Hendry County School District

Information Technology Policy and Procedures for District Employees

300 W. Cowboy Way
LaBelle, FL 33935
(863) 674-4559
www.hendry-schools.org

6/22/2021

Table of Contents

1.0 Overview 3

2.0 Purpose 3

3.0 Scope 3

4.0 Acceptable Use Policy 4
- 4.1 General Use and Ownership 4
- 4.2 Security 4
  - 4.2.1 Passwords, Accounts, and Antivirus 4
  - 4.2.2 Network Security and Administrator Rights 5
- 4.3 Sensitive and Confidential Information 6
  - 4.3.1 Definition and Protection 6
  - 4.3.2 Access and End User Support 7
- 4.4 Guest and Vendor Access 7
- 4.5 Portable Device User Policy (Laptops\Tablets, etc.) 8
- 4.6 Revocation of Privileges 8

5.0 Unacceptable Use 9
- 5.1 Unacceptable Use: System and Network Activities 9
- 5.2 Unacceptable Use: Email and Communications Activities 11

6.0 Social Media Expectations 11
- 6.1 District/Professional Use of Social Media 12
- 6.2 Personal Use of Social Media 12

7.0 Security Incidents 13
- 7.1 Definition 13
- 7.2 Response 14
- 7.3 Monitoring 15
  - 7.3.1 Devices and Applications 15
  - 7.3.2 Files and Correspondence 15

8.0 Data Loss Prevention 16

9.0 Purchasing 16

10.0 Inventory 17

11.0 Rostering Software Programs 17

12.0 Requesting Extensions and Applications 17

13.0 Relocation of Equipment 18

14.0 Disposal of Technology Equipment 18

15.0 Enforcement 18

16.0 Revisions 18

Appendix A 19

Acceptable Use Policy (AUP) for Faculty and Staff 19

Appendix B 21

Non-Student/Non-Staff Guest Access and Usage Agreement Form 21

Appendix C 22

Portable Device Usage Agreement 22

Appendix D 23

Request for Social Channel Account Form: 23

Appendix E 24

Software Rostering Request Form 24

Appendix F 26

Extension or Application Request Form 26

1.0 Overview

The IT Department's intention for publishing Policies and Procedures is to provide clear guidelines and expectations aligned with the established mission of providing users with the best resources possible to educate every student.

The IT Department is committed to protecting Hendry County School District's users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of Hendry County School District. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of Hendry County School District.

Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every Hendry County School District employee and affiliate is required to meet and exceed the standards set forth by Florida State Law, Federal Law, the Hendry County School Board and administrators. It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems and technology within the Hendry County School District. These rules are in place to protect the students, staff, and the Hendry County School District. Inappropriate use, improper planning, and disregard of these procedures exposes Hendry County School District to risks including compromise of network systems and services, possible damage to the network, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporary employees, authorized guests, and other workers at Hendry County School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Hendry County School District including all future purchases.

4.0 Acceptable Use Policy

4.1 General Use and Ownership

Users should be aware that the data they create on the network remains the property of the Hendry County School District. Users should have no expectations of expressed or implied privacy.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for following guidelines established by the IT Department concerning personal use of Network/Internet systems. Improper use could result in termination of network services and/or the removal of technological devices.

Using the Hendry County School District network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.

The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.

The Hendry County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Hendry County School District while on the network. If personal devices (laptops, printers, etc) are connected to the network without prior authorization from the IT Department, they will be confiscated and will not be returned.

For security and network maintenance purposes, the IT Department may monitor equipment, systems, and network traffic at any time.

The Hendry County School District's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security

4.2.1 Passwords, Accounts, and Antivirus

Users, which includes employees and guests of Hendry County School District, will be granted access to the network after they have signed the appropriate Network Usage Agreement forms via the digital documentation provided. (see Appendix A, Appendix B, and Appendix C for preview).

Users must keep passwords secure and should not share their accounts. Authorized users are responsible for the security of their passwords and accounts.

Users shall not leave computers unattended while logged on.

Users of Windows based computers will be required to change their passwords every 60 days as prompted automatically by Windows Active Directory.

