OKEECHOBEE COUNTY SCHOOL BOARD INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

Revised 07/2008

Contents

OKEECHOBEE COUNTY SCHOOL BOARD INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

Okeechobee County School Board (OCSB) Information Technology Policies and Procedures exist in addition to all other legally binding documents to guide the conduct of the Okeechobee County School Board users as it pertains to technology resources. It is not intended to replace in part, or in whole, pertinent Florida or federal laws. Such laws include the Computer Crimes Act, Chapter 815 of the Florida Statues; the Public Records Law; Chapter 119 of the Florida Statutes; the Digital Millennium Copyright Act; the Computer Fraud and Abuse Act of 1986; the Computer Abuse Amendments Act of 1994; or obscenity and child pornography laws.

All users agree to comply with the OCSB Information Technology Policies and Procedures with applicable state and federal laws dealing with appropriate, responsible and ethical use of information technology. It is not the responsibility of MIS to ensure user compliance with this technology policy. It is the responsibility of the user to be aware of the existing policies and to adhere to their guidelines. Non-compliance is a serious breach of the Okeechobee County School Board's standards and may result in legal and/or disciplinary action for all users, employees and students.

These policies are applicable to all OCSB technology resources and are global in scope. It may become necessary for individual departments and/or schools to define in more detail the limitations on their internal computing resources by further refining the policies stated here. No department and/or school may override the guidelines and restrictions contained within this technology policy.

Access To Policy

OCSB Information Technology Policies and Procedures shall be made available on the OCSB website. http://www.okee.k12.fl.us/ Printed copies of these policies and procedures will be distributed to each employee. All newly hired employees will receive a copy as part of the hiring orientation. Additional printed copies shall also be available through the Human Resources & Staff Development Department.

All employees must sign the Okeechobee County Receipt of the OCSB Information Technology Policies and Procedures Manual and Non-Student Network Access Permission & Internet Safety Contract. A copy of the signed agreement will be placed in the employee's personnel file

Ownership and Use of Information Technology Resources

The information technology resources provided and maintained by MIS are intended for OCSB related purposes including the support of the OCSB mission, its administrative functions and activities within the user community. Appropriate use of computing resources includes respecting the privacy of other users

and their accounts, using only those resources you are authorized to 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 OCSB 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 OCSB telecommunications resources can result in felony prosecution as provided for in Florida Statutes. Resource areas are defined as follows:

Technology Equipment

Technology equipment may include but is not limited to workstations, laptops, PDAs, Blackberries, servers and network devices such as routers, patch panels and switches. OCSB may require users of computing equipment to limit or refrain from specific uses of that equipment if their activities are destructive or interfere with OCSB technology operations or resources. No unauthorized user may connect to the OCSB network resources. This includes use of employees' personal computers, equipment owned by sales representatives, consultants, and/or other visiting professionals. Only OCSB technology equipment is authorized for use on the OCSB network. An OCSB computer may be loaned upon request with 48 hours notice to sales representatives, consultants, trainers or others as needed for network access.

Administrative computers are defined as non-classroom computers on which the OCSB has installed software for business functions either BIS or SIS. (TERMS, Skyward) 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

Software owned by the OCSB will be installed on computers set up for the end users by an OCSB 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 OCSB network.

Desktop enhancement software and peer to peer file sharing applications enabling the exchange of files across the OCSB network will not be permitted. If the use of such software is found to violate the OCSB 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 OCSB network, hinder network performance or compromise network security, MIS will notify the user and take necessary action.

All software copyright laws must be observed for any software installations.

Guidelines for the Use of OCSB 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 Okeechobee 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. Okeechobee County School Board makes no warranties of any kind, whether expressed or implied for the provision of computer resources. The OCSB will not be responsible for any damages suffered by any user, including loss of data. The OCSB shall not be responsible for the accuracy or quality of information obtained through the Okeechobee County School Board's Internet connection.

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 OCSB facilities and/or resources to insure that students are aware of the provisions of the OCSB 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 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 OCSB approved and OCSB managed communication systems.

