

HOUSTON COUNTY SCHOOL DISTRICT

RESPONSIBLE USE POLICY (RUP)

&

**TECHNOLOGY HANDBOOK for PARENTS
and STUDENTS**



2018-19

TABLE OF CONTENTS

Introduction.....	3
About Chromebooks.....	3
Who Can Participate	3
General Expectations for Use of School Technological Resources	3
Handling, Care and Use by Students.....	5
Security, Storage and Transport.....	5
Privacy.....	6
Google Account	6
Other School Issued Accounts.....	6
File Storage.....	6
Content Filtering and Restricted Material on the Internet.....	6
Damage to Device.....	7
Loss or Theft.....	7
Reporting Loss/Damage/Theft.....	7
Repair Costs	8
Replacement Costs.....	8
Parent/Guardian Initiated Accommodations	9
Administrator-Initiated Accommodations.....	9
Disclaimer	9
Student/Parent/Guardian Acknowledgement Signature Page.....	11

Introduction

Houston County Schools (HCS) intends that students and employees benefit from technological resources while remaining within the bounds of safe, legal and responsible use. Accordingly, HCS establishes this Responsible Use Policy and Technology Handbook to govern student use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

About Chromebooks

Google Chromebooks are a type of electronic device combining the practicality of a laptop with the simplicity and effectiveness of a tablet. Parents and students who are security conscious are delighted to find out that Chromebooks are among the most secure devices on the market. Chromebooks link directly to the cloud and run Google Apps, but can be used without a Wi-Fi connection.

Who Can Participate

A student who is actively enrolled in any Houston County school may be provided a learning device to use in the classroom. HCS strongly believe this initiative is a vital component in preparing students to be college and career ready.

General Expectations for Use of School Technological Resources

1. District technological resources are provided for school-appropriate purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school district technological resources for political purposes or for commercial gain or profit is prohibited. Student personal use of school district technological resources for amusement or entertainment during the school day is also prohibited without permission from authority.
2. Students must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism.
3. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors. All users must comply with HCS policies.

4. The use of anonymous proxies to circumvent content filtering is prohibited.
5. Users may not install or use any Internet-based file-sharing program designed to facilitate sharing of copyrighted material.
6. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
7. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information (of self or others), or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. Users also may not forward or post personal communications without the author's prior consent.
8. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance.
9. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the expressed permission of the technology director or designee.
10. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.
11. Users are prohibited from using another individual's ID or password for any technological resource.
12. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
13. If a user identifies a security problem on a technological resource, s/he must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
14. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time, to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.
15. Students who are issued district owned and maintained devices must also follow these guidelines:
 - a. Keep the device secure and damage free.
 - b. Do not loan out the device, charger or cords.
 - c. Do not leave the device unattended.

- d. Do not eat or drink while using the device or have food or drinks in close proximity to the device.
- e. Do not place the device on the floor or on a sitting area such as a chair.
- f. Do not leave the device near table or desk edges.
- g. Do not stack objects on top of the device.
- h. Do not leave the device outside.

Handling, Care and Use by Students

- You are responsible for all media, Internet usage, downloads, file creation, file deletion, file sharing, file storage, and other actions that involve all software or applications accessed via your assigned device. Do not allow other users to use the device assigned to you.
- Your device is only for creation of, storage of, access to, and consumption of school-appropriate content. Do not access, store, create, consume, or share unauthorized or inappropriate content with your device.
- Make sure the device logs on to the school district's network daily to receive necessary updates that are critical to keeping the device safe and operational.
- Make sure nothing is ever connected to, or inserted into, any of the ports and/or connectors of the device that are not intended for that particular port or connector.
- Make sure your device is never exposed to liquids or other foreign substances, including drinks, paint, ink, glue, cleaners, polishes, or any type of health/beauty aid (lotion, nail polish, perfume, soap, shampoo, etc.).
- Make sure the surface of your device is not altered or defaced. Do not decorate your assigned device or remove labels, stickers, or tags from the device that are affixed by school district personnel.

