

## **GUIDELINES FOR ACCEPTABLE USE OF DISTRICT INFORMATION SYSTEMS**

**Part one** of this document is intended for all employees. **Part two** of this document is intended for employees who use technology resources with students, and is **in addition** to the information contained in part one. **Part three** is intended for employees who post documents to the District Web server.

This document is supplemented by any language contained and/or referenced in the District elementary and secondary Student Rights and Responsibilities Handbooks and the Rules and Procedures of the District School Board of Escambia County Florida that pertains to the use of technology and that language is hereby included by reference.

### **Part one – Staff Access**

#### **1. Equipment**

Access is provided to students and staff.

Access to certain information and files may be restricted for security reasons.

Users may not connect or install any computing device and/or peripheral (through a wireless or hardwired District network connection or a standalone installation) without prior approval from the appropriate District administrator or school principal and the Information Technology Department.

The District's currently supported and sanctioned desktop operating system(s), network operating system client(s), and virus protection software must be installed on every District owned computing device and/or peripheral connected to the District network(s). This requirement includes computing devices and/or peripherals that are issued to individual students and employees by the District and that are routinely connected and disconnected from the network as a result of being transported between the workplace/school and home. The required setup procedures and installed components for individually owned computing devices and/or peripherals that are sanctioned by the District for usage on District premises during instructional/business hours or during District events are determined by the germane supervising principal or office administrator in conjunction with the Information Technology Department (see Addendum III containing the procedures for obtaining District sanctioned usage of personally owned and individually issued computing devices and/or peripherals).

#### **2. No Expectation of Privacy**

Any and all of a user's online communications (e-mail, synchronous, asynchronous, etc.) received or transmitted are not private despite any such designation by either the sender or the recipient.

Users waive any right to privacy with respect to their files and communications. Users must consent to access and disclosure of their files and communications by authorized District personnel.

#### **3. The Internet**

Internet access is restricted to certain Web sites and certain types of Internet activities. Prohibited Web sites and activities policies are enforced through use of the District's Internet content filter and firewall. When an administrative, operational, or instructional objective cannot be met using current filter and firewall settings, a request can be made to the Information Technology Department, by the appropriate District administrator or principal, for an appropriate adjustment to the filter and/or firewall.

Principals and District office administrators exercise editorial control of all content and functions posted on their school or office Web pages. If a principal or office administrator concludes that content and/or functions not in compliance with District posting restrictions are required for their school or office to provide a legitimate instructional or administrative function, the principal or administrator must present a request to exceed District posting restrictions to the Information Technology Department. See the sanctioning and editorial processes provided in Part Three – District Web Site Guidelines, Section 1 - Content and Section 2 - Security and Editorial Control of Content on School Web Sites within the Guidelines for Acceptable Use of District Information Systems.

#### **4. Electronic Mail System (GroupWise) and the Network Operating System (Novell)**

E-mail and Network Operating System accounts are created and managed by designated administrators.

E-mail and Network Operating System accounts will be created automatically for all employees with routine access to a computer. A principal or office administrator may request provision of e-mail and network operating system accounts for any employee who does not receive an account automatically.

E-mail and Network Operating System accounts are provided for the purpose of conducting District business, achieving educational goals, and for the pursuit of professional growth and limited high-quality personal learning activities. E-mail and files stored within Network Operating System accounts are subject to the same access and retention requirements as other public records covered by the Florida Public Records Law (see Addendum IV).

Employee E-mail and Network Operating System accounts will be disabled and/or re-enabled through use of the District Human Resources system upon the request of the pertinent principal or District administrator.

#### **5. Unacceptable Uses**

##### **a. Personal Safety**

Users shall not violate the provisions of the Florida K-20 Education Code, FERPA, or HIPAA when dealing with a student's right to privacy.

Users shall employ only District sanctioned and managed systems (networks, computing devices and/or peripherals, applications, and online services) to receive and transmit communications over the District network.

**b. Illegal and Prohibited Activities**

Users shall not engage in illegal activities (defined as a violation of local, state, and/or federal laws).

Users shall not plagiarize.

Users shall not violate the rights of copyright owners.

Users shall not install or download software that is not sanctioned by the District.

Users shall not attempt to defeat any District security component or to gain unauthorized access to District resources.

Users shall not make deliberate attempts to disrupt or destroy resources by spreading computer viruses or by any other means.

Users shall not use technology resources to engage in any activities, which interfere with or compromise the safety and security of the District's technology resources, employees, or students.

Users shall not attempt to gain unauthorized access (i.e. hacking) into commercial or governmental sites. Unauthorized access to these sites may involve criminal prosecution.

Users shall not employ privately owned devices and/or privately held wireless network accounts to circumvent policies enforced through the District Internet content filter or firewall or to violate the Guidelines for Acceptable Use of District Information Systems.

**c. Security**

Users shall not share passwords to District systems.

Users shall not provide unauthorized users with access to District e-mail or other District systems. Users will not access another user's e-mail, or other systems for which another user is approved for access, without authorization.