Users needing password resets for various programs must utilize the Password Reset Site (See Appendices). If a user has failed to register into the Password Reset Site prior to requiring its use, then the user must submit an online IT HelpDesk Ticket.

Every attempt will be made to identify the user by positive identification. This method may include sight/voice reconciliation, a predetermined security question, or other questions as determined by the Director of IT.

All computers used by employees or guests that are connected to the Hendry County School's network, whether owned by the user or Hendry County School District, shall be continually executing virus-scanning software with a current virus database.

Users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, ransomware, or Trojan horse code.

4.2.2 Network Security and Administrator Rights

Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential and known only by the IT staff members that need them to perform their duties. Distributing passwords of any kind is strictly forbidden.

Wireless access points will be secured with a security key to be determined by the Technology Director. Any attempt to bypass and/or distribute security keys is strictly forbidden.

Users of Hendry County School District devices may be granted Administrative Rights to those devices. This access will be given as needed to perform job duties. It is the responsibility of the user to not install or download programs that may affect the performance of the device. This privilege may be revoked. The Director of IT or his/her designee will determine if there is another alternative before granting such rights. To satisfy security and audit purposes, other alternatives will always be used when possible.

4.3 Sensitive and Confidential Information

4.3.1 Definition and Protection

When handling sensitive and confidential information, precautions must be taken to prevent unauthorized access to the information. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or other confidential student and user data.

Access to student data is limited by Statute. Section 1002.22(3) (d) F.S. guarantees every student a right of privacy with respect to his or her educational needs. In addition the Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 123g; 34 CRF Part 99 protects the privacy of student educational records and applies to all schools that receive funds from the Department of Education.

All users who have access to or may have access to personally identifiable student and user records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Hendry County School Board Policies and Procedures, and all other applicable State and Federal laws and regulations, as they relate to the release of such information.

Below are the guidelines that must be followed where applicable:

- Encrypt data;
- Password protect data;
- Physically protect devices that can be easily moved such as Portable devices that are used to access sensitive data;
- Avoid creating files that use social security numbers as identifiers. Use employee numbers and/or the student local identification number instead;
- Never download or copy sensitive data to your home computer;
- Never store unencrypted data on a portable device; and
- Protect printed sensitive data. Store sensitive data in locked desks, drawers or cabinets. Do not leave unattended sensitive data on the copier, FAX, or printer. Shred sensitive data that needs to be disposed of.

Contact a school administrator, department supervisor, or district administrator when questions arise regarding protected data.

4.3.2 Access and End User Support

Sensitive data access is restricted to only those personnel who need to perform their job duties. Access restrictions to such data are maintained by the IT Department in conjunction with the Finance Department, the Human Resources Department, the Superintendent of Hendry County School District, and the School Board.

Access to sensitive information is only granted at the request of an administrator with an accompanying and verifiable need. Reviews of accesses and privileges are conducted regularly and monitored to ensure compliance with all School Board Policies as well as State and Federal Laws and regulations.

4.4 Guest and Vendor Access

Guest and Vendor access will not be granted to any Hendry County School District network or network device without a signed and approved vendor contract or a Guest Access Agreement Form (Appendix B).

Using the Hendry County School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all School Board policies and procedures, Florida State law, and Federal laws.

The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.

The Hendry County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Hendry County School District while on the network. The Hendry County School District IT staff can only provide limited support in aspects of network connectivity and access to network resources.

Backing up data and ensuring the security of network devices are the sole responsibility of the owner.

Vendor supplied user ID's, program passwords, guest accounts, and security devices are administered by the IT Department. This information and these devices are kept secure from general users unless knowledge of them is imperative to the course of their job.

4.5 Portable Device User Policy (Laptops\Tablets, etc.)

Users that are issued portable devices by the Hendry County School District must sign a Portable Device Usage Agreement form upon receipt of the device (see Appendix C). Portable Devices must be from the approved list of devices that are available for use. Any other device will not be supported nor allowed network access.

Users will be responsible for the security of the device while assigned to them whether on or off campus.

Users must understand that issued portable devices are property of Hendry County School District and must be returned in their original condition with all accessories upon request.

Users assume all risk of injury or harm associated with the use of the device off-premises, including but not limited to, physical damage or loss, or personal injury.

