GULF COUNTY SCHOOLS

IT Policies and Procedures

The information technology resources provided and maintained by the IT department are intended for GCSB related purposes including the support of the GCSB mission and its administrative functions and activities within the user community. The network must be maintained on a daily basis and security of the network is high priority for the district. Areas of responsibility are designated below:

1. **Management of Student Information System – Assistant Superintendent for Business**
2. **Management of Finance and Human Resource System – Chief Finance Officer**
3. **Management of District Firewall, Routers, and security devices – Network Administrator**
4. **Management of District Web Filter – Network Administrator**
5. **Management of Critical Servers - Network Administrator**
6. **Management of Disaster Recovery Servers - Network Administrator**
7. **Administering user identification codes (IDs), administrator IDs, administrator passwords, guess accounts – Network Administrator**

Appropriate use of computing resources includes respecting the privacy of other users and their accounts, using only those resources which are authorized for use, respecting the finite capacity of these resources so as not to limit their accessibility by others, and abstinence from using any of these resources for personal gain or commercial use not related to GCSB business. Unauthorized and/or inappropriate use of these resources is prohibited and may result in disciplinary and/or legal action. Unauthorized or fraudulent use of GCSB

telecommunications resources can result in felony prosecution as provided for in Florida Statutes.

Technology equipment may include but is not limited to workstations, laptops, PDAs, Blackberries, smartphones, servers and network devices such as routers, firewalls and switches. GCSB may require users of computing equipment to limit or refrain from specific uses of that equipment if their activities are destructive or interfere with GCSB technology operations or resources. No unauthorized user may connect to the GCSB network resources. This includes use of employee and student personal computers, devices, and equipment owned by sales representatives, consultants, and/or other visiting professionals without approval from the Network Administrator. Only GCSB technology equipment is authorized for use on the GCSB network.

Administrative computers are defined as non-classroom computers and teacher PCs on which GCSB has installed software for business functions (TERMS, Pinnacle, etc.). These computers must be kept separate from instructional computers. Students are not to have access to any administrative computer. Every effort should be made to keep classroom computers that are used for grade book activities and staff e-mail functions secure. All 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 another lockout mechanism to prevent unauthorized persons from accessing these environments. No student should work on an administrative computer.

Software owned by the GCSB will be installed on computers set up for the end users by a GCSB Technology Specialist or a person designated to install software at a school site. No users are allowed to install software on computers that are connected to the GCSB network.

Desktop enhancement software and peer to peer file sharing applications enabling the exchange of files across the GCSB network will not be permitted. If

the use of such software is found to violate the GCSB policy, the Digital Millennium Copyright Act, the Florida Computer Crimes Act or federal law, the appropriate disciplinary and/or legal actions will be taken. Streaming of live media (audio, video, etc.) not related to instruction is strictly prohibited. If the operation of such software is found to interfere with the normal functioning of the GCSB network, hinder network performance or compromise network security, IT will notify the user and take necessary action. All software copyright laws must be observed for any software installations.

GUIDELINES FOR THE USE OF GCSB TECHNOLOGY RESOURCES

It is a general policy that the network/Internet will be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of the Gulf County School Board. Failure to adhere to policies and guidelines may result in legal and/or disciplinary action.

The following Guidelines have been developed for all users.

1. **Acceptable uses of the network are activities which support learning and teaching. Network users are encouraged to develop uses which meet their needs and which take advantage of the network's functions: email, conferences, access to databases, and access to the Internet.**
2. **Classroom teachers are responsible for teaching proper techniques and standards for participation, for guiding student access to appropriate sections of the network and for assuring that students understand that if they misuse the network they may face disciplinary or legal action. Particular concerns include issues of privacy, copyright infringement,**

email etiquette, cyber bullying and intended use of the network resources.

3. Users should follow rules for webpage development and network use.
4. Users are expected to use "Netiquette". They are expected to abide by the generally accepted rules of network etiquette. Be polite. Do not use vulgar or obscene language. Students should not reveal their private address or phone number or those of others. Adults should exercise caution in revealing name and address information over the network. Electronic mail is not guaranteed to be private.
5. Gulf County School Board makes no warranties of any kind, whether expressed or implied for the provision of computer resources. GCSB will not be responsible for any damages suffered by any user, including loss of data. GCSB shall not be responsible for the accuracy or quality of information obtained through the Gulf County School Board's Internet connections.

