Technology and Electronic Communications Use and Procedures

Hardee District Schools provides and promotes technology use, by furnishing resources to its students and staff for educational and administrative purposes. The goals in providing these resources are to promote educational excellence in Hardee County Schools by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff.

Proper behavior as it relates to the use of computers is no different than proper behavior in all other aspects of the activities of Hardee District Schools. Users are expected to utilize computers and computer networks in a responsible, ethical, legal, and polite manner. While using the Hardee District Schools Technology and Electronic Communications you must observe the following:

School District Property:

The computer system is the property of Hardee District Schools and is intended to be used for approved school business purposes only. Users should have no expectations of privacy accessing the district's network from on-site or off-site locations and should not use the district's equipment or network for personal use from office or home.

No Expectation of Privacy:

The school district, as providers of the computer equipment and servers, is given the right to monitor your school communications when you use the district's computers. This statutory authority is given to ensure the appropriateness of school communications and to allow random computer system checks.

Public Records:

The users of the school district's computers recognize they are bound by state public record laws, and documents, that are created to formalize knowledge or transact business of the school district, are considered public records and are open to the review and copying by the general public. These include all work records on your computer system, data transmitted over the district network from on-site or off-site locations, and portable media such as disks, floppy disks, CDs and any other transportable media. All records must be retained according to Florida public records statute.

General Rules and Guidelines:

All web pages, created by staff, students, and student organizations on the district's computer system, will be subject to treatment as district-sponsored publications. Accordingly, the district reserves the right to exercise control over such publications.

Electronic Mail – (Email)

Email is not a confidential medium. It can be reviewed by others and should be used only for legitimate educational or district purposes.

Email may be monitored; there is no guarantee of privacy when using any school technology.

Outside Email is strictly prohibited. (i.e., Hotmail, Yahoo mail, etc)

Deleted E-mail - Please understand that when you press the delete key, your e-mail is not actually deleted. The space is marked as free space but may or may not be overwritten. Your old Email can easily be retrieved from your hard drive,

server or other backup devices by a computer forensic specialist or other person.

There is sophisticated software that mines all your Email and other documents. Modification, damage, or removal

Users shall not modify, damage, or remove electronic communications resources that are owned by Hardee District Schools or other users without proper authorization.

Hardee District Schools will not be responsible for any damages suffered through the loss of data. The district is not responsible for the accuracy or quality of information obtained through the Internet.

Damage caused by intentional misuse of equipment will be charged to the user Hostile working environment Users shall not use electronic communications resources in a manner that creates a hostile working environment (including sexual or other forms of harassment), or that violates obscenity laws.

It is incumbent upon the employee as a computer user to familiarize themselves with the basics of what specific communication triggers sexual harassment, other harassment, copyright, trademark and other relevant computer abuse laws. Lack of knowledge is not a defense to computer abuse or violation of laws.

Security

Encroaching on others' access and use - Users shall not encroach on others' access and use of Hardee District Schools electronic communications resources. This includes but is not limited to: the sending of chain-letters or excessive messages; printing excessive copies; running grossly inefficient programs when efficient alternatives are available; unauthorized modification of electronic communications resources; attempting to crash or tie up electronic communications resources.

Passwords - Passwords are for internal use and are not allowed to be distributed to anyone without the express permission of MIS Network Security. Additionally, passwords do not create an expectation of privacy when it comes to employer monitoring, and internal and criminal investigations. Users are responsible for safeguarding their own passwords, and will be held accountable for the consequences of intentional or negligent disclosure of this information.

Unauthorized or destructive programs - Users shall not intentionally develop or use programs such as, but not limited to: viruses, backdoors, logic bombs, Trojan horses, bacteria, and worms that disrupt other users, access private or restricted portions of the system, identify security vulnerabilities, decrypt secure data, or damage the software or hardware components of an electronic communications resource. Hardee District Schools recognizes the value of research and

education in game development, computer security, the investigation of self-replicating code, and other similar pursuits. Such legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized to the extent that the pursuits do not compromise Hardee District Schools electronic communications resources.