While portable devices are being used off campus, the Hendry County School District has no control over the information accessed through the internet and cannot be held responsible for content viewed.

Hendry County School District and its users will not be held liable for claims or damages that may arise from the use of issued portable devices while not on school property.

4.6 Revocation of Privileges

Privilege and access to all Hendry County School District network devices, software, email, and information systems will be revised or revoked as necessary in the event of the following:

- Transfer of employee;
- Resignation of employee;
- Termination of employee;
- Termination of vendor contract;
- Purposeful tampering or alteration of property, network, or network peripherals;
- Termination of consulting contract; or
- In the event of an investigation of an employee, vendor, or consultant where revision or revocation of privileges and access is necessary.

5.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

Under no circumstances is an employee, student, or authorized guest of Hendry County School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Hendry County School-owned resources, to include the network and Internet.

Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others.

Attempts to circumvent or defeat mechanisms put in place by the Hendry County School District staff to manage the network is strictly forbidden.

Users shall not attempt to download and/or install services, electronic file sharing, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, and .msi. The list below is not exhaustive, it does, however, provide a framework for activities which fall into the category of unacceptable use.

5.1 Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Physically accessing the network infrastructure hardware. Although network hardware components are accessible, under no circumstances, should anyone attempt to modify and/or touch these components;
- No one should try to conceal, block, or hide the network hardware that is accessible. There should be no covering and/or objects placed over, around, above, etc any network hardware and/or component in any room. This includes, but is not limited to fabrics, flags, drapes, statues, trophies, etc.;
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Hendry County School District;
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted

software for which Hendry County School District or the end user does not have an active license is strictly prohibited;

- Using district devices and/or networks for commercial or private financial gain;
- Using district devices and/or networks for product advertisement or political campaigning;
- The exporting of software, technical information, encryption software and/or technology;
- The introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home;
- Using a Hendry County School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;
- Making fraudulent offers of products, items, or services originating from any Hendry County School District account; and
- Effecting security breaches or disruptions of network communication.

  Security breaches include, but are not limited to:
  - Accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
  - Port scanning or security scanning unless prior notification and approval is received beforehand;
  - Executing any form of network monitoring unless prior notification and approval is received beforehand;
  - Circumventing user authentication or security of any host, network or account;
  - Interfering with or denying service to any user other than the user's host (for example, denial of service attack);
  - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the network/Internet; and

- Providing information about, or lists of, Hendry County School District's users to parties outside the Hendry County School District without prior permission from the Superintendent of Schools.

5.2 Unacceptable Use: Email and Communications Activities

Under Florida law, e-mail addresses are public records. If you do not want your email address released in response to a public records request, do not send electronic mail.

The following are all prohibited on the District network:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages (shall include forms of harassment via social networks);
- Unauthorized use, or forging, of email header information;
- Solicitation of email or any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type. Use of unsolicited email originating from within Hendry County School District's networks of other internet/network service providers on behalf of, or to advertise, any service hosted by Hendry County School District or connected via Hendry County School's network; and
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.0 Social Media Expectations

The Hendry County School District recognizes that many of our staff, students, parents, and community members are active social media users. Actively participating in these digital environments is an integral part of 21st century learning. These guidelines are intended to provide protection for both the employee's reputation and that of the Hendry County School District. These guidelines complement, but do not replace, any existing policies regarding the use of technology (Acceptable Use Policy) including computers, email, and the Internet that are currently in place in the Hendry County School District. By accessing, creating or contributing to sites such as Facebook, Twitter, LinkedIn, YouTube, blogs, wikis, podcasts, or any other form of online activity, you agree to abide by these guidelines.

6.1 District/Professional Use of Social Media

Although each school or department operates its own social media outlet, all District social media accounts are a voice for our district. A central database compiled by the IT Department ensures continuity in social media. Schools and teachers who use social media accounts as part of their communication strategy must provide the names of social media administrators as well as their phone numbers and e-mail addresses on a Social Media Account Form (Appendix D) to their building administrator, who will send that information to the IT Department. Accounts should be created using your Hendry Schools email account. In the event of an emergency this information will be helpful if the administrator of the page is not available to take care of the emergency in a timely manner. This information will be kept strictly confidential and used only for access during emergency situations.