SAFETY GUIDELINES FOR ALL USERS

In order for the network to be as safe as possible, every teacher and administrator should remember the following:

1. **It is the responsibility of the faculty member who grants access to GCSB facilities and/or resources to insure that students are aware of the provisions of the GCSB acceptable use policies and guidelines, and of any rules, procedures, or courtesies for the outside network they are accessing.**
2. **It is the responsibility of the faculty member to always supervise students when they are accessing the network.**

3. **Whenever possible place the computers in central locations in the classroom or media center where the screens are highly visible.**
4. **Discuss the network access guidelines.**
5. **Since filtering isn't foolproof, users are still responsible for appropriate use.**
6. **Access must be limited only to educational sites.**
7. **Do not reveal your personal information or that of any other person (name, address, phone number).**
8. **Users shall receive or transmit communications using only GCSB approved and GCSB managed communication systems.**

ACCESS TO TECHNOLOGY RESOURCES

Users will be granted appropriate access to all technology resources necessary when conducting GCSB business for their jobs. Normal operation and maintenance of computing resources requires: backups and caching of data communications, logging of resource activity and monitoring of general usage patterns, as well as other activities necessary in providing service to the user. GCSB may monitor activity and/or accounts of individuals without notice.

USER ACCOUNTS

Appropriate persons will be authorized to access GCSB administrative data files. The Department Head or Principal must email the Network Administrator and the Asst. Superintendent for Business for staff needing access to GCSB administrative systems. Access to GCSB data files and computer programs will be authorized only if such operation is clearly a part of, or directly related to, the administrative workload of the school or administrative unit. It is

solely the responsibility of the individual's supervisor to ensure proper training and use of any computer programs or data files.

When employment with the GCSB terminates access privileges are revoked. If duties are changed so that access to computer equipment or data files is no longer required or a transfer to another school or department is made, the user account must either be disabled or altered to reflect the change in the individual's position, departmental or school affiliation. It is solely the responsibility of the individual's supervisor to inform the Network Administrator when such changes are necessary. Students, volunteers and non-school staff shall not be provided access to GCSB data files.

VENDOR/CONSULTANT ACCESS AND EQUIPMENT

1. **Vendors and consultants may only access the GCSB networks with prior authorization from the Network Administrator or designee.**
2. **Vendor/consultant equipment that uses a password will be changed by the District, once the equipment is fully-operable and working to the satisfaction of the Technology department. The vendor password will be completely removed.**
3. **If a vendor/consultant needs to work on equipment on our network, they will be given a temporary password that will be removed once the vendor or third party has completed their task.**

GULF COUNTY SCHOOLS

LOGGING ON

1. **With all GCSB computers, the end-user will not have administrative rights with their log-on.**
2. **Each end-user has a unique log-on the network.**
3. **Servers and other critical hardware will have a unique log-on for each user.**
4. **Servers and other critical equipment will have a log history and it shall be maintained and reviewed by the Network Administrator or designee on a monthly basis.**

PASSWORDS

The Network Administrator shall supply each duly authorized user with a unique user identification code and initial password that will permit the user to sign on to the GCSB network. Passwords must be changed every 60 days (or as dictated by the individual program) by the user to maintain systems' security. Passwords are required to be a minimum of 8 characters. Passwords need to be complex and contain at least 1 number and 1 capital character. Each authorized user will be responsible for use of the computer equipment. Each user must protect all data files and computer programs by signing off or locking the system before leaving their workstation. Users must change their password(s) at any time if security is compromised. A periodic review of user access rights to ensure that access privileges are appropriate is conducted and documented bi-annually.

GULF COUNTY SCHOOLS

DISCLOSURE OF PASSWORDS

It is a violation for any person to disclose any password to any other person, except to a member of the IT staff for problem resolution purposes. Passwords must be changed upon resolution if the password was given to a technician. Thus, it is the responsibility of each employee to maintain the confidentiality of password(s). Under no circumstances shall passwords be posted or kept in a place that is accessible. Access to these accounts and their passwords to any unauthorized personnel are prohibited. It is the responsibility of the account owner to notify their supervisor and IT whenever unauthorized account access is suspected. The account owner must then change his/her password(s).

