

Cypress-Fairbanks ISD High School Laptop Project Parent Handbook 2009-2010



Table of Contents

Purpose of the High School Laptop Project	1
Terms of the Laptop Loan	2
Insurance Fee	3
Table of Estimated Repair Pricing.....	4
Use of Computers and Laptops on the Network	5
General Laptop Rules	6
CFISD Network/Acceptable Use Policy	7-12
Student Code of Conduct	
– Misbehaviors & Consequences.....	12-13
Texas Penal Code §33.02.....	14

Purpose of the Laptop One to One Project

The High School Laptop Project (HSLP) is intended to prepare our graduates for post-high school experiences by providing one year of technology intensive coursework, building technology competency so that students are prepared for the next phase of their lives. Funding for the HSLP was included in the 2007 bond referendum.

Cypress-Fairbanks Independent School District (CFISD) students who are enrolled in the United States History course will be issued a laptop computer to use in the course for a modest insurance fee the student may use the laptop away from school.

Students taking US History will experience a blended delivery of media-rich content, using Moodle, a virtual learning environment designed to facilitate collaboration and creativity. Much of the content will come from lessons on the computer enriched by a wide variety of primary source material. Students will use the primary source material to critically analyze historical events. Technology will play a vital role as US History is brought to life through multimedia such as FDR's famous "Day of Infamy" speech before Congress. Discussion boards and online surveys will afford students the opportunity to collaborate with their peers and share their insights online through tools such as Google Docs. In addition, One Note 2007 will be provided as a technology tool for students to take class notes and learn important study and organization skills. The 24/7 collaborative web environment provides access outside the scheduled class period to facilitate each student's learning. The High School Laptop Project, while not yet a total virtual school, is a good first step towards the vision that the District has of offering virtual courses for students.

Terms of the Laptop Loan

Terms:

In exchange for the right to use the property outside your assigned classroom, you must pay a nonrefundable insurance fee of twenty-five dollars (\$25) on or before taking possession of the property. Once possession of the property has been taken refunds are not allowed. There is a fifty dollar (\$50) deductible for any insurance claim.

You must comply at all times with the Cypress-Fairbanks School District's Parent and Student Laptop Handbooks and Acceptable Use Policy, incorporated herein by reference and made a part hereof for all purposes. Any failure to comply may terminate your rights of possession effective immediately and the District may repossess the property.

Title:

Legal title to the property is in the District and shall at all times remain in the District. Your right of possession and use is limited to and conditioned upon your full and complete compliance with this Agreement and the Parent and Student Laptop Handbooks.

Loss or Damage:

If the property is damaged, lost or stolen, the insurance coverage will cover the loss after the \$50 deductible, unless the damage resulted from abuse or vandalism in which case you are responsible for the reasonable cost of repair or replacement. Loss or theft of the property must be reported to the District immediately, and in no event later the following school day after the occurrence, and a police report regarding the loss or theft must be filed. Insurance WILL NOT pay for an unexplained disappearance or loss in accordance with the insurance coverage.

A table of estimated pricing for a variety of repairs is included in the Parent and Student Laptop Handbooks to which reference is hereby made. You will be required to pay all fees and charges accrued as a result of damage or loss to the property before receiving copies of your school records, and, in some instances, you may also be prohibited from participating in certain school activities.

Repossession:

If you do not timely and fully comply with all terms of this Agreement and the Parent and Student Laptop Handbooks, including the timely return of the property, the District shall be entitled to terminate your rights of possession of the property and physically retrieve the property. The District may also take possession of the property at your place of residence, or other location of the property, or cause a third party, such as law enforcement, to take possession of the property, if required.

Term of Agreement:

Unless earlier terminated by the District, your right to use and possession of the property shall terminate the earlier of the last day of the school year or your withdrawal from the District.

Appropriation:

Your failure to timely return the property and the continued use of it for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property and repossession efforts as stated above may be instituted, including notice to law enforcement of the unauthorized appropriation of the property.

Insurance Fee

Students will pay a non-refundable insurance fee of \$25.

- Students will pay the fee on or before taking possession of the laptop.
- In case of theft, vandalism, and other criminal acts, a police report **MUST** be filed by the student or parent by the next school day following the occurrence. Incidents happening off-campus must be reported to the police by the parent and a copy of the report must be brought to the school.
- If the laptop is stolen and the student reports the theft (by the next school day) and police filed a report, then the student will be charged only the \$50 deductible provided the loss is not an unexplained disappearance or a loss in accordance with the insurance policy, in which case the student and parent must pay the replacement fee of \$860.
- Student will be charged the replacement fee of the laptop if lost, deliberately damaged or vandalized.
- Students/Parents are responsible for the reasonable cost of repair for deliberately damaged laptops (see Repair Pricing chart – Page 4).

