# Jefferson County School District

# Information Technology Policies and Procedures

575 S. Water Street
Monticello, FL 32344
(850) 342-0100
www.jeffersonschooldistrict.org

June 2014

# Table of Contents

## 1.0 Overview

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

The IT Department is committed to protecting Jefferson 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 Jefferson 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 Jefferson County School District.

Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every Jefferson County School District employee and affiliate is required to meet and exceed the standards set forth by Florida State Law, Federal Law, the Jefferson 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 within the Jefferson County School District. These rules are in place to protect the students, staff, and the Jefferson County School District. Inappropriate use, improper planning, and disregard of these procedures exposes Jefferson 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 students, employees, contractors, consultants, temporary employees, authorized guests, and other workers at Jefferson County School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Jefferson 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 Jefferson 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 creating guidelines concerning personal use of Network/Internet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager (School Board Policy (SBP) 3.102).

Using the Jefferson 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 Jefferson County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Jefferson County School District while on the network.

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

The Jefferson 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, students, and guests of Jefferson County School District, will be granted access to the network after they have signed the appropriate Network Usage Agreements forms and forwarded them to designated administrator (see Appendix A, Appendix C, and Appendix D).

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 computer's 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 contact the IT Department. This authority may be assigned to a site based employee.

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 Technical Support Services.

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

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, 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 mechanism to be determined by the Technology Director. Any attempt to circumvent and/or distribute ways to circumvent this security mechanism is strictly forbidden.

Users of Jefferson 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 Technical Support Services 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), Jefferson 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 PDA and 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 un-encrypted data on a portable device; and

- Protect printed sensitive data. Store sensitive data in locked desk, drawer or cabinet. Do not leave unattended sensitive data on copier, FAX, or printer. Shred sensitive data that needs to be disposed.

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 Jefferson 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 Jefferson County School District network or network device without a signed and approved vendor contract or a Guest Access Agreement Form (Appendix D).

Using the Jefferson 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 Jefferson County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Jefferson County School District while on the network. The Jefferson County School District IT staff can only provide limited support in aspects of network connectivity and access of 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 administrated 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 Jefferson County School District must sign a Portable Device Usage Agreement form upon receipt of the device (see Appendix B).

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 Jefferson 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 Jefferson County School District has no control over the information accessed through the internet and cannot be held responsible for content viewed.

Jefferson 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 Jefferson 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;
- Termination of consulting contract; and
- In the event of an investigation of 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 Jefferson County School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Jefferson 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 Jefferson County School District staff to manage the network is strictly forbidden.

Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, .zip, .msi, and .rar.

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:

- 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 Jefferson 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 Jefferson County School District or the end user does not have an active license is strictly prohibited;

- 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 Jefferson 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 Jefferson County School District account;

- 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, via any means, locally or via the network/Internet; and

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

### 5.2 Unacceptable Use: Email and Communications Activities

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).

Students shall not use social network sites including, but not limited to, myspace.com, facebook.com, chat rooms, etc.

Students shall not agree to meet with anyone met online.

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 Jefferson County School District's networks of other internet/network service providers on behalf of, or to advertise, any service hosted by Jefferson County School District or connected via Jefferson County School's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

## 6.0 IT Technician Responsibilities

It is the responsibility of the IT Technicians to follow the guidelines and policies of the Director of Technical Support Services, Jefferson County School District, Florida Department of Education, and all State and Federal Laws.

IT Technicians report to the Director of Technical Support Services. Training and meetings, as determined by the Directory of Technology, are to be held between the IT Technicians and the

Director of Technical Support Services in order to maintain close working relationships and openness in day-to-day communications.

Among their other responsibilities, the IT Technicians should use reasonable efforts to:

- Respond to requests for support, information, problem determination and problem resolution.
- Become familiar with all applicable Jefferson County School District IT policies.
- Participate in required IT Technicians training and regular meetings as determined by the Director of Technical Support Services.
- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.
- Treat information about, and information stored by, the network users in an appropriate manner; and
- Take precautions protecting the security the network and the security and confidentiality of the information contained therein.