NETWORK MANAGEMENT AND SECURITY

In the information age in which we live, management of network resources and the security of the Gulf County School's network are fundamental to the pursuit of the GCSB goals of academic excellence and serving the needs of Gulf County Schools. Network resources, accepted network behavior and their associated policies are defined as follows:

BANDWIDTH

Bandwidth, or the transmission capacity, of our network hardware is a finite resource all electronic information on our network must share. This information can be referred to as network traffic. GCSB reserves the right to develop the rules governing these priorities based on the relative importance of different applications, users, and groups in conjunction with available resources.

GULF COUNTY SCHOOLS

HACKING

Hacking is the interference with or unauthorized access to any computer or computer network. This may or may not reflect malicious intent. Specific examples of "hacking" include but are not limited to:

- **Any attempt to gain root or system administrator privileges on any GCSB network machine or equipment without permission.**
- **Any attempt to gain unauthorized access to files, equipment or accounts.**
- **Any attempt to do anything that result in the interruption of any service to GCSB users.**
- **Any use of chat robots.**
- **Any attempted use of password cracking software.**
- **Circumventing GCSB approved firewalls and Content filters.**
- **Specific software attacks including 'Smurf Attacks' and 'Ping of Death'.**
- **Any attempt to access or change system files without permission.**
- **Any unauthorized attempt to store user files outside their predefined areas.**
- **Installation or attempted use of SUID programs of any type without permission.**
- **Any attempt to do the above mentioned items through the GCSB network, even if the attempt is aimed outside the network.**
- **Use of shared-multimedia application software such as Napster or Scour.**

Hacking may compromise system availability, data integrity or both. GCSB will, to the fullest extent allowed by law, seek legal action against any individual(s), organization(s) and/or company(s) that directly or indirectly utilizes our network (or causes it to be used) for any practice that is considered to be hacking .

GULF COUNTY SCHOOLS

PORT SCANNING AND SNIFFING

Port scanning and sniffing are legitimate, diagnostic activities that the IT department engages in to maintain the availability and performance of the GCSB network at acceptable levels. Both, however, can be misused for malicious purposes to gain access to sensitive information traveling on our network or to find weaknesses in computer systems that will allow access to unauthorized individuals. Port scanning is only permitted by the Network Administrator and/or appropriate law enforcement agencies for detecting security holes on GCSB workstations and servers. If a system connected to our network is found to have a security hole, the security issue will be addressed or the system will be removed from the network without further notice.

SECURITY INCIDENTS

GCSB has implemented several measures to keep our data secure. Should an incident occur the user will notify their Principal or Dept. Head immediately. The Principal or Dept. Head will then notify the Network Administrator and the Asst. Superintendent for Business of the type of security breach. Depending on the nature of the incident the Network Administrator will determine if the incident is localized or District-wide. The Network Administrator will then notify the affected users on how to respond. The Network Administrator will investigate, and if necessary modify security measures as needed.

GULF COUNTY SCHOOLS

DISTRICT IT INCIDENT RESPONSE PROCEDURE

The purpose of this procedure is to assign responsibility and provide procedures related to the handling of computer security incidents. This procedure contains the process steps for identifying, responding, reporting, and resolving computer security incidents. An incident is defined as "the act of violating an explicit or implied security policy". The Superintendent or designee is responsible for providing policy and procedural guidance for establishing, operating, and maintaining the Board's incident response procedure. Identification and Reporting of Information Security Incidents

1. **District school board employees should inform their school site administrator if they are receiving viruses, worms, SPAM, phishing emails, etc. on any school board equipment or school district networks.**
2. **The Site Administrator will then make the Network Administrator and/or the Assistant Superintendent for Business aware of the issue. Questions that must be considered are: What is the normal amount of reported SPAM daily? Is it up significantly today? Is the malware type a High threat worm? A work order is created by the School site Administrator, with the work order having the option "Security Incident" marked.**
3. **Based on the number of complaints and the severity of threats, the District Network Administrator will determine if a District-wide notification needs to be placed.**
4. **Depending on the type of malware the District is being targeted with, the District Network Administrator will coordinate a response to users and sites on how to manage the incident. The District may choose a notification only for low threats. For higher level threats the District may need to do notifications as well as updating District protection measures, AV signatures, firewall rules, web filter, or immediate email blocking of the offending sites.**

5. **The District Network Administrator or Assistant Superintendent for Business will send out the notifications to schools and administrators as necessary to inform District users on how to respond.**