Table of Estimated Repair Pricing

Repair	Loss, Deliberate Damage, or Neglect
Broken Screen (LCD)	\$ 290
Keyboard	\$ 22
Power Adapter + Cord	\$ 58
Battery	\$ 99
Re-image of Hard Drive due to violation of Acceptable Use Policy	\$ 15
Abandonment Fee (if eventually found)	\$ 15
Approved Backpack or Laptop Case	\$ 5

The costs of any other parts needed for repairs will be based on manufacturer's current price list.

Use of Computers and Laptops on the CFISD Network

CFISD is committed to the importance of students being able to continue with their work when the laptop is experiencing problems. To assist with this problem the District is providing the following:

Network Student Drives

The students will have a network drive set up from their login account. Students can save important items on this network drive, keeping a backup that they can access from anywhere on the network.

Classroom Computers

The District has desktop and laptop computers in the classroom. These computers can be used by students if they do not have their laptop. They will be able to access their saved work on their network drive.

No Loaning or Borrowing Laptops

- Do NOT loan laptops or other equipment to other students.
- Do NOT borrow a laptop from another student.
- Do NOT share passwords or usernames with others.

Internet Access

There are many sites on the Internet that can be potentially dangerous to minors. These sites are blocked while students are logged on to the District network and while at home through a filtering system provided by the District. Students accessing inappropriate sites will be in violation of District policy.

General Laptop Rules

Inappropriate Content

- Inappropriate content will not be allowed on laptops.
- Instructions for creating weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures will result in disciplinary action.
- There is a \$15 reimaging charge to get rid of any of the above.

Sound

- Students will use the earbuds provided at all times unless permission is obtained from the teacher for instructional purposes.

Deleting Files

- Students may not delete any folders or files that they did not create or that they do not recognize. Deletion of certain files will result in a computer failure and will interfere with students' ability to complete class work and may affect their grades.
- There is a \$15 reimaging charge to correct system files.

Music, Games, or Programs

- Music and games may not be downloaded or streamed over the Internet. This may be a violation of copyright laws.
- All software loaded on the system must be District approved.
- There is a \$15 reimaging charge to delete any unapproved software or files.

CFISD Network/Internet Acceptable Use Guidelines

Network/Internet access is available to students, teachers and staff in the Cypress-Fairbanks Independent School District (“the District”). The Internet is a network connecting millions of computer users all over the world. The Internet enables worldwide connections to electronic mail, discussion groups, databases, software, and other information sources, such as libraries and museums. The District provides Network/Internet access to promote educational excellence in the District by facilitating resource sharing, innovation, and communication. The District firmly believes that the valuable information and interaction available on the Network/Internet far outweighs the possibility that users may procure material that is not consistent with the educational goals of the District.

Network/Internet - Terms and Conditions

Training:

The District will provide training in the proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize legal, ethical, and safe use of this resource.

Risk:

Sites accessible via the Network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. **Although the District will attempt to limit access to objectionable material by using filtering software, controlling all materials on the Network/Internet is impossible.** With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Monitored Use:

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. This monitoring may include activity logging, virus scanning, and content scanning. The District does not provide student electronic mail accounts. The District may allow secure, web-based, student accounts to support instruction. Participation in computer-mediated conversation/discussion forums for instructional purposes must be approved by curriculum and campus administration. The District has provided students with access to “Digital Lockers,” a network storage location for files. The “digital locker” provides an area where certain school-related student products can be stored from year to year, thus creating the student digital portfolio.

To enforce the Student AUP and to maintain the integrity of the network, digital lockers, shared network space, and any District storage space will be monitored by District staff and files such as games, inappropriate images and files will be deleted.

External electronic storage devices are subject to monitoring if used with District resources. Student disciplinary action may follow.

User Responsibilities:

Network/Internet users, (students and District employees), like traditional library users or those participating in field trips, are responsible for their actions in accessing available resources. The following standards will apply to all users (students and District employees) of the Network/Internet:

1. The user in whose name a system account is issued will be responsible at all times for its proper use. Users may not access another person's account without written permission from a campus administrator or District level administrator.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
3. Users may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
4. Students are not permitted to use District technology to search the Internet for non-educational purposes. This includes "free search/surf" the Internet which is defined as unsupervised searching of the Internet without an approved educational purpose.
5. A user must not knowingly attempt to access educationally inappropriate material. If a user accidentally reaches such material, the user must **immediately** back out of the area on the Internet containing educationally inappropriate material. The user must then notify the teacher or campus/building administrator of the site address that should be added to the filtering software, so that it can be removed.

