrysalis School.
- Owned by, leased by and/or on loan to any third party engaged in providing services for Chrysalis Schools.
- Any computing or telecommunication devices owned by, in the possession of, or being used by students and/or staff that are operated on the grounds of any Chrysalis School or Chrysalis property or connected to any equipment by direct connection, telephone line or other common carrier or any types of connection including both hardwired, fiber infrared and/or wireless.

AUP—Acceptable Use Policy for Information Technology Resources—Notice of Privacy:

Chrysalis School reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary.

Users should have NO expectation of privacy regarding their use of Chrysalis School property, network and/or Internet access or files, including e-mail. Users who bring personal electronic equipment and use Chrysalis School network, Internet, wireless or other access should also have **NO expectation of privacy including files or e-mail.** Chrysalis staff has the right to seize and search any electronic device being used on Chrysalis School property. This includes both public and personal equipment.

CyberBullying:

Chrysalis School defines CyberBullying as:

- Being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies. It has various forms, including direct harassment and indirect activities that are intended to damage the reputation or interfere with the relationships of the student targeted, such as posting harmful materials, impersonating the person, disseminating personal information or images, or activities that result in exclusion.
- **Any instance or suspected instance of these activities will not be tolerated. Appropriate disciplinary actions may be taken depending on the situation.**
- CyberBullying that takes place off campus, but affects any student on campus and/or during school hours will not be tolerated. Appropriate disciplinary actions may be taken depending on the situation.

Acceptable Uses of the Computer Network or Internet:

These are examples of appropriate activity on the Chrysalis School network. The Staff reserves the right to change, add, remove or alter these at any time:

- Chrysalis School will provide access to technology resources. Users should be aware that these resources will be monitored and there should be NO expectation of privacy.
- All of the school's computer network must be in support of education and research consistent with the school's mission. Chrysalis reserves the right to prioritize use of and access to the network.

Unacceptable Uses of the Computer Network of Internet:

These are examples of inappropriate activity on the Chrysalis School network, but the Staff reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the students, employees, schools, network or computer resources, or (2) that expend network resources, and any activity that Chrysalis Staff determines lacks legitimate educational content/purpose, or (3) other activities as determined by Chrysalis Staff as inappropriate.

- **Violating any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;**
- **Criminal activities that can be punished under law;**
- **Selling or purchasing illegal items or substances;**
- **Obtaining and/or using personal e-mail sites, spamming, spreading viruses;**
- **Causing harm to others or damage to their property, such as:**
 1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
 2. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data; disguising one's identity, impersonating other users, or sending anonymous e-mail;
 3. Damaging computer equipment, files, data, or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
 4. Using any Chrysalis School computer to pursue "hacking," internal or external to Chrysalis School, or attempting to access information protected by privacy laws, or;
 5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."
- **Students may NOT access on Chrysalis equipment:**
 1. Any social media websites including but not limited to: Facebook, MySpace, Twitter, etc.
 2. E-mail on ANY site.
 3. Instant messaging/chatting sites, including but not limited to: AIM, Yahoo, MSN, SKYPE, IRC, etc.
 4. Sites to download any software, add ons, games. Students may not alter Chrysalis equipment in any way.
 5. The desktop settings, control panel, or alter any other hardware or software settings.

Electronic Device Use in the Classroom:

Any use of electronic devices (both Chrysalis School property and personal devices) during group or individual class time **must be pre-arranged by each teacher/staff member**. The teacher/staff member reserves the right to forbid electronic device use during class or individual appointment at any time.

Security:

- Users shall not attempt to gain unauthorized access to the network, misrepresent other users on the network, or seek information, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Communications may not be encrypted so as to avoid security review.

Personal Safety:

- Personal information such as addresses and telephone numbers should remain confidential. Students should never reveal such information without permission from a teacher or other adult.
- Students should never make appointments to meet people in person whom they have contacted on the Internet without parental permission.
- Students should notify their teachers or some other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Copyright:

The unauthorized installation, use, storage, or distribution of copyrighted software or material on school computers is prohibited.

General Use:

- A signed Internet Consent Form must be on file. Students under the age of 18 must have the approval of a parent or guardian to use the network.
- Nothing in these regulations is intended to preclude the supervised use of the network while under the direction of a staff member, teaching assistant, or other approved person acting in conformity with school policies and procedures.

Consequences of Violation of Policy:

- Violations of these rules may result in disciplinary action, including but not limited to a warning to discontinue use, confiscation of the electronic device, the loss of a student's privileges to use the school's information technology resources, parent/consulting teacher conference, involvement of law enforcement or any other disciplinary action deemed necessary.
- From time to time, the school will make a determination of whether specific uses of the network are consistent with regulations states above. Under prescribed circumstances, non-student use may be permitted provided such individuals demonstrate that their use furthers the purpose and goals of the school. For security and administrative purposes, Chrysalis School reserves the right to remove a user account on the network to prevent further unauthorized activity.