Access to Technology Resources

Users will be granted appropriate access to all technology resources necessary in conducting OCSB 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. OCSB may monitor activity and/or accounts of individuals without notice.

User Accounts

Appropriate persons will be authorized to operate computer equipment.

The Department Head or Principal must email the director of MIS for staff needing access to OCSB administrative systems. Access to OCSB 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 OCSB terminates, or 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 MIS when such changes are necessary.

Students, volunteers and non-school staff should not be provided access to OCSB data files.

Passwords

The appropriate MIS Manager 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 OCSB network.

Passwords must be changed every 90 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 special 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.

Disclosure of Passwords

It is a violation for any person to disclose any password to any other person, except to a member of the MIS 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 MIS whenever unauthorized account access is suspected. The account owner must then change their password(s).

Network Management and Security

In the information age in which we live, management of network resources and the security of the Okeechobee County School's network are fundamental to the pursuit of the OCSB goals of academic

excellence and serving the needs of Okeechobee 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. OCSB 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.

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 OCSB 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 OCSB users.
- Any use of chat robots.
- Any attempted use of password cracking software.
- Circumventing OCSB approved firewalls.
- 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 OCSB 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. OCSB 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 .

Port Scanning and Sniffing

Port scanning and sniffing are legitimate, diagnostic activities that MIS engages in to maintain the availability and performance of the OCSB 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 MIS and/or appropriate law enforcement agencies for detecting security holes on OCSB 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.

Network Infrastructure and Communications Closets

The network infrastructure or hardware includes but is not limited to switches, hubs, routers, patch panels and network cable. Only those individuals authorized through the MIS Department or MIS personnel will be allowed access to these communications resources.

In addition, MIS must authorize all networking equipment in use and connected to the network prior to being physically attached to that network. MIS 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.

Network Address Assignment and Dynamic Host Configuration Protocol (DHCP)

Each device attached to a network must have a unique address associated with it. The assignment and accurate maintenance of these addresses is key to a healthy, functioning network. Management of these functions is solely the responsibility of MIS. 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.

Domain Name Registration

MIS staff is the only agent at the Okeechobee County School Board who may register a domain name/host name to any network device before its installation on the OCSB network. All requests for server and workstation domain names/host names and network addresses must go through MIS systems and networking staff. MIS will review requests making certain requested domain names are

appropriate, consistent with the mission of the OCSB and in compliance with standard naming conventions.

Wireless Networks

OCSB 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, MIS 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.

Anonymous File Transfer Protocol (FTP) Sites

All users intending to implement anonymous FTP on any workstation or server must notify MIS of this intention. Users must not offer licensed or illegal software on their site. Users must not allow anonymous users connecting to their site write access. Any FTP site on the OCSB network found in non-compliance with these restrictions will be disconnected immediately

Firewalls

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

LAPTOP COMPUTER AND ELECTRONIC DATA MOBILE DEVICE SECURITY

Policy Statement

Every member of the OCSB 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.

Reason for 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.

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, OCSB policies or contractual language. Managers may also designate data as Confidential. Any disclosure of Confidential Data must be authorized by the Okeechobee County Superintendant 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.

Policy/Procedures

Protection of Confidential Data

Every user of laptop computers or other electronic data mobile devices must use reasonable care, as outlined in the OCSB 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 MIS 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 Okeechobee County School District.

Reporting Loss/Theft of Equipment or Data

In the event an OSCB owned or controlled laptop computer or other electronic data mobile device is lost or stolen, the theft or loss should be reported immediately to your Site Administrator and the MIS department. In the event any device containing confidential data is lost or stolen, the loss or theft should also be reported to your Site Administrator and the MIS 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 or cleaned before assigned 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 Okeechobee County School Board Policy 8.80. 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 Okeechobee 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.
    g. 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.
    h. 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.
    i. Individual users are responsible for keeping and archiving their own business-related email. Retention of these files is subject to Florida State laws.

3. All email accounts must be established and terminated by MIS. Email accounts are password protected. Under no circumstances shall employees share passwords with others or use another employee's password.

4. 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.