In addition, official school and department social media outlets should be managed by a district employee/administrator, NOT external/volunteer representatives (i.e. PTA, PTO, booster clubs, etc.).

Parent Opt Out: Parents must be given the opportunity to opt their student(s) out of participating in social media sites. Social media sites are not to take the place of any regular communication about assignments nor should it be required.

6.2 Personal Use of Social Media

The Board respects the right of employees to use social media as a medium of self expression on their personal time. As role models for the school system's students, however, employees are responsible for their public conduct even when they are not performing their job duties as employees of the school system. Employees will be held to the same professional standards in their public use of social media and other electronic communications as they are for any other public conduct. Further, school employees remain subject to applicable state and federal laws, Board policies, administrative regulations and the Code of Ethics for Florida Educators, even if communicating with others concerning personal and private matters. If an employee's use of social media interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment.

Employees are responsible for the content on their social media sites, including content added by the employee, the employee's friends or members of the public who can access the employee's site, and for Web links on the employee's site. Employees shall take reasonable precautions, such as using available security settings, to restrict students from viewing their personal information on social media websites and to prevent students from accessing materials that are not age-appropriate. Any use of electronic social media by employees

during the school day must be limited and must not interfere with job duties. Any use of school system technological resources (including computers and cell phones) must be in accordance with the Code of Ethics and the Code of Professional Practice and Conduct for Florida Educators.

District procedure discourages employees from "friending" or "following" students, unless a student is also a family member. Procedures also discourage "friending" or "following" parents of students. The following response is recommended when denying such requests:

> *As an employee of Hendry County Schools, practice discourages me from 'friending' or "following" students or parents. I would encourage you to 'like' our school/classroom/district account.*

7.0 Security Incidents

7.1 Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- Loss of information confidentiality (data theft);
- Compromise of information integrity (damage to data or unauthorized modification);
- Theft of physical IT assets including computers, storage devices, printers, etc.;
- Denial of service;
- Misuse of services, information, or assets;
- Infection of systems by unauthorized or hostile software;
- An attempt at unauthorized access;
- Unauthorized changes to organizational hardware, software, or configuration; and
- Reports of unusual system behavior, etc.

7.2 Response

If a District staff member becomes aware of a security incident, they must provide notification of the incident to the IT Department. Upon confirmation, the Administrator of IT will notify the user's supervisor (if a Hendry County School District employee) or School Administrator (if a Hendry County School District student).

Other steps that may be taken:

- Temporarily suspend or restrict the user's computing privileges during the investigation;
- Remove the affected computer device, as appropriate, from the network; and
- Reactivation is at the discretion of the Director of IT.

These steps may be taken only after authorization by the Administrator of Technology unless the situation represents an emergency or immediate threat to network security/integrity. In such a case, the IT Technician must take corrective action and notify the Administrator of IT as soon as possible. Actions should be taken in such a way that any impacts to non-offending users are minimized.

IT Technicians are responsible for notifying the Administrator of IT of any observed violations of Hendry County School District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

IT Technician must report any computing incidents which clearly compromise network integrity

Security incidents include but not limited to:

- Notification by outside institutions or individuals of any incident;
- Data loss or theft.\;
- Inappropriate systems or information access or use;
- Any other breach or violation of IT policies of which they become aware; and
- Material changes in network architecture or administration.

IT Technicians, when requested, are expected to cooperate fully with the Administrator of IT in any investigation, identification, and resolution of network incidents.

IT Technicians are not responsible for the content of files, images, video or audio clips, electronic communications, and news postings produced by others.

The IT Technician is also not responsible for unauthorized software installed by others.

7.3 Monitoring

7.3.1 Devices and Applications

In an effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department, at the discretion of the Director or Administrator of IT, can and will monitor network activity. These monitoring devices/applications include but are not limited to:

- Firewall logs;
- Web Filtering logs;
- Network Traffic Monitoring;
- Active Directory Monitoring;
- Mail Scanner logs;
- Database, backup, and usage logs on servers; and
- Event logs and histories created in individual machines.