**d. Inappropriate Communications and Access**

Users shall maintain a professional tone to communications and will always comply with the District Code of Ethics when using District systems.

Users shall not use, view, download, copy, send, post or access obscene, profane, lewd, vulgar, or threatening communications, language, images or video. Users shall not use, view, download, copy, send, post or access material that advocates illegal acts, violence, or discrimination towards others.

Users shall not post information that could cause damage or pose a danger of disruption to the operations of the District.

Users shall not harass another person.

Users shall not post messages that are false or defame or libel any person or organization.

**e. Respecting Resource Limits**

Users shall not post chain letters or engage in “spamming”.

Users shall check their e-mail frequently and archive or delete unneeded messages promptly, in accordance with the Public Records law (see Addendum IV).

Users shall subscribe only to high quality discussion groups, mail lists, RSS feeds, or any other form of synchronous or asynchronous communications that are relevant to their education, career development, or operation of District business.

**f. Inappropriate Use of Resources**

Users shall not use technology resources for commercial purposes or financial gain.

Users shall not use District resources for political lobbying purposes.

Users shall not engage in activities that violate the District’s mission, goals, policies, or procedures.

**6. Responsibility of the District**

The District assumes no liability for the content of any advice or information acquired over the Internet, or any cost or charges incurred from this advice or information.

Any costs, liability or damages resulting from a users use of the Internet is the user’s responsibility.

The District assumes no liability for any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District.

The District is not liable for accidental or willful damage, accidental or willful destruction, or theft of personally owned computing devices and peripheral computing equipment (absence of District liability pertains to hardware, software, and data). The owner uses this equipment at his or her own discretion and risk. Willful and criminal destruction, damage, or theft of personally owned computing devices and peripherals will be treated as any other malicious or criminal act taking place on District premises or at District sponsored events.

## **1. The Internet**

A student will be allowed to utilize the Internet and/or online services for educational purposes unless the student's parent or guardian denies the student access by proactively requesting, completing, and returning a Denial of Permission Form (see Addendum I) to the student's school. The Denial of Permission Form is available to a parent or guardian upon request from the student's school.

If a student does not have parental permission to use the Internet and/or online services, teachers will make a reasonable effort to provide an alternative assignment covering the same Sunshine State Standards Benchmarks contained in the Internet-based instruction. In the event that equivalent instruction cannot be reasonably provided, an alternative assignment will be given to the student. However, the parent will assume responsibility for the student's mastery of those Benchmarks that cannot be addressed in the alternative assignment.

Staff is responsible for providing guidelines for Internet use by students.

Staff is responsible for supervising student access to the Internet and ensuring that access is being used for educational purposes and in accordance with Guidelines for Acceptable Use of District Information Systems.

## **2. Unacceptable Uses**

### **a. Personal Safety**

Student users shall agree not to contact or actually meet with anyone they originally met online unless their parent or guardian is aware of and approves of that contact or actual meeting.

Student users shall promptly disclose to their teacher or another school employee any message they receive or any interaction they engage in that is inappropriate or that makes the user feel uncomfortable.

### **b. E-mail**

Student users shall not access or use individual e-mail accounts at school.

All student e-mail collaboration shall be done through teacher-moderated accounts.

### **c. Synchronous and Asynchronous Online Communication and Social Networking Applications**

Student users shall not access or use online synchronous or asynchronous communication applications such as e-mail, chat, blogs, wikis or social networking Web site functions (i.e., discussion threads, document posting, RSS feeds, etc.) while at school. These restrictions apply unless: 1) this access and use takes place within a teacher-moderated online environment; 2) the online

activities are being used for legitimate instructional purposes; 3) the applications and/or functions are hosted on District servers behind the District firewall; 4) and students are restricted to interaction with other District students. The prescribed teacher moderation must include individual examination of each student communication and/or file posting to confirm that only appropriate and instructionally valid content is present.

The District's currently sanctioned and supported online Learning Management System provides the capability for teachers to implement moderated synchronous or asynchronous communication applications and online functions similar to those provided by social networking sites (providing the applications and functions are used for legitimate instructional purposes). The District sanctioned and supported Learning Management System restricts students to interaction with users registered in the District's currently sanctioned and supported online Learning Management System. This method is recommended and sanctioned by the District for delivery of these capabilities to District classrooms.

A process is in place for requesting permission to use other teacher moderated and appropriate online educational systems or resources not described above and/or to use teacher moderated and appropriate online educational systems or resources in a manner that varies with the above cited restrictions. If a principal or a teacher wishes to request this permission or if a principal or a teacher has a question about whether use of an online educational system or resource is permissible, the principal of the school contemplating use of that system or resource should contact the Information Technology Department and reference the sanctioning and editorial processes provided in Part Three – District Web Site Guidelines, Section 1 - Content and Section 2 - Security and Editorial Control of Content on School Web Sites within the [Guidelines for Acceptable Use of District Information Systems](#).

