CRISTO REY JESUIT

COLLEGE PREPARATORY SCHOOL OF HOUSTON

Parent/Student Handbook for 1:1 Technology Integration

Technology Policy

Overview

Cristo Rey Jesuit College Preparatory School decreed and orders a technology policy designed to protect the student body and secure the authenticity of the School. The policy and measures put in place ensure reasonable and ethical behavior of all members of the Cristo Rey Jesuit College Preparatory School community. The procedures also safeguard against the innumerable of negative and unethical uses for technology that can discourage the students from the mission of the School. Cristo Rey Jesuit College Preparatory School does not intend for its technology policy to pause individuality, social collaboration or academic enhancement.

Computer/Internet

Cristo Rey Jesuit College Preparatory School provides technology resources to its students solely for educational purposes. These technology resources include, but are not limited to, hardware, software, networks, the internet, personal electronic devices and Chromebooks ("Technology Resources"). Through technology, Cristo Rey Jesuit College Preparatory School provides access for students and staff to resources from around the world. Expanding technologies take students and staff beyond the confines of the classroom and provide tremendous opportunities for enhancing, extending, and rethinking the learning process. The goal in providing these resources is to promote educational excellence at Cristo Rey Jesuit College Preparatory School by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, faculty and staff. The Student Acceptable Use Policy (the "SAUP") governs student use of Technology Resources.

The Opportunities and Risks of Technology Use

Access to technology brings with it the obtainability of material that may not be of instructive value in the context of the school setting or may be detrimental or disorderly. Because information on networks is transitory and diverse, Cristo Rey Jesuit College Preparatory School cannot completely predict or control what students may access. Cristo Rey Jesuit College Preparatory School believes that the educational value of the use of Technology Resources outweighs the potential of students encountering material that is not consistent with the educational goals or values of Cristo Rey Jesuit College Preparatory School.

Parent(s)/guardian(s) are directed that determined users may be able to gain access to information, communication and/or services on the internet to which Cristo Rey Jesuit College Preparatory School has not authorized for educational purposes and/or their Parent(s)/guardian(s) may find inappropriate, offensive, objectionable and/or controversial. Parent(s)/guardian(s) assume this risk by consenting to allow the student to participate in the use of Technology Resources.

Privileges and Responsibilities

Cristo Rey Jesuit College Preparatory School's electronic network is part of the curriculum and is not a public forum for general use. Students may access Technology Resources only for educational purposes. The actions of students accessing networks through Cristo Rey Jesuit College Preparatory School reflect on our school. Students, therefore, must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Students are responsible for their behavior and communications while using Technology Resources.

Disciplinary Action

Violations of the SAUP, or any administrative regulations and guidelines governing the use of technology, may result in disciplinary action that may include loss of network access, loss of technology use, or expulsion, or other appropriate disciplinary action. A student and his/her parent/guardian must pay for the cost of repairs if the student defaces, damages or alters Technology Resources. If a student intentionally transfers a virus-infected file and/or software program that infects Technology Resources and causes damage, the student and his/her parent or legal guardian is liable for any and all repair costs necessary to make the affected Technology Resources operational. A student's access to Technology Resources may also be suspended until the full repair costs are paid by the student or his/her parents or legal guardians. Violations of local, state or federal law may subject students to prosecution by appropriate law enforcement authorities.

Privacy

Students should not expect that communications or files stored on Cristo Rey Jesuit College Preparatory School servers or utilizing Technology Resources will be private. Students must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside Cristo Rey Jesuit College Preparatory School. The school administration will report any communications or

relating to or in support of illegal activities to the appropriate authorities.

Although files stored on the Cristo Rey Jesuit College Preparatory School network are private, any computer files, web logs, internet site visits, and/or e-mails that originate or reside on Cristo Rey Jesuit College Preparatory School computers/servers and/or CWSP Job Partner servers may be monitored at any time, without prior notice to the student. Cristo Rey Jesuit College Preparatory School is not responsible for any damages the student may suffer, including the loss of data. Cristo Rey Jesuit College Preparatory School is not responsible for the accuracy or quality of any information obtained through any school internet connection.

Safety

Students should never agree to get together with someone they "meet" online without parent/guardian approval and participation. If someone offers to meet them, students should notify a Cristo Rey Jesuit College Preparatory School staff member and parent/guardian immediately. If a student receives an inappropriate message(s) or one that makes him or her uncomfortable, s/he should promptly notify a Cristo Rey Jesuit College Preparatory School staff member and parent/guardian. The student should not delete the message(s) until written permission has been given by the Director of Information Technology. Students must secure prior written approval from a Cristo Rey Jesuit College Preparatory School staff member before joining bulletin boards or chat rooms.