7.3.2 Files and Correspondence

In the course of their duties, it may be necessary for IT Technicians to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user, protect the security and integrity of the Hendry County School District's network, protect the rights or property of Hendry County School District or third parties, or to ensure compliance with Hendry County School District policy or applicable law.

Examples include:

- The identification/restoration of lost, damaged or deleted files;
- The identification of a process that is interfering with normal network functions; and
- In more serious circumstances, an investigation of a Security Incident.

In all such cases, the IT Technician shall take into consideration the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with. The Administrator of IT must be advised of and approve any non-routine monitoring that occurs. Non-routine monitoring includes directed investigations of potential policy and/or security violations. Discovery of such violations in the course of routine monitoring must be reported.

8.0 Data Loss Prevention

To prevent data loss from a disaster, the IT Department will follow all disaster policies and guidelines set forth by the Hendry County School District. In addition, the IT Department will take routine measures to protect and restore critical on-site systems by performing daily, weekly and monthly backups and storing backups in two separate and secure locations. Contracts for information systems off-site include data loss protection plans and disaster recovery plans as a rule before approval.

In the event of immediate threat the IT Department will take the following actions:

- Backups will be performed and stored in both locations if possible;
- Most servers, except mission critical servers (Active Directory), will be shut down;
- Information will be provided on the Hendry County School District website;
- Network closets and battery backups (UPS) should be turned off if unnecessary; and
- In the event the MIS building is damaged or destroyed, operations will be reestablished at one of the schools or department buildings;

Additionally, each school and district office department should take the following steps to protect data and equipment:

- Computers should be turned off and unplugged, if connected to battery backups these should be turned off and unplugged as well; and
- Computers should be moved away from windows, off the floor, and covered with plastic if possible.

Please see Hendry County School Board's Disaster Recovery Plan for additional information including Disaster Response team and recovery in the event of a disaster.

9.0 Purchasing

The IT department is responsible for the seamless integration of any hardware or software into the existing network system and maintaining an inventory of all such items. When considering the purchase of any technology related item, prior approval from the IT Department is required and requested items must be selected from the approved list of devices. Please contact the IT Department for a current list of approved devices or to inquire about purchasing products that are not already District approved. If this is circumvented in some manner through grant purchasing or other funding sources, the IT Department will not permit these devices to connect to the Hendry County School District Network nor will these devices be supported by the IT Technicians.

10.0 Inventory

The IT Department maintains inventory of all technology devices within the district. After an item is purchased it must be added to the inventory system prior to being placed in the classroom, office or delivered to a student or employee. The procedures for inventory are as follows:

- Receive approved equipment;
- Label equipment with appropriate barcode;
- Scan barcode into inventory system (Destiny Resource Manager); and
- Enter ALL item details pertaining to equipment within the system.

Ownership of entering the inventory information is dependent on the equipment. The following Departments are responsible for entering the inventory information:

- Department or School/Classroom Equipment - Department or School
- Teacher chromebooks - IT Department
- Student Chromebooks - IT Department

11.0 Rostering Software Programs

The IT Department is responsible for the integration of District approved software purchases into the existing network system. Creating student and staff accounts and providing access to these programs falls under this responsibility. A Software Rostering Request Form (See Appendix E) must be submitted at a minimum of two weeks before access to any program is to be expected. Once rostered the program may take 24-48 hours to fully sync with our systems. The software program must also have already been approved by the District Technology Committee and relevant Director of Schools. The IT Department will not roster any requested software applications or programs that have not gone through this process.

12.0 Requesting Extensions and Applications

Third party extensions and applications could pose a security risk to the District network and the privacy of its users. Therefore, all extensions and applications must be requested through the Extension and Application Request Form (See Appendix F). These requests must be submitted at a minimum of two weeks before access to any extension or application is to be expected. The extension or application must be approved by the school site administrator and must be installed by grade, school, or district level only. Individual account installations are not allowed unless mandated by an Individualized Education Plan (IEP) or 504 Plan.

13.0 Relocation of Equipment

When considering the relocation of any technology related item, prior approval from the IT Department is required. Please contact the IT Department for approval. If equipment is relocated without prior approval the IT Department will not service said equipment due to any error caused by relocation nor will they incur or cover any repair expenses associated with this relocation.