5. 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 Okeechobee County School Board's technology resources must complete, with applicable signatures, an Okeechobee County School Board Student Network Access Permission & Internet Safety Contract, and Photo Release Form and follow the guidelines stated in the contract. Access to OCSB 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. Students will read and follow the rules as stated in the OCSB Information Technology Policies and Procedures document.
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

6. All security issues should be reported to administrative personnel immediately.

OCSB Telecommunication Plan and Electronic Communication 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 OCSB-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 Okeechobee County 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 Network

Any student found violating the terms and conditions of the Okeechobee County School Board policies, school rules, 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 Okeechobee Code of Student Conduct.

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 or meet with someone they have met online without parental approval.
- 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 OCSB approved and OCSB managed communication systems.

Web Publishing Policy

The Okeechobee County School Board provides Web hosting services to all OCSB schools and departments in the district. The use of web pages and web sites must be in support of educational and professional activities that are consistent with the educational goals and policies of the Okeechobee County School Board. This policy applies to all associated web content hosted by the OCSB including but not limited to, all web pages supported on the OCSB servers, whether created by school, departments, staff, or students. Web pages are public documents inviting the outside world to the individual schools, departments and the school district, while at the same time linking students and staff to outside sources of information. All web pages hosted on the OCSB servers are the property of the Okeechobee County School Board.

Statement of Purpose:

The purpose of these procedures is to outline the responsibilities of OCSB webmasters. It also provides guidelines for the publishing of web pages. The OCSB web site is managed by the MIS department, but schools and district offices may also post and maintain individual web sites.

1. Department Level
    a. The department web site is the responsibility of the director or coordinator who may designate a department webmaster. For design, development and publishing, the webmaster must coordinate with the district webmaster.
    b. All Okeechobee County School web pages will reside on the OCSB network server(s), not through an outside vendor.
    c. MIS will assist with uploading of any web pages.

2. School and Teacher Level
    a. The school web site is the responsibility of the principal who may designate a school webmaster. The school administration is responsible for managing the school web site and monitoring class, teacher, student, and extracurricular web pages.
    b. All school web sites must be hosted on an OCSB web server, not through an outside vendor.
    c. Personal (for profit, not-for-profit, non-educational, not related to school or classroom) web pages are not allowed to be housed on district or school equipment.
    d. All school web pages must adhere to the Okeechobee County School Board Information Technology Policies and Procedures before publishing.
    e. Teachers must obtain written approval from the principal before publishing a web page. Approval should be documented using Okeechobee County School Board Web Page

Development Approval. The original should be kept at the school level and a copy should be sent to the MIS Department.

3. Student Published Web Pages
    a. Students may publish web pages on the school/district web site as part of a class or school sponsored activity with parental consent and principal approval prior to publishing.
    b. If students develop web pages for the school they must sign a form stating that all content belongs to the school and they must have parental consent. (See the OCSB Student Web Page Permission Contract.)
    c. Material presented on a student web site must follow the Okeechobee County School Board's Web Publishing Guidelines.
    d. It is the teacher's or advisor's responsibility to make sure that students follow the design, development and best practice guidelines defined in this policy for creating and maintaining web pages.

Design and Development Guidelines

1. Department/School Level
    a. An OCSB District Webmaster will provide a template for use in the development of all department/school web pages.
    b. Every Department must provide useful information including, services of their department/school, contact staff, and/or a department/school mission statement.
    c. Web sites must include email address of the person responsible for the site's correspondence.

2. School Level
    a. Any student web page must contain the Okeechobee County School Board's logo. The OCSB logo must be a proper and unaltered version of it.
    b. Students' web sites must include an e-mail address to the teacher or advisor that is responsible for that site's correspondence.

Content Guidelines for Department, School, and Teacher Web Pages

1. All Department or School home pages must contain a link to the OCSB web site (www.okee.k12.fl.us) This link to the official Okeechobee County School Board home page

should be located on the opening page of the school or department web site. The OCSB web site will contain a list, with appropriate links, to all school web sites.