Publishing on the Internet

Recognition:

First and last names and grade level may be used on the Internet to recognize personal achievements. Permission for the following items is granted or denied through the initial Emergency Information and Medical/Parent Authorization form given to each student at the beginning of the school year.

Student Work:

Student work will be published on a CFISD.net web page only with parental permission. Examples of published work could include short stories, poems, slide shows, and/or artwork. First and/or last names may be included with the student work.

Photographs:

Student photographs will be published on a CFISD.net web page only with parental permission. If a photograph of the student is included with the posting of the recognition and/or student work, only the first or last name may be included with the photograph.

Publishing on the Internet

Exceptions to the above:

Any exceptions to the items above will be secured through the Communication Office. Individual campuses may elect not to publish student work and/or photographs on the campus website even though the parent has given permission to do so.

Web Authoring:

The District and each campus have an authorized web site. Students, District employees, and community members are prohibited from authoring a private web site which represents itself as the official site for the District. For example, this would include, but not be limited to, campus, club, and department sites.

Network Etiquette:

Students are not provided District e-mail accounts and are prohibited from accessing unauthorized e-mail services while using District equipment. System users of e-mail or other communication messaging systems are expected to observe the following network etiquette. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited. Transmitting obscene messages or pictures is prohibited. Revealing personal addresses or phone numbers of the user or others is prohibited. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Inappropriate Use:

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations below, that violate the rules of network etiquette, or that hamper the integrity or security of this or any networks connected to the Network/Internet. Please refer to the “Consequences of Violation” section of this document.

Commercial Use:

Use for commercial purposes, income-generating or “for-profit” activities, product advertisement, or political lobbying is prohibited. Sending unsolicited junk mail, or chain letters, is prohibited.

Vandalism/Mischief:

Vandalism and mischief are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data of another user, hardware, peripherals, the District network and Internet, or any networks that are connected to the District network and Internet. This includes, but is not limited to, the creation or propagation of computer viruses. Any interference with the work of other users, with or without malicious intent, is construed as mischief and is strictly prohibited.

Playing Games and Downloading Music or Video Files or Game Files

These activities are prohibited unless approved for educational purposes.

Electronic Mail Violations:

Forgery of electronic mail messages is prohibited.

Reading, deleting, copying, or modifying the electronic mail of other users, without their permission, is prohibited.

File/Data Violations:

Deleting, examining, copying, or modifying files and/or data belonging to or created by other users, without their permission, is prohibited.

System Interference/Alteration:

Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Unauthorized Disclosure:

Unauthorized disclosure, use and dissemination of personal information regarding students and employees are prohibited.

Security

Reporting Security Problems:

If a user identifies or has knowledge of a security problem on the Network/Internet, such as filtering software not working, the user should immediately notify a teacher, administrator, or the System Administrator. The security problem should not be shared with others.

Impersonation:

Attempts to log on to the Network/Internet impersonating a system administrator District employee will result in revocation of the user's access to Network/Internet.

Other Security Risks:

Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the District's Network/Internet.

Violations of Law:

Transmission of any material in violation of any US or state law is prohibited. This includes, but is not limited to: copyrighted material, threatening, harassing, or obscene material; or material protected by trade secret. Any attempt to break the law through the use of a District Network/Internet account may result in litigation against the offender by the proper authorities. If such an event should occur, the District will fully comply with the authorities to provide any information necessary for the litigation process.

Consequences of Violations:

Any attempt to violate the provisions of these guidelines may result in revocation of the user's access to the Network/Internet, regardless of the success or failure of the attempt. In addition, disciplinary action consistent with the District discipline policy and/or appropriate legal action, which may include restitution, may be taken. District administrators will make the final determination as to what constitutes inappropriate use. With just cause, the System Administrator or other administrator may deny, revoke, or suspend Network/Internet access as required, pending the outcome of an investigation.

Computer Software Policy

In accordance with Board Policy EFE (local) and Administrative Regulation EFE-R, it is the practice of the District to respect all computer software copyrights and to adhere to the terms of all software licenses to which the District is a party. Technology Services is charged with the responsibility of enforcing these guidelines. All computer software installed on District equipment must be purchased, reported to, and installed by Technology Services or its designee. Software acquisition is restricted to ensure that the school District has a complete record of all software that has been purchased for District computers and can register, support, and upgrade such software accordingly. Software on District computers used for instructional and/or administrative purposes must be approved by a District curriculum coordinator and Technology Services. Students, District employees, and volunteers may not duplicate any licensed software or related documentation for use either on the District's premises or elsewhere unless Technology Services is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject the employee and/or the school District to both civil and criminal penalties under the United States Copyright Act. Students, District employees, and volunteers may not give software to any third party including relatives, clients, contractors, etc. District employees, students, and volunteers may use District-approved software on local area networks or on multiple machines only in accordance with applicable license agreements.