Responding to Information Security Incidents

A. *Preparation*

The goals of initial response are to:

1. **Verify an incident has truly occurred;**
2. **Was there a policy breach;**
3. **Determine what attacks were used to gain access and identify which systems and data were accessed by the intruder; and**
4. **Determine what an intruder did after obtaining access.**

B. *Identification*

1. **Receive Alert and Review Finding: School Site Technology Contacts are notified of a suspected security event. Begin by reviewing the details of the event. What type of alarm is it? Is only one system affected or are multiple systems?**
2. **Start Logbook: The next step is to start a logbook. The logbook is used to document everything: all people interviewed, what happened, which systems were involved, what action was taken, what tools and commands were used, and what the results were. The first entry in the logbook should include an incident notification checklist:**
    a. **who is calling/paging;**
    b. **date/time;**
    c. **phone;**
    d. **nature of incident (virus, theft, unusual activity);**
    e. **when did the incident occur;**
    f. **how was the incident detected;**

g. who discovered the incident;
h. when was the incident detected;
i. what is the immediate and future impact to client;
j. is it a business critical machine;
k. targeted computer(s):
    1) Host name;
    2) OS;
    3) IP address (es);
    4) location;
    5) Attacking computer(s);
    6) IP address (es).

3. Review Results

4. Request Logs

C. *Containment*

Once the issue is reported and identified, then the Network Administrator must isolate the threat (i.e., unplug the network cable, block host from the router, filters, etc., VLAN segmentation on a network switch, or change administrative passwords). It may be that the technician just needs to alert users to take a specific action or just to be aware of a specific threat.

D. ***Eradication***

If a worm is detected and identified, then technicians may apply the proper eradication methods (i.e., if worm x is in fact identified, then there is likely a vendor removal solution).

Remove malicious software by running Panda Anti-virus software, anti-spyware/anti-malware software, or wiping (erase all files) clean the infected device.

E. ***Recovery***

Continue to monitor the situation, keeping in mind the actual identified threat.

F. ***Lessons Learned***

After things calm down and all systems appear to be stable, technicians will try to understand how the District got infected with this piece of malware(virus, worm, etc.) in the first place. Was it a user's lack of awareness (i.e., someone brought in an infected USB drive or laptop and connected it to the LAN)? Did someone open an unsolicited e-mail? Did someone browse to a risky web site? Was the District attacked from the outside? Was the attack or incident an internal event only? How could it have been prevented? The technician will then close-out the "Security Incident" work order.

GULF COUNTY SCHOOLS

NETWORK INFRASTRUCTURE AND COMMUNICATION CLOSETS

The network infrastructure or hardware includes but is not limited to switches, firewalls, network filters, hubs, routers, and other devices. Only those individuals authorized by the Network Administrator will be allowed access to these communications resources. In addition, the Network Administrator must authorize all networking equipment in use and connected to the network prior to being physically attached to that network. IT department staff will manage all network equipment. Any unauthorized equipment of any kind found attached to the network will be disconnected immediately and without notification to the owner. All closets and rooms where network equipment is installed shall be locked and accessible by authorized persons only.

NETWORK ADDRESS ASSIGNMENT AND DHCP

Each device attached to a network must have a unique address associated with it. The assignment and accurate maintenance of these addresses is instrumental to a healthy functioning network. Management of these functions is solely the responsibility of the IT department. DHCP is a readily available method by which address assignment can be automated. No unauthorized use of DHCP will be permitted. Any unauthorized device acting as a DHCP server will be disconnected immediately without prior notification to the owner.

GULF COUNTY SCHOOLS

DOMAIN NAME REGISTRATION

The Network Administrator is the only agent at Gulf County School Board who may register a domain name/host name to any network device before its installation on the GCSB network. All requests for server and workstation domain names/host names and network addresses must go through the Network Administrator. The Network Administrator will review requests making certain requested domain names are appropriate, consistent with the mission of the GCSB and in compliance with standard naming conventions.

WIRELESS NETWORKS

GCSB is solely responsible for the design, operation and management of the wireless network. Wireless equipment includes but is not limited to wireless transceivers or Access Points directly connected to the wired network and wireless antennas which amplify radio frequency signals. Any tampering with any of these devices will result in appropriate disciplinary action. Any unauthorized wireless device found connected to the wired network will be disconnected immediately without notification to the owner. If other wireless devices in use cause interference with the network, the IT department will work with the person, school, or department owning the device to find an alternative solution. Wireless transmissions are not secure. All users should exercise caution in accessing sensitive or personal information when using the wireless network. Wireless encryption must be enabled.