Remote Access - The use of communications software that provides the ability to remotely "take over" a network-connected PC is prohibited unless authorized by

MIS Network Security. If it is used, it should be strictly controlled by the local administrator and user. It should be turned on only when support is needed (and the user has given permission, if applicable) and immediately turned off once the support has been provided.

Any software that has been designed to allow unauthorized persons to infiltrate computers on the network, view and modify data, spy on a user's keystrokes in an effort to get user ids and passwords, etc is prohibited. MIS Network Security reserves the right to randomly scan or monitor any computers attached to Hardee District Schools County network in an effort to detect the presence of such software or irregular operations that may be present on the network. MIS also reserves the right to disconnect any device or user on the network that appears to pose a threat.

Unauthorized equipment

Users shall not install or attach any equipment to a School District of Hardee electronic communications resource without the explicit approval of the site administrator or MIS Network Security for that electronic communications resource. This includes cordless phones and cell phones..

Unauthorized Use of Applications

Games, chat sessions and instant messenger applications - These applications are prohibited on Hardee District Schools network unless there is a legitimate educational purpose and prior approval. Chat and instant messenger applications can tie up a great deal of bandwidth and may be used by students for many inappropriate purposes. In particular, students can easily be put in contact with persons who may be a threat to their safety.

MPEG files (including the MP3 and MP4 formats) - MPEG files are audio and video files digitized and/or compressed into a format that can be read and transferred by a computer. Downloading or storing files of these or any other formats that do not have any educational value is prohibited. These files, though greatly compressed, are still fairly large and can tie up a great deal of bandwidth and computer storage. In addition, most have been illegally copied and infringe on copyrights owned by the artists and record/movie companies. Users should be aware that record/movie companies are notifying the district when an MPEG file of copyrighted material has been downloaded and what location received it.

Copyright and Trademark Infringement

Copyright Infringement - No computer user can upload, download, transmit to another computer, print a hard copy or any way infringe upon the exclusive rights of reproduction, distribution, adaptation, public performance and public display of an on-line or off-line copyrighted work. Not all works on the Internet or Intranet are in the public domain. The computer user must check with the site administrator if there is any uncertainty whether an article or software is copyrighted. Additionally, it is a violation of the Digital Millennium Act to remove any copyright management information (e.g. title, author name, date of registration). There are serious civil and criminal penalties for violating the Federal copyright laws and international copyright treaties.

Trademark Infringement - No symbol, logo, phrase or other trademark from a document, website, or other source can be uploaded, downloaded, linked or in any way transmitted to another computer without the express permission of the trademark owner. Trademark infringement carries stiff civil and criminal penalties.

Hardee District Schools Network Security:

Hardee District Schools Internet content filtering technology limits the kinds of Internet sites that can be viewed on Hardee District Schools Internet connection. Pornography sites, sites advocating violence or bigotry, sites with games, hacking tools, and cracked software (software that has had its internal security broken and has been made available to others) are examples of what will be blocked. There will be no bypassing of Hardee District Schools Internet content filtering without MIS Network Security authorization. Internet content filtering audit logs showing Internet activity and sites visited by users will be reviewed on a regular basis.

Administrative computers are defined as non-classroom computers on which Hardee District Schools requisition and business functions, staff Email directives, staff tasks, etc. are stored and/or viewed. These computers should be kept physically and virtually separate from instructional computers. Students are not to have access, either physical or virtual, to production servers or any administrative computers.

Every effort should be made to secure classroom machines on which student testing, test grading and evaluation, grade book activities and staff Email functions are carried out. This includes installing application passwords and timeouts, up-to-date anti-virus software, possible storage of grade and test data on removable media, and limiting unsupervised student access as much as possible. Individual student accounts or common student accounts (STUDENT01, etc.) should be separate from teacher accounts.

All administrative computers and server consoles that are used to access or control sensitive data should have a screen saver timeout and password after a specific period of inactivity or some other lockout mechanism to prevent unauthorized persons from accessing these environments. These computers may also have boot-up passwords.

Classroom computers are defined as computers used by students or servers that connect instructional computers. There are to be no administrative applications, especially mainframe sessions, installed on any of these computers or servers.