For further information regarding the purchase and installation of computer software, please call the District's HELP Desk at 281.897.HELP (4357).

DISCLAIMER:

These guidelines apply to stand-alone computers as well as computers connected to the Network/Internet. The District makes no warranties of any kind, whether expressed or implied, for the services it is providing and is not responsible for any damages suffered by users. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its negligence or user errors or omissions. The District is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the Network/Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

1. Consequences

The student in whose name a system account and/or computer hardware issued will be responsible at all times for its appropriate care and use.

Noncompliance with the guidelines published here in the Student Code of Conduct and in Board Policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequence of the Code of Conduct. Violation of

applicable state or federal law, including the Texas Penal Code, Computer Crimes, and Chapter 33 will result in criminal prosecution or disciplinary action by the District.

Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

The District cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of email and network communications are governed by the Texas Open Records Act; proper authorities will be given access to their content.

Student Code of Conduct – Violations & Disciplinary Options

(The following is an excerpt from the Student Code of Conduct.)

LEVEL II VIOLATIONS

Level II violations include those infractions that are more serious in nature and/or a continuation of Level I. These infractions will result in a referral to an administrator. The infractions may occur on school property (including school bus) or during any school-sponsored or school-related activity. Certain Level II violations may be elevated to Level III violations based on the severity or context of the misconduct.

Level II Violations include such behaviors as, but not limited to:

- altering or deleting digital files
- cheating and/or copying (plagiarism) the work of others from any source (Internet, library resources, other students, etc.)
- purchasing, selling or soliciting for sale any merchandise on the school campus without the authorization of the building principal (including the use of Internet resources and/or digital devices)
- violating the District Electronic Devices Policy

Level II - Disciplinary options of which one or more may be used:

- administrator/counselor/teacher/student/parent conferences
- assignment to peer mediation or conflict resolution classes
- campus or community service assignment
- detention after school, during school, or Saturday
- exclusion from extracurricular activities
- grade penalty for copying and/or cheating
- in-school suspension – Discipline Management Class (DMC)
- involvement of law enforcement/security department
- removal from school bus
- restoration and/or restitution, as applicable
- Saturday detention hall
- teacher removal of student from class
- withdrawal of various student privileges

- other appropriate disciplinary actions

LEVEL III VIOLATIONS

Level III violations include those infractions in which the effect or potential effect of the misconduct is disruptive and more serious in nature than Level I or II. Infractions may occur on school property (including school bus) or during any school-sponsored or school-related activity. A violation of this magnitude may result in a student being suspended and/or placed in a disciplinary alternative educational program. The principal or designee will determine the disciplinary consequence used.

Level III Violations include such behaviors as, but not limited to:

- acts of disobedience or disorderly behavior which are detrimental to the school, harmful to health and safety, or inhibit the rights of others such as: harassment, bullying, cyber bullying or creating or possessing a hit list
- misuse of District technology, including, but not limited to, the Internet, the District network, or District-owned equipment or software
- stealing, burglary, robbery, extortion, gambling, or possession of stolen property

Level III Violations include such behaviors as, but not limited to:

- using any device that permits recording the voice or image of another in any way that invades the privacy of an individual or others, or is made without the prior consent of an individual or others
- vandalism and/or defacing District or personal property
- verbally, physically, or via online resources, harassing other students
- any other act that seriously disrupts the orderly process of the school

Level III - Disciplinary options of which one or more may be used:

- confiscation of items such as, but not limited to, lighters, matches, laser pens, and communication devices
- exclusion from extracurricular activities and/or school-sponsored or school-related events
- in-school suspension /DMC
- involvement of law enforcement/security department/citations
- restitution and/or restoration, as applicable
- removal from school bus
- removal to a Disciplinary Alternative Education Program (Transportation is not provided.)
- school or community service assignment
- suspension for up to three (3) days per occurrence of misconduct (suspensions at home)
- other appropriate disciplinary options

Texas Penal Code

§33.02. Breach of Computer Security

- (a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
- (b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:
 - (1) a Class A misdemeanor if the aggregate amount involved is less than \$1,500
 - (2) a state jail felony if
 - (A) the aggregate amount involved is \$1,500 or more but less than \$20,000; or
 - (B) the aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;
 - (3) a felony of the third degree if the aggregate amount involved is \$20,000 or more but less than \$100,000
 - (4) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or
 - (5) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.