

**Greater Egg Harbor Regional
High School District**

**Computer/Network
User Agreement**

I. Introduction

Computer information systems and networks are an integral part of education and business at the Greater Egg Harbor Regional High School District. The district has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

- Enhance the educational process.
- Protect this investment.
- Safeguard the information contained within these systems.
- Increase the efficiency of the business operations.

II. Violations

Violations may result in disciplinary action in accordance with district policy. Failure to observe these guidelines may result in disciplinary action by the district depending upon the type and severity of the violation, whether it causes any liability or loss to the district, and/or the presence of any repeated violation(s).

III. Administration

The superintendent is responsible for the administration of this policy.

IV. Contents

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Computer viruses
- Access codes and passwords
- Physical security
- Copyrights and license agreements
- Reporting problems
- Classroom computers
- Lab computers
- Network availability

V. Statement of responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

Supervisor responsibilities

Supervisors must:

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

IT manager responsibilities

The IT manager must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

VI. The Internet and e-mail

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

Policy

Access to the Internet is provided to employees for the benefit of the district and its students to improve the educational process. Employees are able to connect to a variety of educational information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive, the following guidelines have been established regarding the usage of the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the district, therefore responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain educational information from commercial Web sites.
- Accessing databases for information as needed.
- Using e-mail for business contacts.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the district, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Conducting a personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

Downloads

Downloading from the Internet has been restricted from every computer in the district. Any download request must be sent through TroubleTrakker. This is to ensure that the computer can handle what is being downloaded and to eliminate any unnecessary problems. The ability to open and read text files from the Internet is still available.

Employee responsibilities

Any employee who uses the Internet or e-mail shall:

- Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.

- Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
- Not transmit copyrighted materials without permission.
- Know and abide by all applicable district policies dealing with security and confidentiality of district records.
- Run a virus scan on any executable file(s) received through the Internet.
- Avoid transmission of nonpublic student information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the district and/or legal action by the copyright owner.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the district and *may be regarded as public information*. The district reserves the right to access the contents of any messages sent over its facilities.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

VII. Computer viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of district resources.

Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

IT responsibilities

IT shall:

- Install and maintain appropriate antivirus software on all computers.
- Respond to all virus attacks, destroy any virus detected, and document each incident.

Employee responsibilities

These directives apply to all employees:

- Employees shall not knowingly introduce a computer virus into company computers.
- Employees shall not load diskettes, CDs, or Flash storage drives of unknown origin.

- Incoming files shall be scanned for viruses before they are read.
- Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IS manager.

VIII. Access codes and passwords

The confidentiality and integrity of data stored on the district computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

Passwords are issued to assist in securing the network and the information that is stored and shared within the school district's computer system. Faculty and staff are responsible for maintaining their passwords. For the majority of staff and faculty there are three different passwords that must be maintained. They are:

- Windows Network Login
- Genesis (Student Information System)
- K12 Email System

Each password should be unique and be changed on a regular basis. Passwords must also be at least **10** characters in length and should not be your name. Passwords should not be left where someone can find them. You may be prompted to change your password at different times. Please keep in mind that K12 will not remind you to change your password, however, it should still be changed periodically.

Passwords are only issued to district employees. Substitute teachers and other individuals who work in the building from time to time are prohibited from accessing the district's computer network. Substitutes who are hired on a long-term basis will be issued computer accounts if that individual is recognized by the Board of Education as an employee and the administration deems it necessary.

Our student information system (Genesis) is web based, so it is particularly important for each staff and faculty member to safeguard their passwords to it to prevent third parties from accessing the system from remote locations.

IT responsibilities

- The administration of access controls to all district computer systems.
- Will process adds, deletions, and changes upon receipt of a written request from the end user's building principal.

Employee responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
- Will change passwords at least once every 40 days.
- Must use passwords that will not be easily guessed by others.
- Must log out when leaving a workstation for an extended period.

Principal's responsibility

Principals should notify the IT manager promptly whenever an employee leaves the district or transfers to another school so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination. Principals are also responsible for informing the IT manager of new employees so the appropriate accounts can be created.