14.0 Disposal of Technology Equipment

All technology equipment must be disposed of in a manner that adheres to all State and Federal Laws as well as Hendry County School Board Policy. You must submit a HelpDesk ticket to dispose of technology.

15.0 Enforcement

Failure to adhere to these policies and guidelines may result in suspension or revocation of the offender's privilege or access to the network, confiscation of Hendry County School District property, and/or other disciplinary or legal action.

16.0 Revisions

The Hendry County School Board reserves the right to revise these policies and procedures at any time to ensure the operability and safety of the network and its users.

Appendix A

Hendry County School Board

Acceptable Use Policy (AUP) for Faculty and Staff

TERMS AND CONDITIONS AGREEMENT

To access the Network/Internet through the District's computers/network, employees must sign and return this Agreement on an annual basis to the Director of Information Technology. The signed agreement is to be archived at the user's local site and in the IT Department of the School Board building.

Use of the Network/Internet is a privilege, not a right. The Board's Network/Internet connection is provided for business, professional and educational purposes only. Personal files need to be saved on your own personal storage devices. DO NOT save/place personal files and/or software on computers belonging to the Hendry County School Board. Unauthorized or inappropriate use will result in a cancellation of this privilege.

The District has implemented Technology Protection Measures which is a specific technology that will protect against (e.g., block/filter) Internet access to visual displays that are obscene, pornaraphic, or harmful to minors.

Staff members accessing the Network/Internet through the District's computers/network assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Network/Internet.

The District reserves the right to monitor, review and inspect communications, files and/or messages residing on or sent using the District's computers/networks. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

The staff member agrees to abide by local, state, federal, and School Board regulations.

It is the responsibility of each staff member to use due diligence in keeping the District's network resources secure. This includes but is not limited to keeping **confidential all passwords** assigned for use of District computing resources.

As a staff member of the Hendry County School District, I understand that any misuse of equipment that results in the loss, damage, or vandalism is to be paid for by the staff member.

(continued on next page)

I have read and agree to abide by the District IT Policies and Procedures. I understand that any violation of the terms and conditions set forth in the Policy is inappropriate and may constitute a criminal offense and/or employment violation. As a user of the District's computers/network and the Network/Internet, I agree to communicate over the Network/Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

_____ _____

Staff Member's Full Name **(please print)**: School/Department

_____ _____

Staff Member's Signature Date

The Superintendent, or designee, is responsible for determining what is unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the District's Staff Network and Internet Acceptable Use and Safety Policy and related Procedures and take such other disciplinary action as is appropriate pursuant to the applicable collective bargaining agreement and/or District Policy.

Appendix B

Non-Student/Non-Staff Guest Access and Usage Agreement Form

The Hendry County School District (HCSD) welcomes anyone whose intentions it is to better the lives and education of our students. In this effort we have created policies regarding the use of portable devices and other electronic equipment not belonging to the HCSD on the HCSD network.

Using the HCSD network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all School Board policies and procedures, Florida State law, and Federal laws.

The use of excessive bandwidth, reproduction of copyrighted materials, and attempts to circumvent or defeat mechanisms put in place by the HCSD staff to manage the network is strictly forbidden and will result in the termination of network services.

The HCSD assumes no responsibility for costs associated with loss or damage to devices not owned by HCSD on the HCSD network. The HCSD staff can provide support in aspects of network connectivity and access of HCSD network resources. Backing up data and ensuring the security of network devices is the sole responsibility of the owner.

The HCSD has the right to rescind privileges and or change this policy in the future.

Please sign below to acknowledge that you have read, understand, and agree to adhere to these policies.

Guest printed name:_____

Reason for Access: _____

_____ _____

Guest Signature Date

Start Date: _____

End Date: _____

Guest Hendry Wifi Key: _____

Appendix C

Staff Portable Device Usage Agreement

Check Out Guidelines

Laptop/tablet/iPad/etc (Devices)

Hendry County School Board ("HCSB") devices may be issued to individuals for job related activities.