2. All web pages must reflect only educational, technological and community information that affects the school or department. Information not related to the educational process, such as commercial endorsements or community information not related to school or department activities cannot be posted.
3. Web pages may not contain links to text, images, movies or sounds that contain pornography, obscenity, or language that offends or tends to degrade others.
4. Web pages may not contain links to on-line chat areas.
5. Web sites may have a section that lists business partners who are associated with that school or department. This will be the limit of "advertising" for a business partner on any OCSB sponsored web site.
6. Each web site must have an email address on the first page to the teacher or advisor responsible for maintaining all pages.
7. No OCSB web site may contain a link to the personal web pages of any OCSB employee or student.
8. Commercial use of the OCSB web site, district computers, or district servers for the pursuit of personal or financial gain is prohibited.
9. All publications must comply with all state, federal, and international laws concerning copyright, intellectual property rights, and legal uses of network computers.
10. Publications must include a statement of copyright when appropriate and indicate that permission has been received when including copyrighted materials.
11. All publications must comply with the Okeechobee County School Board's Web Publishing Guidelines, and the OCSB Information Technology Policies and Procedures.
12. All OCSB web pages should meet the goals of high quality in both style and presentation.
13. Correct grammar and spelling are expected.
14. Links from a school or district department should include a disclaimer for links that leave the OCSB site. The disclaimer link needs to be on the homepage and on all other pages of the web site containing links to other non-OCSB sites.

    Disclaimer: The appearance of external links (or hyperlinks) on this page does not constitute endorsement by the Okeechobee County School Board (OCSD) of linked web sites or the information, products or services contained therein. OCSB is not responsible for the privacy practices, activities, or content of aforementioned sites. For other than authorized activities, OCSB does not exercise any editorial control over the information you may find at linked locations. Such links are provided consistent with the stated purpose of this web site.
15. The creator of the web site is responsible for checking with the data operator to ensure that student information, including photos, have not been excluded from release by the parent or by other security codes such as: Court Order, Parents work for Law Enforcement, etc.
16. Web sites must not be used as a forum for political, religious, or personal philosophy.
17. Site layouts or any map-like image that depicts the layout of the school in detail is prohibited.

18. All pages containing an e-mail link must have the following statement located on the bottom of the page.

    "Under Florida law, *e-mail addresses* are public records. If you do not want your e-mail address released in response to a public records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing."

Best Practices Guidelines for Web Page Development

1. Use a consistent design with clear navigation throughout the web site.
2. Keep the length of a page manageable.
3. Do not type text in all capital letters and keep text and link colors in sharp contrast to the background color or pattern.
4. Keep graphics, sound and animation to a minimum.
5. Give web pages a brief but specific descriptive title within the title section of the page.
6. Avoid dead links and posting pages still under construction.
7. Avoid using large images. Control image size using image-editing software.
8. Prior to publishing, preview your site with multiples browsers.
9. Include the date of the last update on the homepage.
10. Design your page to fit 800X600 pixels. Viewers may miss important information if they have to scroll left or right. View your webpage using different screen resolutions before publishing.
11. Spell check and proofread all of your pages.
12. Keep backgrounds simple and small in size.
13. Select backgrounds that make text easy to read.
14. Images should be kept in the images folder.
15. Test the download time of each page to insure prompt loading of the page.
16. Department and school web sites should be reviewed and maintained on a weekly basis. Teacher and student web sites should be reviewed and maintained on a monthly basis.
17. Unless otherwise requested in writing from the responsible teacher or advisor all student web pages will be deleted at the conclusion of the normal school year.

Web Site Limitations and Restrictions

Should at any time a web page becomes detrimental in its activity towards the general stability or health of the OCSB network or internet access, OCSB reserves the right to remove the page from publication.

Video and Audio Podcasts

1. No Podcast shall be published without authorization of the Principal/Director or designee of a school or department.
2. All Podcasts must reflect only educational, technological, or community information that affects the School or Department. Information not related to the educational process, such as

commercial endorsements or community information not related to School or Department activities cannot be posted.