Promptly inform the Director of Technical Support Services of any computing incidents which clearly compromise network integrity, including but not limited to:

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

Promptly notify the Director of Technical Support Services of material changes in network architecture or administration.

IT Technicians, when requested, are expected to cooperate fully with the Director of Technical Support Services 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.

IT Technicians are responsible, however, for notifying the Director of Technical Support Services of any observed violations of Jefferson County School District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

## 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 an IT Technician becomes aware of a security incident, they must provide notification of the incident to the Director of Technical Support Services. Upon confirmation, the Director of Technical Support Services will notify the user's supervisor (if a Jefferson County School District employee) or School Administrator (if a Jefferson 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 Directory of Technology

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

## 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 of Technical Support Services, 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 Jefferson County School District's network, protect the rights or property of Jefferson County School District or third parties, or to ensure compliance with Jefferson 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; or
- 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 Director of Technical Support Services 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 Jefferson 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 Jefferson County School District web site;
- 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 re-established at one of the schools or department buildings.

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 Jefferson 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.

## 10.0 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 Jefferson County School Board Policy.

Please see the Property Disposal Policy for more information about proper disposal of Jefferson County School owned equipment (SBP 6.122).

## 11.0 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 and/or other disciplinary or legal action.

## 12.0 Revisions

The Jefferson 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

# Jefferson County School Board
## *Network/Internet 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 Technical Support Services. 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 Jefferson 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, child pornography 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 Jefferson County School District, understand that any misuse of equipment that results in the lost, damage, or vandalism is to be paid for through the staff member's homeowner insurance.

**Please complete the following information:**

Staff Member's Full Name (please print): _____

School/Department: _____

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. 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 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

# Check out guidelines

**Laptop/tablet/iPad/etc (Devices)**
**JCSB issued devices may be issued to individuals for job related activities.**

Guidelines for using a JCSB device:

1. If taking the device home, you MUST have homeowner's or renter's insurance to cover the device.
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 JCSB 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.
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:

_____ _____
Signature Date

_____ _____
Name Property Control Number

_____ _____
Approved Date

Items: [ ] Device [ ] Carry Case [ ]Power Adapter Other_____

# Appendix C

## Student Network/Internet Acceptable Use Policy

The Jefferson County School Board's Network(s) provide access to network(s)/Internet services for educational purposes. The Internet is an information highway connecting thousands of computers all over the world. I understand that I will have access to the Internet and with this access comes the availability of some material that may not be considered to be of educational value within the context of the school setting.

Efforts will be made to direct students to educationally related material. However, on a telecommunications network(s) it is impossible to control all materials and sites. I believe that the valuable information and interaction available on the network(s)/Internet services far outweigh the possibility of users gaining access to sites that are not acceptable.

I understand that if I violate these guidelines established by the Jefferson County School Board, I will have my access to the network(s) services denied and terminated. My signature indicates that I have read the Acceptable Use Policy of the Jefferson County School Board and that I understand the significance of the terms and conditions of the Policy.

Student Name: _____ Student Signature: _____
(Please print)

School: _____ Date: _____

## Parent or Guardian Network/Internet Contract Acceptable Use Policy (Required if student is less than 18 years of age.)

As the parent or guardian of _____, I have read the Terms and Conditions of the Jefferson County School Board's Acceptable Use Policy. I understand that this access is designed for educational purposes. I understand that some materials on telecommunications network may be objectionable, but I accept responsibility for guidance of network use – setting and conveying standards for my daughter or son to follow when selecting, sharing, or exploring information and media.

I understand that this permission will be in effect for the duration of my student's education experience at this school. As the parents or legal guardian of the minor student signing above, I grant permission for my son or daughter to access networked telecommunication services.

Parent or Guardian: (Please print) _____

Signature: _____ Date: _____

Home Phone: _____ Work Phone: _____

## Appendix D

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

The Jefferson County School District (JCSD) 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 JCSD on the JCSD network.

Using the JCSD 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 JCSD staff to manage the network is strictly forbidden and will result in the termination of network services.

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

The JCSD 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: _____

Signature: _____

Date: _____

Time Period Requested:

Start Date: _____ End Date: _____