Outside access to Hardee District Schools networks should only be through “hardened” web servers. This means that web servers should have no other applications running on them and should not connect easily to the rest of Hardee District Schools network.

Personally owned computing devices such as desktops, laptops or personal digital assistants (PDA’s) should not be connected to Hardee District Schools network without approval. These devices may have applications, configurations, viruses, etc. that could pose a risk to the network. MIS Network Security may grant approval after, as time permits, certifying the device is not a threat to district networks.

Technology and Electronic Communications Use and Procedures

School and district bulletin boards will be setup as closed forums for the sole purpose of information dissemination to district employees.

Users will not transmit confidential information concerning students or others over systems not designated for that use, and will use care to protect against negligent disclosure of such information.

Network accounts are to be used only by the proper authorized owner of the account.

Any use of the network for commercial, personal, or private business is prohibited.

Any use of the network for product advertisement, political lobbying, or non-secular promotion is prohibited.

Users must be aware of the finite capacity of the network and must cooperate with the MIS Network Security.

Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users or misrepresent other users on the network.

All communications and information accessible via the network should be assumed to be public record.

Use of the network shall not disrupt other users on the network; hardware or software shall not be destroyed, modified, or abused in any way.

Malicious use of the network to write programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

Hate mail, harassment, discriminatory remarks, profanity, obscenity, or language which may be offensive to another are prohibited on the network.

The illegal installation of copyrighted software for use on any district computer is prohibited. Installation of district software on home computers is prohibited unless approved by MIS Network Security.

Any violations of the use of the Internet shall be reported to the assigned teacher or technology facilitator and the assigned administrator.

Users are responsible for keeping copyrighted software of any kind from entering the local area network via the Internet.

The user shall maintain the integrity of the district network. The user is responsible to report all violations. The user is also responsible for making sure all Email/web pages sent or received by him/her does not contain pornographic material, computer viruses, or files that are potentially dangerous.

Users shall log in/out correctly from all network connections.

All student Internet connections must be monitored by a teacher, technology facilitator, or administrator.

Users do not own accounts on Hardee District Schools computers, but are granted the privilege of exclusive use of their accounts. Use of the network does not alter the ownership of data stored on the network.

Remote Use of Computers:

Use of computers away from the traditional business site includes but is not limited to: home, car, hotel, cell phone, personal digital assistants and other off-

site locations. You have no expectation of privacy at off-site locations. Additionally, you must adhere to all the same policy restrictions as if you were using the computer on-site. Remote computer usage carries a higher duty of care and responsibility. All off-site computer communication must have a district purpose and should be properly secured with anti-virus and firewall protection.

Laws and Regulations:

All existing laws (federal and state) and School District of Hardee regulations, policies, and standards of professionalism and civility apply, including not only those that are specific to computers and networks, but also those that may apply generally to personal conduct. These include but are not limited to: the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section1232[g]), the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), and the Florida Computer Crimes Act (FS Chap. 815) . Illegal reproduction of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment. The UM School of Law supports the policy of EDUCOM on Software and Intellectual Rights.

Hardee District Schools policy shall support and help protect all students as outlined under the Federal Children's Internet Protection Act. In relation to this act, Hardee District Schools will diligently work to do the following:

- Limit access by minors to inappropriate materials on the Internet and World Wide Web;
- Maintain the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Limit unauthorized access and other unlawful activities by minors online;
- Limit unauthorized disclosure, use, and dissemination of personal information regarding minors, and;
- Limit materials that may be harmful to minors.

Litigation:

In the event of litigation, all computer users are on notice that federal and state civil rules of procedure may allow discovery of all computer hardware and software. This includes but is not limited to your office computer, laptop, home computer, printers, cell phones and other electronic equipment. Any attempt to damage or destroy evidence in your computer will trigger stiff civil and criminal penalties (known as spoliation claims). If your computer equipment is subpoenaed or you anticipate litigation, contact your site administrator for guidance on how to proceed.

Amendments:

This policy may be amended or revised from time to time as need arises. Users will be provided with copies of all amendments and revisions.

Effective Date: 1-20-2006