Security, Storage and Transport

- Keep the device powered off when not in use.
- Do not hold, lift, or suspend the device in the air solely by the screen/display.
- Handle the device with caution. Do not throw, slide, drop, toss, etc. the device.
- Relocate a device that is powered on, opened up, and in use for class to a secure location to be monitored by a staff member if leaving the classroom at school. Do not leave it on a small or unstable desk in a crowded classroom if you are leaving the room, even if only for a moment.
- Keep your device secure. Students are responsible for their device at all times. Devices should be stored in appropriate classroom charging cart overnight.

Privacy

No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer. Under certain circumstances, HCS may be required to disclose such electronic information to law enforcement or other third parties. For example, release student activities or correspondence as a response to a document production request in a lawsuit, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

Google Account

Through a HCS student login, the district provides students with a district owned and managed account to access Google Apps for Education. Google provides access to specific Google products to school districts on an a-la-carte basis. HCS chooses which Google services students have access to and manages the secure Google accounts. Services that students have access to include, but are not limited to, Drive, Mail, Sites and Calendar.

Other School Issued Accounts

To provide access to appropriate online resources and services, their teachers or schools may issue students accounts. Because new technologies are being developed every day, students may gain or lose access to different services or resources during the school year. All services and resources will be vetted for appropriateness of content and compliance with Federal CIPA and COPPA privacy regulations. Educational software and web based educational tools do collect and store the students' information as to assess their progress. It is our duty to inform each parent that personal information is collected for education and assessment purposes.

File Storage

- Every student is provided storage on Google Drive for school related files and content.
- Flash drives, etc. formatted as storage devices can be used on HCS Devices.
- Any time a device requires repair or maintenance, all data and documents stored locally on the device will be lost.

Content Filtering and Restricted Material on the Internet

HCS employs a third party filtering application on all district computers that is updated regularly. These updates are pushed to student devices each time they are logged on to the district's network. The content filter, as configured by the district and as operates on the device in possession of a student who is using the device will restrict inadvertent access to unapproved content online and deter attempts to deliberately access unapproved content online. This does

not absolve the user from attempting to access unauthorized or inappropriate sites on the Internet. Attempts to disable, reconfigure, or circumvent the content filter is a violation of the aforementioned usage policies and can result in administrative referral for disciplinary consequences or restrictions of a student's technology use privileges.

Because of the nature of the Internet, no content filter is capable of preventing all access to all online content that is not school-related. Although the content filter will provide a degree of protection to the user and the device, the user assumes responsibility for not accessing content that is not school-related, whether blocked by the filter at that particular time or not. HCS recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school district personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. HCS shall ensure that technology protection measures are used and are disabled or minimized only when permitted by law and board policy. HCS is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service). Any access of unapproved content online, whether through a district-owned device, personal cell phone, or any other personal electronic device, while at school is a violation of usage policy.

Damage to Device

By taking possession of a borrowed device, the borrower agrees to assume full responsibility for the safety, security, care, and proper use of the borrowed property. In case of accident or careless handling of the property, the borrower agrees to assume full responsibility for the damaged device as deemed necessary by the school district. In the case of damage to a borrowed device, the user must report a potentially damaging incident to school administration of the appropriate building within one school day of the occurrence. Failing to report damage or potentially damaging incidents in a timely manner described here may result in a financial obligation for the student/parent/guardian in the amount of repair costs for the damaged property.

Reporting Loss/Damage/Theft

By taking possession of a borrowed device, the borrower agrees to assume full responsibility for the safety, security, and care of the borrowed property.

- In the case of loss or theft occurring at school, the borrower must report the incident to school administration of the appropriate building within one school day of the occurrence.
- Failing to report loss or theft in the manner described here will result in the missing property being categorized as lost rather than stolen and may result in the user assuming full responsibility for the loss of the device and the corresponding financial obligation for the replacement costs of the lost property.