Guidelines for using a HCSB device:

1. If taking the device home, you are responsible for the care and maintenance of the device. You are responsible for the replacement cost of the device if it is lost.
2. If theft of the device occurs when you have removed it from campus, you (or your insurance company) are responsible for its replacement.
3. A police report is required for the loss of any HCSB equipment.
4. If damage that is not covered by warranty occurs to the device when you have removed it from campus, you are responsible for the cost of having it fixed or replaced.
5. Devices should never be left at home. If you take the device home, you must bring it back to your work site with you the next day.
6. All devices must be turned in to the principal or technology coordinator upon request and at designated times.
7. Devices should always be in a secured area when leaving them at your job site overnight.
8. Proper care must be taken with the device:
    - · Do not leave the device in a hot car;
    - · Keep your device away from food and drink; and
    - · Do not place stickers on the device's casing.
9. Devices may only be used by employees. They may not be used by family members (children, spouse, etc.) or friends. They are for work related activities only.
10. A Removal of Property form must be signed and on file with the property manager.
11. This memo must be signed and on file with the principal or designee.

Please sign that you have read and agree to the guidelines as stated above:

_____ _____

Print Full Name Date

_____ _____

Signature Property Control Number (Barcode)

Approved Date: _____ Items: [ ] Device [ ] Carry Case [ ]Power Adapter

Appendix D

Request for Social Channel Account Form:

Social Channel Account Request Form

PLEASE NOTE: One form must be completed for EACH account.

Date: _____

Department/School/Sport/Club:_____

Name of staff or faculty member responsible for account: _____

Contact email: _____

Contact Phone: _____

Social Media Channel (ex. Facebook, Twitter): _____

Link / Username of account: _____

Password: _____

How will this account help meet the district's social media mission?

What audience are you hoping to reach?

I agree that the purpose of this social media page is to promote the district's official academic programs, events and news. I agree that as the official District representative for this site, I will monitor this page daily to ensure all content is related to district business and does not contain material that violates district policies. I agree to positively represent the district and uphold the mission and values.

Name & Signature of registrant:
Date: ____/____/____

Name & Signature of supervisor:
Date: ____/____/____

Appendix E

Software Rostering Request Form

Name of Software Program and Parent Company if Applicable:

_____

Date of Initial Request: _____

Name of Person Requesting Program: _____

Has program been approved by the School Administrator: ____ Yes ____ No

Name of Administrator: _____ Signature:_____

Has program been approved by the appropriate Director of Schools: _____ Yes _____ No

Name of Director:_____ Signature:_____

Has program been approved by the District Technology Committee: _____ Yes _____ No

School Level Support Personnel (**Onsite Contact**): _____

Software Program Support Contact Name: _____

Software Program Support Contact Phone Number: _____

Software Program Support Contact Email Address: _____

Has the Software Vendor provided any documentation relevant to the IT Department, such as Integration Guidelines, Interoperability, SFTP Templates or SSO information? ___Yes ___No

If yes, please attach a copy of those to this request or email those to the Director of IT.

Has this program been purchased or is it free? _____

If purchased, what funding source was utilized? _____

(Continued on back)

How many licenses have been purchased or will be used? _____

Was a technical support plan purchased? If yes, please attach a copy of agreement to this request.

What are the course number(s), grade level(s), content area(s), and teacher name(s) of those that will be using this program?

School	Full Teacher Name	Grade Level	Content Area	Course Number	Section Number

Appendix F

Extension or Application Request Form

Name of Extension or Application being requested: _____

Date of Initial Request: _____

Is this an extension or application: _____

Is this for: ___ Chromebook ____ iPad

URL to extension or application: _____

Person submitting request: _____

School/Department Contact:_____

Has this extension or application been approved by the school site administrator or Department Head? _____ Yes _____ No

Name of Administrator:_____ Signature: _____

Is this extension or application free? ____Yes ____No

If not, which department or school will be/has purchasing/purchased?

_____

If applicable, how many licenses were purchased? _____

If this is part of an IEP or 504 plan, what is/are the student name(s) and identification number(s) associated with the desired account access?

School	Student Name	StudentID

(Continued on back)

What grade level(s) or school(s) will this be applied to?

School	Grade Levels