We encourage parent(s)/guardian(s) to have a frank discussion with their students about Catholic values and how those beliefs should guide the students' activities while using Technology Resources. Every student and his/her parent or legal guardian must sign the SAUP, and every student must abide by its policies.

Personal Electronic Devices

Cell phones and other personal electronic devices are only permitted in class with the stated permission of the teacher of that specific class. Otherwise, cell phones and other personal electronic devices should be stored in the student's backpack out of the view of the teacher at all times. If a teacher requests that students cease using any electronic device, then the students must put the devices away and out of view. If the student refuses or fails to do so, then the teacher will inform the principal. At no point, are cell phones or other electronic devices permitted while standardized testing is in progress. Failure to observe the rule regarding standardized tests and electronic devices will result in immediate suspension, contact of parent/guardian, and turning over of the test to state testing officials.

Cristo Rey Jesuit College Preparatory School permits cell phones and other electronic devices in the public areas of the building, including hallways, bathrooms, cafeteria, gym, auditorium or offices. Students, however, may not make phone calls during academic hours or enrichment hours. They may make calls at the conclusion of academic hours – after seventh period – to coordinate their pick-up.

Cristo Rey Jesuit College Preparatory School does not permit the use of cell phones or other electronic devices inside the church/chapel or at the workplace. Cristo Rey Jesuit College Preparatory School reserves the right to extend the area of prohibited cell phone and electronic device usage to any other section of its campus at its discretion If a student is observed using any electronic devices in these designated areas without permission, s/he risks having that device confiscated by Cristo Rey Jesuit College Preparatory School.

If a student has been granted permission to use an electronic device and s/he "abuses" that privilege by engaging in any activity other than purpose for which permission was granted, that student risks suspension and confiscation of that device by Cristo Rey Jesuit College Preparatory School for a period of time at the discretion of Cristo Rey Jesuit College Preparatory School.

If a student is asked to hand over a device by an administrator and s/he refuses, creates an incident, or argues against the request, he or she risks further corrective action at the discretion of Cristo Rey Jesuit College Preparatory School.

Please be advised that any electronic devices are the sole responsibility of the owner of that device. At no point is Cristo Rey Jesuit College Preparatory School nor any Cristo Rey Jesuit College Preparatory School employee or volunteer responsible for that device unless Cristo Rey Jesuit College Preparatory School confiscates that device. If a device is missing or lost, that student must report it to an administrator immediately and file the appropriate paperwork. The principal, at her discretion, will decide the outcome of this situation. If another student took or destroyed another's property, then Cristo Rey Jesuit College Preparatory School will promptly dismiss that student; and the principal pursue any legal action at her discretion.

Cristo Rey Jesuit College Preparatory School does not permit personal laptops, netbooks, tablets and any similar device or equipment on its campus at any time.

Students are not permitted to wear smart watches, including iWatches, at school or work. If a student is caught violating this rule, the principal will take the watch away and only the parents of the student can pick up the watch at school.

Cristo Rey Jesuit College Preparatory School of Houston Administration Procedures

No. 2314 P-1

Attachment 1

TECHNOLOGY RESOURCES USE AGREEMENT (STUDENT)

Parent or Guardian:

The students in Cristo Rey Jesuit have direct access to the Internet and the wifi network, with this privilege comes responsibility. All students must be informed of the rules regarding Internet and network use and agree to abide by these rules. The schools utilize GoGuardian content filtering to prevent students from accessing inappropriate online materials. Users of the network are required to sign a "Technology Resources Use Agreement." Please read and discuss this information with your student and sign on the back. Parents and students will be required to complete the "Technology Resources Use Agreement" upon first technology usage. Also note, each school year may require annual completion.

Student:

The use of the network is a privilege and inappropriate use may result in a cancellation of those privileges. Security on any computer system is a high priority, especially when the system involves many users. If the user identifies a security problem on the system, the user must notify staff and must not demonstrate the problem to other users. Students are responsible for good behavior on school computer networks just as they are in a school classroom or a school hallway.

Please sign this document and **return it** to the **School** or as **directed by your teacher**

The following information was extracted/adapted from the "**Cristo Rey Jesuit College Preparatory School Board Procedure #2314 P-1 Technology Resources."** Copies of the complete board policy no. 2314 and procedures are available on the http://cristoreyjesuit.org website.