GULF COUNTY SCHOOLS

FIREWALLS

Firewalls are barriers to unsolicited or malicious network activity as well as being a barrier to unauthorized users of a network. GCSB maintains its own firewall as an added protection against malicious use of our network. All workstation firewalls will be managed by the IT department so as not to interfere with overall network.

LAPTOP COMPUTER AND ELECTRONIC DATA MOBILE DEVICE SECURITY

POLICY STATEMENT

Every member of the GCSB community who utilizes a laptop computer or mobile electronic data device (e.g. Blackberry, Flash Drive, Smart Phone, Hand Held PC, etc.) is responsible for the District data stored, processed and/or transmitted via that computer or device, and for following the security requirements set forth in this policy and in the Acceptable Use Policy.

POLICY/PURPOSE

The purpose of this policy is to comply with federal regulations governing privacy and security of information, and to protect Confidential Data in the event of laptop computer or mobile electronic data device theft. The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal guarantee of the privacy of educational records for student and their parents.

GULF COUNTY SCHOOLS

DEFINITIONS

Mobile Electronic Data Device: **Any electric and/or battery operated device that can be easily transported, and that has the capability for storing, processing and/or transmitting data, including but not limited to mini hard drives, back-up hard drives, Zip Drives, Flash Drives, Personal Data Assistants (i.e. PDAs, including but not limited to Blackberries), Smart Phones, Hand Held PCs, or any other mobile device designed or modified to store, process and/or transmit data.**

Confidential Data: **Information protected by statutes, regulations, GCSB policies or contractual language. Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by the Gulf County Superintendent of Schools or his/her designee. By way of illustration only, some examples of Confidential Data include:**

- **Medical records**
- **Student records and other non-public student data**
- **Social Security Numbers**
- **Personnel and/or payroll or records**
- **Individualized Education Plans**
- **Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction.**

PROTECTION OF CONFIDENTIAL DATA

Every user of laptop computers or other electronic data mobile devices must use reasonable care, as outlined in the GCSB Acceptable Use Policy. Protection of Confidential Data against physical theft or loss, electronic invasion, or unintentional exposure is provided through a variety of means, which include

user care and a combination of technical protections such as encryption that work together to secure a computer against unauthorized access. Prior to use of Confidential Data via laptop computer or other electronic data mobile device, users are responsible for contacting the Network Administrator to obtain appropriate protections for such computers or devices, or for verifying that such protections are already in place. The use of unprotected equipment to access or store Confidential Data is prohibited regardless of whether the equipment is owned or controlled by the Gulf County School District. An information security breach is an unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information. An information security breach can be intentional or can occur due to an accident or negligence. The process to ensure confidentiality includes protecting an individual's first name, middle initial and last name, or any middle name and last name, in combination with any one or more of the following data elements:

- **Social Security Number**
- **Student ID Number**
- **Driver's License Number**
- **Passwords or access codes to accounts that would identify the individual**

This information is protected on our network by network management and log in policy.

REPORTING LOSS/THEFT OF EQUIPMENT OR DATA

In the event a GSCB owned or controlled laptop computer or other electronic data mobile device is lost or stolen, the theft or loss should be reported immediately to the employee's supervisor and the IT department. In the event

any device containing confidential data is lost or stolen, the loss or theft should also be reported to the employee's supervisor and the IT department.

DISPOSAL OF PROPERTY USED TO ACCESS OR STORE CONFIDENTIAL DATA

All electronic devices that have been used to store or access any confidential data, whether District owned or personal-owned, must be destroyed if they are to be disposed of or cleaned before assigning to another user.

ELECTRONIC MAIL

DEFINITION OF EMAIL

Email is the electronic transfer of information, typically in the form of electronic messages, memoranda, and attached documents, from a sending party to one or more receiving parties by means of an intermediate telecommunications system.

PURPOSE

The purpose of these procedures is to delineate acceptable uses of email by approved employees. These procedures supplement Gulf County School Board Policy 8.60. The considerable benefits of email communication to convey

information quickly must be balanced by reasonable risk management and limits designed to protect the electronic network.