3. Designers of Podcasts must be identified as the designer somewhere in the introduction. The identification should list their name (first only for students) and school or department. All student works will be published through the classroom teacher but approved by the Principal or designee.
4. All Podcast must state the District's Disclaimer Policy. The text of the disclaimer is:

> **The MIS Department of The School District of Okeechobee County maintains Internet access and related services for the users on its wide area network. Please note the following:**
>
> **The School District of Okeechobee County makes every reasonable effort to assure the accuracy of information provided on websites under its direct control. However, the School District makes no warranty or guarantee that the information found on or via District Web Sites is accurate, authoritative or factual.**

This will be verbally stated on audio Podcasts and will be provided on a typed slide on a video Podcast.

> **References to commercial products or trademarks, either directly (by name) or indirectly, on Podcasts are for informational purposes only and do not constitute an endorsement of any company and/or product by the School District of Okeechobee County, nor does the School District assume any liability for information at other sites outside of its direct control**

5. Podcasts must not be used as a forum for political or personal philosophy. They can, however provide information provided there is no violation of the Telecommunications Board Policy.
6. Schools and Departments hosting a podcast are responsible for keeping all data in the pod cast current. Old, out-of-date information should be "trimmed" regularly and Podcasts that are no longer relevant should be removed from the host site.
7. Unless otherwise requested in writing from the responsible teacher or advisor all student pod casts will be deleted at the conclusion of the normal school year.
8. Concern must be paid to the intellectual property rights of others. Information and graphics shall not be placed in a Podcast without prior approval of the author. If permission is then granted, appropriate acknowledgement shall be made.
9. Signed permission is required for any pictures of students shown in the video Podcast, even pictures that do not have identifiable people in them. If student names are to accompany the picture, only first names may be used. All reasonable efforts must be made to insure the anonymity of any student's pictures that will appear in a video Podcast. Signed permission is accomplished using the Okeechobee County School Board Student Network Access Permission, Internet Safety Contract and Photo Release Form.

Loss Prevention, Emergency Preparedness and Disaster Recovery

When threatened by a natural disaster, MIS will take routine measures to protect and restore locally stored data. The administrator or their 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 Okeechobee County School Board web site.

Each school and district office department should take the following steps to protect data and equipment:

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

Okeechobee County School Board Receipt Information Technology Policies and Procedures Manual & Non-Student Network Access Permission and Internet Safety Contract

Acknowledgement of MIS Policies and Procedures Manual

I hereby acknowledge receipt of the Okeechobee County School Board Information Technology Policies and Procedures Manual. I understand it is my responsibility to review the handbook, disciplinary procedures and standards in detail and request any clarification needed from my supervisor, Human Resource/Staff Development Department or MIS Director.

I agree to comply with the Okeechobee County School Board Information Technology Policies and Procedures. I understand that violation of any policies, procedures and standards shall be grounds for disciplinary proceedings.

I understand the policies, procedures and standards established herein are to be applied in both a progressive and cumulative manner.

I also understand this signed acknowledgment of receipt will become a permanent part of my personnel file.

I acknowledge receipt of the Okeechobee County School Board Information Technology Policies and Procedure Manual. I further acknowledge that I can download and save or print a copy of the Okeechobee County School Board Information Technology Policies and Procedure Manual from the Okeechobee County School Board website.

Network Access and Internet Safety Contract

I have read, understand and will abide by the policies state in the Okeechobee County School Board Information Technology Policies and Procedures Manual. I understand that access to computer resources is a privilege designed solely for the support of education and research consistent with the educational goals of Okeechobee County Schools. I understand that any violation of the established Okeechobee County School Board County Technology Policies and Procedures or unauthorized use which includes, but is not limited to: accessing the Internet for personal use; downloading materials that are trademarked, copyrighted or trade secrets without the permission of the owner of such materials; sending or posting threatening messages; and accessing, downloading, viewing and/or printing sexually explicit materials, may result in losing access to computer resources or other appropriate discipline up to and including termination of employment and/or legal action taken against me. I further understand that school and district administrators decide what unacceptable use is and that their decision is final.

Print Name Employee ID _____

Position Title School/Department_____

Employee's Signature Date_____

THE OKEECHOBEE COUNTY SCHOOL BOARD TEACHER WEB PAGE DEVELOPMENT APPROVAL

I hereby acknowledge receipt of the School Board of Okeechobee County Web Publishing Policy. I understand it is my responsibility to review the procedures and guidelines in detail and request any clarification needed from my supervisor or MIS staff.