Personal Internet Safety:

1. **Do Not** reveal personal contact information about yourself (address, phone number, etc) while online
2. **Do Not** agree to meet people that you have been in contact with over the Internet without parent permission
3. **Do Not** give out private or confidential information about yourself or others
4. **Tell** your teacher or other school employee about any message you receive that is inappropriate or makes you uncomfortable

Acceptable Use:

The use of this account **must be** in **support** of **education** and **educational research.**

Unacceptable Use:

Examples of Activities (but not limited to), which are **NOT PERMITTED**:

1. Displaying sexually explicit, pornographic, obscene, lewd or other inappropriate messages or pictures
2. Using obscene language or material
3. Participating in offensive and/or threatening attacks via "Cyber Bullying" against individuals or groups
4. Damaging computers, computer system or computer networks
5. Violating copyright laws
6. Using other users' passwords
7. Trespassing on other users' work: systems, folders, work or files
8. Excessive use of limited resources (beyond time authorized by administrators)
9. Personal email or free "web surfing" during school hours
10. Employing the network for commercial, personal or political purposes
11. Modifying software on school equipment or installing personal technology on the network without written permission
12. Accessing any computer not explicitly authorized for use

Student Email

Cristo Rey Jesuit College Preparatory School creates email accounts for all students, which includes email access if needed. Cristo Rey Jesuit College Preparatory School is providing this service because it is obligated, "to ensure that all students use computers, networks and communications (including e-mail) in schools for school related purposes in an appropriate manner." The mastery of effective and proper e-mail communications is expected of Cristo Rey Jesuit College Preparatory School students and is embedded in the Essential Academic Learning Requirements and Grade Level Expectations in Educational Technology Digital Citizenship, Component 2.3," communicate with peers and teachers using email." Consequently, Cristo Rey Jesuit College Preparatory School students will be expected to utilize their Cristo Rey Jesuit College Preparatory School e-mail account for school communication.

This account will be assigned to students as they enter the school and will be available for school/educational usage throughout their career in Cristo Rey Jesuit. In addition to email, this account will provide access to collaboration tools (word processor, calendar, spreadsheets), as well as other educational related tools.

Student - (signature required)

I understand and will abide by the Technology Resources Use Agreement Policy and agree to use the network responsibly. I further understand that any violation of the regulations contained therein may result in disciplinary action and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action or appropriate legal action may be taken.

Student Full Name (please print) _____

Signature _____ Date _____

Parent or Guardian Permission – (If student is under the age of 18, a parent or guardian must also read and sign this agreement)

As a parent or guardian of this student, I have read the Technology Resources Use Agreement Policy. I understand that this access is designed for educational purposes only. I recognize that it is impossible for Cristo Rey Jesuit College Preparatory School to completely restrict access to offensive, inappropriate or other controversial information and materials available through Internet or other sources from the network, and I will not hold Cristo Rey Jesuit College Preparatory School responsible for information and materials obtained by this student from the network. I understand this agreement will be kept on at the school.

I also understand that from time to time the teacher or school may wish to publish examples of student projects, unidentified photographs of students and other work on an Internet accessible server via staff or school website.

Please circle.

I have read and reviewed the Student/Parent Technology Handbook with my child and understand my responsibilities with respect to technology use at Cristo Rey Jesuit College Preparatory School, and at home.

(This document can be reviewed online at the website and each student will be reviewing this at the start of each school year)

Yes No

My child may use the Internet and email (with teacher supervision) at school, and at home according to the rules outlined.

Yes No

My child's work may be published on the Internet for classroom/school purposes.

Yes No

Parent/Guardian Name (Please print) _____

Signature _____Date_____

****For additional information, please contact your student's principal or Technology Department****

Implemented 8-15-2020 Revised 07-06-2020

Internet Safety for Children

The Internet is a wonderful place to find information and connect with people and friends. It does pose safety and privacy risks, though, especially to minors.