PROCEDURES

Mail is to be used for school and district business by authorized employees. When approved by supervisors to use the district email system, support employees will also follow these guidelines.

1. **Pursuant to School Board policy and administrative procedures, this email system is the property of the School District of Gulf County and to be used for official business only.**
2. **Prohibited uses of email include but are not limited to:**
    a. **Non-district sponsored solicitations, including, but not limited to such things as advertising the sale of property or other commercial activities;**
    b. **Sending copies of documents in violation of copyright laws or licensing agreements;**
    c. **Sending messages which violate student confidentiality rules or education records guidelines;**
    d. **Sending content that may constitute prohibited forms of harassment or be considered discriminatory, obscene or derogatory, whether intended to be serious or humorous;**
    e. **Sending communications reflecting or containing chain letters.**
    f. **Sending material promoting political positions or actions.**

GULF COUNTY SCHOOLS

EMAIL MONITORING, ARCHIVING AND STORAGE

1. **The district does not intend to routinely monitor the contents of email messages; however, users should expect that electronic mail messages may be accessed by authorized supervisors or system administrators.**
2. **Any requests for access to the contents of email in order to respond to legal process, such as subpoenas and public records law requests, or for purposes involving litigation, investigation or claim must be immediately brought to the attention of the Superintendent.**
3. **Email will be archived and stored pursuant to Florida State Public Record laws. Individual users are responsible for keeping and archiving their own business-related email. Retention of these files is subject to Florida State laws.**
4. **Mailboxes have a finite capacity. Users will be responsible for mailbox cleanup.**

EMAIL SECURITY

1. **All email accounts must be established and terminated by the Network Administrator. Email accounts are password protected. Under no circumstances shall employees share passwords with others or use another employee's password.**
2. **Use of district-designed group distribution lists by instructional and approved support staff is limited to the work site of the employee or to the subject area or grade level of the employee. Instructional or**

support employees needing to send messages to wider audiences must obtain approval of an administrator.

3. Any allegations of staff misconduct received by email must be brought immediately to the attention of the principal/supervisor or a higher-level administrator.

STUDENT TECHNOLOGY PRIVILEGES AND ACCEPTABLE USE

All student users of the Gulf County School Board's technology resources must complete, with applicable signatures, a Gulf County School Board Student Network Access Permission & Internet Safety Contract, and Photo Release Form and follow the guidelines stated in the contract. Access to GCSB technology resources will be denied to students that do not have this form signed and on file. Students that violate these policies will be reported to the Principal of their respective school and their computing privileges will be suspended or revoked, depending on the severity of the violation. All illegal activities will be reported to the Superintendent or his designee and prosecuted to the fullest extent of the law. Computer use by students is a privilege, not a right.

COMPUTER LAB SCHEDULING/RULES

1. Each school/campus will be responsible for planning and scheduling computer lab use and creating computer lab rules.
2. Computer lab rules must be posted and students must be made aware of these rules and the consequences for not following them.
3. Teachers, Paraprofessionals and students will read and follow the rules as stated in the GCSB Information Technology Policies and Procedures document and the GCSB Instructional Materials Manual.

4. **Students must sign a Student Network Access Permission and Internet Safety Contract, and Photo Release Form each school year.**
5. **Students will be expected to go through a Computer Lab "orientation" before they use the lab. This orientation should include but not be limited to:**
   a. **How students log-in to the workstation**
   b. **Proper care of hardware**
   c. **Programs available for use in the lab**
   d. **Computer lab rules**
   e. **On-line safety rules**
   f. **Appropriate use of computer lab supplies (paper, printer ink, etc.)**
   g. **Password requirements and security procedures**
   h. **All security issues should be reported to administrative personnel immediately.**

GCSB TELECOMMUNICATION PLAN AND ELECTRONIC USE POLICY

Telecommunication network facilities, such as FIRN2 (Florida Information Research Network2) and the Internet are to be used for providing expanded learning opportunities for students and educators. The GCSB provided access must be used in a responsible, efficient, ethical and legal manner. Failure to adhere to this policy and guidelines may result in suspension or revocation of the user's network access and other disciplinary action as found in the Gulf County Schools Code of Student Conduct. Internet usage and other online activity by students shall be pursuant to staff authorization only and must be in pursuit of a legitimate educational goal. Recreational use of the Internet and World Wide Web is prohibited. Internet or other online usage by students shall be monitored by school staff. Staff shall take reasonable efforts to ensure that

students are not exposed to inappropriate or harmful matter on the Internet and World Wide Web. To ensure the safety and security of students, the following computer and Internet usage by students is strictly prohibited, unless otherwise authorized by law:

- **Use of electronic mail, chat rooms, and other forms of direct electronic communication, unless specifically authorized by staff in pursuit of a legitimate educational goal;**
- **Unauthorized Internet, online, or other technology access, including so-called "hacking" and other unlawful activities;**
- **Disclosure, use, and dissemination over the Internet of personal information regarding students.**

VIOLATING INTERNET POLICY, RULES AND REGULATIONS OR INAPPROPRIATE USE OF THE GCSB NETWORK

Any student found violating the terms and conditions of the Gulf County School Board policies, school rules, traditional and mobile computer lab rules, and/or regulations on the use of the Internet, or internal network, as set forth in the annual form published by the school district, will lose access privileges and be subject to school disciplinary actions and/or appropriate legal action. (See Gulf County Schools Code of Student Conduct and GCSB Instructional Materials Manual).

GULF COUNTY SCHOOLS

SAFETY GUIDELINES FOR STUDENTS

Student users are expected to protect themselves by following these guidelines:

- **Do not reveal any personal information of yours or that of any other person (name, address, phone number)**
- **Never share your password with anyone.**
- **Student users shall not agree to meet someone.**
- **Student users shall promptly disclose to their teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.**
- **Student users shall receive or transmit communications using only GCSB approved and GCSB managed communication systems.**

LOSS PREVENTION, EMERGENCY PREPAREDNESS

When threatened by a natural disaster, the IT department will take routine measures to protect and restore locally stored data. The Network Administrator or designee is responsible for keeping a backup of the school's server off site. In the event of immediate threat from a hurricane or other natural disaster emergency information will be posted on the Gulf County School Board web site. Each school and district office department should take the following steps to protect data and equipment:

1. **Users shall make regular backups of important documents to removable media and store it in a safe off site location.**
2. **Backups of school servers should be stored off site and in a secure location.**
3. **Computers shall be turned off and unplugged.**
4. **Computers shall be moved away from windows and off the floor.**

GULF COUNTY SCHOOLS

DISASTER RECOVERY

At the Gulf County School Board, four servers have been identified as critical to the functioning of our school district. These servers are listed below in the order they will be brought back up in case of an emergency:

1. **Active Directory and Exchange Server- Controls all email communications within and without the district;**
2. **Food Service Server- student lunch accounts , free and reduced lunch system information;**
3. **Transportation server- controlling bus routes, zoning info, field trips request, etc.; and**
4. **HR and Financial Record Storage Server.**

With the identification of the district's critical servers, the following plan is in place:

1. **All servers will be backed up by a local on-site server. The server will mirror the processes and save all data from each mother server.**
2. **All critical servers will also be backed up at a "Cloud" location. Currently, the HR/Finance Server is backed up with NWRDC and their Cloud locations are in Georgia and Florida. Remaining servers have back up "Cloud" locations in Washington or other locations.**
3. **The plan of recovering both data and processes will be "tested" twice a year to ensure that the district has access to both data and processes in a timely manner.**
4. **In case of a disaster and servers are destroyed are damaged, the order of server restore is:**

a. Active Directory Server
b. Email Server
c. Food Service Server
d. Transportation Server
e. HR and Financial Record Storage Server

COMPUTER DISPOSAL

Property record numbers of computers no longer in use or deemed irreparable will be sent to the Network Administrator and after a determination of usefulness has been made, the Network Administrator will send a letter to the Superintendent asking that they be removed from property records and disposed of. As a security measure, administrative computers and other computers with district/student data will have their hard drives removed and disposed of separately.

SUPPORT

GCSB uses the following procedures and staff for support of computers, software and network problems. Each school should have at least one person designated for technology assistance.

A user who has an issue is to follow these steps for corrective action.

1. **Contact the school technology person and explain in detail the issue at hand.**
2. **The technology person will try to correct the issue.**

3. **If the technology person cannot resolve the issue they will submit a problem report (TroubleTrakker) with details of the problem.**
4. **The problem report will be assigned to the appropriate staff (IT or Curriculum).**
5. **The staff member looks at or resolves the problem and either closes the ticket or keeps it open until it is properly resolved.**