I agree to comply with the School Board of Okeechobee County Web Publishing Policy.

_____

Teacher's Name

_____

Position

_____

School Name

THE OKEECHOBEE COUNTY SCHOOL BOARD STUDENT WEB PAGE PERMISSION CONTRACT

PLEASE PRINT ALL INORMATION

Student's Full Name:_____

Teacher:_____

School:_____ Grade:_____

Student Number:_____

STUDENT AGREEMENT:

I have read, understand and will abide by the Terms and Conditions for the Okeechobee County School Board and Guidelines for Web Publishing. I further understand that creating a web page is a privilege designed solely for educational purposes and any violation of the Policy and Guidelines may result in the loss of privileges, school disciplinary actions and/or appropriate legal action initiated against me. In addition, I understand that anything I may create for my school's web site is the property of the Okeechobee County School Board.

Student Signature:_____ Date:_____

PARENT OR GUARDIAN (Also required if applicant is under the age of 18)

As the parent or guardian of this student, I have read and understand the Okeechobee County School Board Procedures and Guidelines for Web Publishing. I understand that creating a web page is designed solely for educational purposes, and the Okeechobee County School Board has taken reasonable precautions to supervise students during this process. However, I also recognize that it is impossible for the District to restrict unsupervised access to all information and materials, and I will not hold it responsible for material acquired on the network during the creation of web pages. I also accept full responsibility for the supervision of my child or ward in connection with such access outside of the school setting and at home. I hereby give permission for my child to participate in the creation of web pages in school and certify that the information contained on this application is true and correct to the best of my knowledge and belief.

Parent/Guardian Signature: _____ Date:_____

Parent/Guardian Name (Please Print):_____

Parent/Guardian Work Phone: _____

THE OKEECHOBEE COUNTY SCHOOL BOARD STUDENT NETWORK ACCESS PERMISSION, INTERNET SAFETY CONTRACT, AND PHOTO RELEASE FORM

PLEASE PRINT ALL INFORMATION

Student's Full Name: _____

Teacher: _____ School:_____ Grade:_____

STUDENT AGREEMENT:

I have read, understand and will abide by the Terms and Conditions of the Okeechobee County School Board Information Technology Policies and Procedures. I further understand that Internet access is a privilege designed solely for educational purposes and any violation of the Terms and Conditions of the Okeechobee County School District policies may result in losing my access privileges, school disciplinary actions and/or appropriate legal action initiated against me.

Student Signature: _____Date: _____

PARENT OR GUARDIAN (Also required if applicant is under the age of 18)

As the parent or guardian of this student, I have read and understand the Terms and Conditions of the Okeechobee County School Board Information Technology Policies and Procedures. I understand that this access is designed solely for educational purposes, and the School Board of Okeechobee County has taken reasonable precautions to supervise network usage. However, I also recognize that it is impossible for the District to restrict unsupervised access to all information and materials, and I will not hold it responsible for materials acquired on the network. I also accept full responsibility for supervision of my child or ward in connection with such network access outside of the school setting and at home.

Florida Statute, 1002.22 (2) (C), provides that an educational institution may, without authorization from parents, guardians, or eligible students, release "Directory Information". Directory information includes the following: Student's name, address, telephone listing if not an unlisted number, date and place of birth, a major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, most recent educational institution attended by student, photographs in the school year book and similar information.

In addition, Okeechobee County Schools includes photos and videos of students, teachers, and school activities on its websites. Though the names of faculty, staff, and administration will regularly be used, it is our policy that the full names of students will not. Occasionally, it might be necessary to use the first name of a student, but no last names, addresses, and/or telephone numbers will ever be used.

☐ Please check here if you ***DO NOT*** want your child's information and/or image published in any format, including group or individual photos.

By signing this form, I acknowledge receipt of the Okeechobee County School Board Information Technology Policies and Procedures

Parent/Guardian Signature:_____ Date:_____

Parent/Guardian Name (Please Print):_ _____

Parent/Guardian Work Phone: _____