What you can do to protect your children online:

1. Talk about Internet safety as soon as they begin using the Internet. It is never too early.
2. Consider placing the computer in a common area of the house. Stay involved in their online world by monitoring with whom they email and chat. Get to know the websites they're visiting.
3. Know their usernames and screen name and make sure they are appropriate.
4. Use safe search engines. For younger kids in particular, use age-appropriate filtering and monitoring software.
5. Educate yourself about computers, the Internet and potential risks to children

1. policy requires users to be at least 13 years old, but many younger kids join by pretending to be older. By default, adults' posts are public; kids' posts can be seen by friends of their friends.
2. **Twitter** is a real-time information network where people get the latest news, ideas, and opinions about what interests them. There's no age limit. Tweets are public by default.
3. **LinkedIn** is a social site that allows professionals to network with business connections, search for jobs and hiring managers, join groups, etc. Users need to be at least 18 years old. LinkedIn users have a private and a public profile, the visibility of which they can control.
4. **YouTube** is a free video sharing site and social network. Anybody can upload, watch and share videos on YouTube.
5. **Snapchat** is a photo messaging application developed by Stanford University students. Using the app, users can take photos, record videos, add text and drawings, and send them to a list of

online.

What your children should not do:

1. Tell your child to never share their passwords with anyone, including friends.
2. Teach them not to fill out forms without your knowledge, or open emails from strangers.
3. Do not allow your child to go into private chat rooms.

Social Networking

Social networks have become very popular among adults and children alike. These sites allow users to communicate and share information. They can be accessed anywhere there is an Internet connection, including on smartphones.

The basics on some popular socialnetworks:

Facebook is a free social networking site used by people all over the world.

How to protect your children's safety:

1. Teach them to only accept requests from Facebook friends and Twitter followers they know personally ("Don't talk to strangers").
2. Instruct your children to never agree to meet face-to-face someone they only know online.
3. Keep lines of communication open.
4. Your kids might not tell you everything, but that doesn't mean you shouldn't ask.

Cyberbullying

1. Cyberbullying is using the Internet to harass or bully someone, for example, by spreading false rumors or sharing inappropriate images online.

1. Your kids might not tell you everything, but that doesn't mean you shouldn't ask.

How to prevent cyberbullying:

1. Speak with your children about what is appropriate to say and do online. Be kind online.
2. Review your child's online information from time to time. Seeing what others say on your child's pages can help you

recipients. These sent photographs and videos are known as "Snaps".

6. **Instagram** is an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, such as Facebook, Twitter, Tumblr and Flickr.
7. If your child wants to use social networks, talk to them about your expectations: how they should behave; what is safe and what isn't;

Tik Tok is an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, such as Facebook, Twitter, Tumblr and Flickr

How to protect your children's privacy and reputation:

1. Go through Tik Tok, and Facebook's privacy settings together and select levels you're both comfortable with. Encourage your children to require their approval before they can be tagged in posts (one of Facebook's privacy settings). Set Tweets to be protected (private) by default.
2. Teach them to never post personal
3. Discourage the use of webcams. Tell them to never send any image or video to a stranger.
4. Under no circumstances should they upload a photo that contains nudity (it's illegal).
5. Most importantly, teach them online common sense: think before you post or tweet. Would you want the entire school to see this post, photo, or video? If you would not say something to someone's face, do not say it in an online message.

stop cyberbullying. 3. Try to spot changes in your child's behavior that might suggest cyberbullying such as avoiding computers or appearing stressed when receiving an email or text. **What to do if you feel your child is a victim of cyberbullying:** 1. Tell your children not to respond to cyberbullying, but to stop, block and tell. 2. Stop interacting with the bully. 3. Block the bully from sending any more messages. 4. Tell an adult they trust. 5. Document emails and communication. 6. Seek help. 7. If you feel your child is in immediate danger, report the incident to law enforcement immediately.	

Protecting your identity

- Using strong passwords protects your valuable personal information and keeps you safe.

Password Do's and Don'ts:

1. Do use a mix of letters, symbols and numbers.
2. Do not use sequences (123 or abc) or personal information such as your birth date.
3. Do not use easy dictionary words.
4. Do not reuse old passwords.

Email "Phishing"

This is when scammers send emails that pretend to come from a real company to try to trick you into revealing private information, like addresses or account numbers.

How to avoid Phishing:

1. Don't reply to messages that ask about personal or financial information.
2. Check the link: If you do not trust the website or sender, DO NOT click on any links in the email.

Spyware and Viruses

This is when a computer program gathers your information without your knowledge or permission. Spyware can make your computer work poorly (slow browsing, program crashes, etc.).

Insurance

The school carries an Accidental Breakage policy that will cover one (1) accidental break per device per year for a total of four (4) breaks over four (4) years. Should your device be damaged more than once per year, you are responsible for the cost of materials that are required to be purchased in order to return your device to working order.

Notice

Students will be allowed to keep their Chromebook upon graduation. However, if you leave the school for any reason before graduation you will be required to return your device.