IX. Physical security

It is district policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Employee responsibilities

The directives below apply to all employees:

- Storage media such as flash drives, DVDs, CDs, and diskettes should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
- Storage media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge protector.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
- Since the IT manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
- Employees shall not take shared portable equipment such as laptop computers out of the school without the informed consent of their department supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it, and for what purpose it will be used. If a faculty or staff member has been assigned a laptop as part of the faculty laptop initiative then it is understood that they will follow all of the district computer use guidelines even when not on school grounds.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

X. Copyrights and license agreements

It is district policy to comply with all laws regarding intellectual property.

Legal reference

The district and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the district and the responsible employee(s) to civil and/or criminal penalties.

Scope

This directive applies to all software that is owned by the district, licensed to the district, or developed using district resources by employees or vendors.

IT responsibilities

The IT manager will:

- Maintain records of software licenses owned by the district.
- Periodically (at least annually) scan company computers to verify that only authorized software is installed.

Employee responsibilities

Employees shall not:

- Install software unless authorized by IT. Only software that is licensed to or owned by the company is to be installed on company computers.
- Copy software unless authorized by IT.
- Download software unless authorized by IT.

Civil penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner.
- Profits that are attributable to the copying.
- Fines up to \$100,000 for each illegal copy.

Criminal penalties

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the employee(s) responsible to the following criminal penalties:

Fines up to \$250,000 for each illegal copy.
Jail terms of up to five years.

XI. Reporting problems

Any technical problems regarding a computer or printer must be reported through TroubleTrakker. If you cannot access TroubleTrakker at the computer in your room, you can either see your supervisor, go to another computer or ask a co-worker to report the problem. This process is extremely important in aiding the Technology department in prioritizing and solving district technology problems in a timely and effective manner. Do not submit a second TroubleTrakker ticket for an existing problem. Technical problems will not be handled properly unless received through TroubleTrakker, therefore do not stop a technician in the hallway or call in problems.

XII. Classroom/office computers

Classroom/office computers are district property and are assigned to specific classrooms/offices. They are to be utilized as instructional aides and to assist with administrative tasks such as grading and attendance. Students are permitted to use those computers as long as there is constant faculty supervision. Computers should never be moved from the classroom or office area. Computers are to stay in their assigned classroom even if the teacher's room assignment should be changed.

XIII. Lab computers

Computer labs (both stationary and mobile) are the primary computers for student use. Every student has a unique student ID number and password assigned to them. Faculty and staff accounts will not work in the computer labs because of steps taken to increase the security of the computer network.

IT Responsibility

- Install and maintain appropriate software on all computers.
- Respond to any hardware or software problems with the computers.

Supervisor Responsibility

- Maintain a schedule of the availability of the computer labs.
- Ensure that all appropriate personnel are aware of and comply with this policy.

Employee Responsibility

- It is the teacher's responsibility to assure that no food or drink is brought into the vicinity of any district computer lab.
- Submit a lesson plan (brief description of activity) at least two days in advance, but no more than 2 weeks in advance, for evaluation and approval by supervisor.
- Provide a seating chart for students. For mobile laptops each student should be assigned a specific laptop.
- Sign-up for the room you want to use and include the number of students you believe will be participating.
- Provide a list of any special equipment needed.
- Teachers must provide paper needed for the room.
- All teachers must be in the lab with students at all times.
- If absent, provide alternative plans for substitute other than going to the computer lab.
- For mobile lab use appropriate time should be allotted in each lesson to handout and collect the laptops and examine them for damage and vandalism. The laptops should be signed out by each student and distributed by the teacher in the beginning of class and then signed back in and collected by the teacher at the conclusion of the lesson. At no time should students be in charge of the dissemination and collection of the laptops, it is the sole responsibility of the faculty member who has signed out the mobile laptop. Any faculty member unable to follow these guidelines may have his/her mobile lab privileges revoked.
- Faculty should check all equipment before and after student use and notify the Technology Dept and their supervisor immediately if any damage has occurred. If the damage is the direct result of malicious student behavior the responsible student should be identified and disciplined in accordance with district policy. Some of the items to look for are as follows:
 - Check computer for any indication of graffiti.
 - Check for any visible damage to the computer screen.
 - Check for damage to the keyboard & mouse.

