

## Stockton Collegiate International Schools Technology Acceptable Use Policy

**SUMMARY:** *This policy was written to inform students, their families, and staff about the acceptable ways in which technology systems may be used in Stockton Collegiate International Schools ("Stockton Collegiate"). Stockton Collegiate is committed to improving student achievement and preparing all students to be college ready graduates. School Technology, which includes but is not limited to: computer hardware, software, and the Internet provide powerful tools to access information and communicate with people, enhancing learning and enabling the school to operate. With the constant introduction of new technology, new ways to communicate, and new ways to access and transfer information, it is critical that Stockton Collegiate continue to define a policy that ensures a safe learning environment for students and staff as well as the protection of Stockton Collegiate's technology. The use of Stockton Collegiate technology is offered to students and staff as a privilege which must be safeguarded by all learners.*

### Technology Acceptable Use Policy

Stockton Collegiate provides technology, including, but not limited to: computers, tablets, networks and Internet services. **Acceptable use of Stockton Collegiate Technology is for purposes that support student learning and prepare students to be college ready graduates.** All Stockton Collegiate technology remains at all times the property of Stockton Collegiate.

This policy shall conform to school policies, established procedures and copyright laws, and shall not violate federal, state or local laws.

The Technology Acceptable Use Policy is in place to prevent unauthorized access and other unlawful activities by Learners online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "Learner" includes anyone, including employees, students, and guests, using Stockton Collegiate technology, including, but not limited to, computers, tablets, networks, Internet, email, chat rooms and other forms of technology services and products. Only Learners who agree to this Acceptable Use Policy are authorized to use Stockton Collegiate technology.

This policy describes acceptable uses of school technology systems (hardware, software, network, and internet) as well as unacceptable uses. This policy is established to:

- Enhance teaching and learning;
- Increase safety for students and staff;
- Improve the efficiency of school technology systems;
- Ensure compliance with applicable school policies, state and federal laws; and
- Educate students, staff, and other who use Stockton Collegiate technology

Stockton Collegiate will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network. Stockton Collegiate reserves the right to monitor Learners' 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. Learners should have no expectation of privacy regarding their use of Stockton Collegiate property, network and/or Internet access or files, including email.

Learners and other users are required to follow this policy and report any misuse of the Stockton Collegiate's technology, including network or Internet, to a supervisor, or other appropriate Stockton Collegiate personnel. Access is provided primarily for education and Stockton Collegiate business.

Staff may use the Internet for incidental personal use only during duty-free time. By using the network, Learners have agreed to this policy. If a Learner is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor, or other appropriate Stockton Collegiate personnel.

Violation of these policies may result in one or more of the following:

- Disciplinary action and/or termination for employees and temporary staff, termination of contracts for consultants or contract employees;
- Dismissal for interns and volunteers; or

Current May 2020

- Disciplinary action in the case of a student.
- Additionally, individuals are subject to loss of access privileges, and/or potentially civil, and criminal prosecution. Stockton Collegiate will attempt to tailor any disciplinary action to the specific issues related to each violation.

### **Unacceptable Uses of Stockton Collegiate Technology**

The following are examples of inappropriate activity, but the School reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for Stockton Collegiate students, employees, schools, network or computer resources, or 2) that use Stockton Collegiate technology resources on content Stockton Collegiate, in its sole discretion, determines lacks legitimate educational content or educational purpose, or 3) other activities as determined by Stockton Collegiate as inappropriate.

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
5. Causing harm to others or damage to their property.
6. 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.
7. Deleting, copying, modifying, or forging other users' names, emails, files, or data disguising one's identity, impersonating other users, or sending anonymous email.
8. 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.
9. Using any Stockton Collegiate computer to pursue "hacking," internal or external to Stockton Collegiate, or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".
11. Using web sites, email, networks, or other technology for political uses or personal gain.
12. Stockton Collegiate internet and intranet property must not be used for personal benefit.
13. Learners must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
14. Advertising, promoting non-school sites or commercial efforts and events.
15. Learners must adhere to all copyright laws.
16. Learners are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

### **Security**

1. Learners must report any weaknesses in Stockton Collegiate internet and intranet security, any incidents of possible misuse or violation of this agreement to an Administrator.
2. Learners must not attempt to access any data or programs for which they do not have authorization or explicit consent.
3. Learners must not purposely engage in activity that may degrade the performance of Stockton Collegiate Technology systems and related Technology property; deprive an authorized Stockton Collegiate Learner access to a Stockton Collegiate resource; obtain extra resources beyond those allocated; circumvent Stockton Collegiate security measures.
4. Learners must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of Stockton Collegiate Technology systems and related Technology property.

5. All data must be kept confidential and secure by the Learner. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. If this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.
6. All software programs, applications, source code, object code, documentation and data shall be guarded and protected.
7. Access to Stockton Collegiate Technology equipment must be properly documented, authorized and controlled.

#### **Acceptable Use Policy Supporting Information**

1. Stockton Collegiate reserves the right to remove any content (organizational or personal) on the Internet or intranet at any time, without cause or notice.
2. There is no guarantee of personal privacy or access to Stockton Collegiate Technology. Stockton Collegiate reserves the right to search and/or monitor any information created, accessed, sent, received, and/or stored in any format by any Stockton Collegiate employee on school equipment or any equipment connected to the school's network.
3. Schools and Departments responsible for the custody and operation of Stockton Collegiate technology shall be responsible for proper authorization and related technology utilization, the establishment of effective use, and reporting of performance to management.
4. All commercial software used on Stockton Collegiate Technology systems are copyrighted and designated for School use. Learners must abide by all license agreements.

*Adopted: August 10, 2011*

#### Parent/Guardian Acknowledgment:

I have read Stockton Collegiate's Technology Acceptable Use Policy and reviewed it with my child. I understand that violation of these provisions may result in disciplinary action taken against my child, including but not limited to suspension or revocation of my child's access to the school's technology resources.

I understand that my child's technology usage is not private and that the school will monitor my child's use of technology resources. I consent to the school's interception of or access to all communications sent, received or stored by my child using the school's technology resources.

I agree to be responsible for any unauthorized costs arising from my child's use of the school's technology resources. I agree to be responsible for any damages caused by my child.