- In the case of damage to a borrowed device, you must report the potentially damaging incident to school administrators of the appropriate building within one school day of the occurrence.
- Failing to report damage or potentially damaging incidents in the timely manner described above may result in the user assuming responsibility of necessary repair costs for the damaged property.

Repair Costs

- Repairs will be made to a borrowed device if the nature of the damage makes the device inoperable or leaves the device in a state where the damage is likely to increase after redistribution resulting in need of repair for a future user.
- The student/parent/guardian is responsible for any cost of repairs related to a damaged device. Principals may use their discretion for charges where malice intent and/or obvious neglect are present.

Repair	1 st Incident	2 nd Incident	3 rd Incident or neglect
Broken Screen	\$45 max	\$55 max	\$65 max
Charger	\$35 max	\$40 max	\$45 max
Broken or Missing Keys (minor damage)	\$5 per key	\$7 per key	\$10 per key
Broken or Missing Keys (major damage)	\$45 max	\$50 max	\$55 max
Top Plastic Case	\$30 max	\$35 max	\$40 max
Bottom Plastic Case	\$30 max	\$35 max	\$40 max
Battery Replacement	\$45 max	\$55 max	\$65 max
** This table is based on market conditions and is subject to change.**			

Replacement Costs

- A student/parent/guardian is responsible for cost of replacement of a lost device. The replacement cost of a lost device is based on the cost of a replacement device based upon the device value. Principals may use their discretion for charges regarding a lost device.
- A student/parent/guardian is responsible for the replacement cost of any device accessories lost while in their possession. Replacement costs of device accessories are based on the price for which HCS purchases replacement accessories from 3rd party vendors. Principals may use their discretion for charges regarding lost accessories.

Parent/Guardian Initiated Accommodations

It is the belief of HCS that every student should be granted equal access to the resources provided by the school district for learning. It is not the district's recommendation that a student be restricted access to any learning resource that is granted to all other students. If circumstances outside of school call for a student to have limited or restricted access to district-provided resources, a written request by the student's parent/guardian, in collaboration with a school administrator, must be placed on file with the particular school from which the parent/guardian is requesting the special accommodation. If the request is initiated by parent/guardian, then approved by a school administrator, and placed on file with the school's technology department, a student may be granted "as needed only" or "by teacher request only" access to their device, rather than having it issued into the student's possession.

Administrator-Initiated Accommodations

Noncompliance with the expectations of the Responsible Use Policy can result in the loss of privilege with, or restricted access to, district-provided technology as a consequence for misuse or a safety measure for a particular student. If this is the case, a school administrator will collaborate with the student and parent/guardian to make arrangements that may deny or restrict access to the resource in question. The use of HCS technology is a privilege rather than a right and can, therefore, be taken away from a user who has displayed behavior, or a pattern of behavior, that is considered by an administrator to be potentially unsafe or unhealthy for the user, other students, staff, the technology itself, or the learning environment.

Disclaimer

HCS makes no warranties of any kind, whether express or implied, for the service it is providing. HCS will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

Portions Modified/Quoted from Lebanon Special School District, Lebanon, TN. Legal References: U.S. Const. Amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 et seq.; 20 U.S.C. 6777; G.S. 115C-325(e); HCS Board Policies; and Student Handbooks.

HCS reserves the right to update this Responsible Use Policy at any time deemed necessary. For the most up-to-date RUP, please visit our website www.houston.k12.tn.us.

**PLEASE SIGN & RETURN THIS PAGE TO
YOUR CHILD'S SCHOOL PRINCIPAL**

Student & Parent/Guardian Acknowledgement:

I have received, reviewed, and agree to abide by the Houston County Schools Responsible Use Policy and Technology Handbook for Parents and Students.

Parent/Guardian Signature: _____ Date: _____

Student Signature: _____ Date: _____