XIV. Network availability

The availability of the network is as follows:

Monday - Friday 6:00 AM - 10:00 PM

Saturday & Sunday 6:00 AM - 10:00 PM

The network is also available on holidays. *The network will be unavailable during scheduled outages for maintenance.

XV. Faculty Laptops

As part of the faculty laptop initiative laptops have been assigned to all teachers for their professional use. By signing the acceptable usage policy each teacher accepts personal responsibility for their assigned laptop. The assigned laptops will be distributed at the beginning of the school year and will be regarded to be returned at its conclusion. The laptop should always be secured regardless of where it has been utilized. If a teacher is unable to properly secure their assigned laptop his/her computer privileges may be revoked by the technology department. At no time should unsupervised students, teacher aides, or substitute teachers make use of a faculty member's assigned laptop for any reason. For all other items the policy for the use of laptops follows the same guidelines as district computers as stated in this policy.

IT responsibilities

- Install and maintain appropriate software on all laptops.
- Respond to any hardware or software issues with the laptops.
- Maintain records of sign outs and damage reports.

Supervisor responsibility

- Submit initial request for faculty member to sign out the laptop.
- Ensure that all appropriate personnel are aware of and comply with this policy.

Employee responsibility

- Follow the proper procedures for signing out a laptop.
- Return the laptop in the same condition it was in when it was signed out.
- Follow district policy pertaining to computers.

XVI. Exclusive use prohibited

Although the computers have been purchased by departments using department budget allocations, this does not give the departments, which submitted the requisition, the right to exclusive use of the equipment. All equipment is district property and must be made available to all instructional areas.

XVII. Inventory management

Management of the computer inventory is very difficult because there are so many components to the systems, which are small and easy to carry. Further, when a drive or monitor goes out, it is relatively simple to move a unit from another system and get the defective system operational. This creates confusion and has resulted in many problems. Everyone using the computer systems must be aware of the difficulty and make every effort to maintain the integrity of the inventory. Computers and computer peripherals (printers, scanners, etc.) must not be moved from their location. All computers and computer equipment are inventoried by their location within the district. Supervisors may request to move computers, but all relocations must be approved by the IS department.

IS Responsibility

- Maintain an accurate inventory of all computers and computer equipment.

Supervisors Responsibility

- Submit requests for any necessary relocations to the IS department.
- Ensure that all appropriate personnel do not move computers or computer equipment.

Employee Responsibility

- Do not move any computers or computer related equipment.

XVIII. Personal Computers and Peripherals

This section addresses the issue of staff bringing personal computers, peripherals and software to school. While the school district does not expressly prohibit the use of personal computers, the school district does not permit the use of personal peripherals and software connected to our network or to our district computers.

Personal Computers

Any computer that is not district property will not be supported by the school district. These computers are not permitted to connect the network, run district owned programs or use district owned peripherals like printers, scanners or LCD projectors. The technology department cannot support these computers in any capacity; the district will not be responsible for any personal computer or equipment that is stolen or damaged.

Personal Peripherals

Faculty and staff are not permitted to bring any computer peripherals to connect to district owned computers. That means no printers, scanners, projectors, cameras or any other device not owned by the district is permitted to be connected and installed on any district computer.

Personal Software

Faculty and staff are not permitted to bring any software to school and load it on district owned computers.

The district cannot support personal computers and peripherals. With the limited technology staff available, time is needed to maintain district property. Also, personal computers and peripherals may not be compatible with the districts network and computers. Faculty and staff are permitted to donate computers and peripherals to the district. Any computers or peripherals accepted by the district will be utilized and tagged as inventory.

Please remove any printers, scanners or other devices you may have brought from home or make arrangements to donate the equipment to the school district.

FACULTY AND STAFF

I have read the Computer/Network User Agreement; I understand and will abide by the Computer Network/User Guidelines. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense and/or result in disciplinary action. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

Name (print): _____

Signature: _____ Date: _____