**d. Inappropriate Communications and Access**

Parents or guardians should instruct their student user(s) if there is material that they think would be inappropriate for them to access (in addition to material already blocked by the District firewall and content filter). The District fully expects that student users will follow these instructions.

Students shall inform a teacher if they mistakenly access inappropriate information or content.

**Part Three – District Web Site Guidelines**

**1. Content**

The subject matter and provided functionality of every page of a District office or school Web site must be related to District or school information, services, business, curriculum, or activities and must provide a legitimate instructional, operational, or administrative function. All work published on District Web pages must be free of spelling or grammatical errors.

All Web content and Web-based services posted by District offices and schools are subject to the following restrictions. District offices' and schools' Web content and Web-based services:

- 1) must be developed and provided by the District;
- 2) must be hosted on District servers behind the District firewall;
- 3) must be restricted to internal District use (no communication with sites external to District schools and offices is possible);
- 4) must be delivered in a manner compliant with the restrictions pertaining to student use of online synchronous or asynchronous communication applications and/or social networking Web site functions as cited in Part Two – Student/Community Access, Section 2c - Synchronous and Asynchronous Online Communication and Social Networking Applications within the Guidelines for Acceptable Use of District Information Systems (if a school elects to have its Web site make use of those types of applications and functions).

These restrictions apply unless one or more of the following applicable conditions can be conclusively demonstrated by an office or school to the Information Technology Department, in which case the applicable condition(s) will nullify the corresponding restriction(s). These applicable and nullifying conditions include the following:

- 1) A specific and legitimate administrative, operational, or instructional function(s) cannot be developed and provided by the District and can only be provided through the services of an Internet-based application service provider or developer.
- 2) A specific and legitimate administrative, operational, or instructional function(s) cannot be practically hosted on District servers behind the District's firewall.
- 3) Access to and by sites external to the District is essential to the effective use of a specific and legitimate administrative, operational, or instructional function(s).
- 4) In the case of school Web sites making use of synchronous and asynchronous communications applications and social networking functions, the application or function cannot be practically delivered as prescribed in Part Two – Student/Community Access, Section 2c - Synchronous and Asynchronous Online Communication and Social Networking Applications within the Guidelines for Acceptable Use of District Information Systems (teacher moderation that includes individual examination of each student communication and/or file posting to confirm that only appropriate and instructionally valid content is present is a nonnegotiable restriction).

Any contemplated variances from the restrictions cited above, ostensibly based on the conclusive demonstration of any of the applicable and nullifying conditions cited above, must be presented by the appropriate District office administrator or school principal to the Information Technology Department for review and sanction. Any resulting sanction is subject to continuous review and/or reversal by the Information Technology Department and the District Technology Advisory Committee. Any variances present on District Web pages prior to the adoption of this document and its stated policies are subject to review at the discretion of and by the Information Technology Department and the District Technology Advisory Committee to determine if any of the applicable and nullifying conditions cited above justify a specific previously existing variance or a class of previously existing variances.

Advertisements and/or content appearing on District Web pages shall comply with District guidelines (see Addendum II), which adhere to the self-regulatory guidelines of

the Children’s Advertising Review Unit, the Children’s Online Privacy Protection Act, and the Children’s Internet Protection Act.

District Webmaster assistance with school and office Web site construction will be most efficiently provided to those schools and offices using a District sanctioned Web editor (for which the District provides training, including the District’s internally developed online Web editor). A standardized District header and footer are available to all schools and offices for use in conjunction with District supported Web editors. All schools and offices are encouraged to migrate toward use of a District supported Web editor as part of a long-term goal to achieve a consistent user interface across all District Web pages.

No personal student information may be publicly posted on a District Web site. Documents publicly posted on District Web pages may not include a child’s phone number, street address or box number, or names of other family members. Information or any combination of information that facilitates identification of a student or which provides the physical location of a student at a given time or attendance at a particular school or school activity may not be included.

All school or office content that is out-of-date, inaccurate, or obsolete as of September 1 of each year is subject to removal at the discretion of the District Webmaster.

## **2. Components of a well conceived school Web site**

### **a. Basic components**

School information including name, address, telephone number, and e-mail link for the principal and/or school Web manager (required)

School community information including history, the campus, the community, and student body

Calendar of events including district calendar dates as a minimum

Testing information including test dates and preparation tips

Navigation tools including links to the main pages of the school site

### **b. Intermediate components**

Staff directory including contact information and responsibilities for administration, faculty, and other instructional personnel, excluding home phone numbers and addresses

Programs and/or Department information (particularly those that are unique to the school)

Club information

Sports information

Committee information

Parent/Teacher organization information

School Improvement Plan

Technology Plan

**c. Advanced components**

Teacher or Team or Course pages with basic information/syllabus, curriculum, resources, assignments/homework, and student work (many of these components will be addressable through use of the District's electronic grade-book and the related parent portal)

Faculty Committee pages

Extracurricular activities including clubs and sports

**3. Maintenance of appropriate content on school Web sites**

In order for school staff members to post files to their pages on the District Web server, the school's Web manager must establish a school Web site account with the District Webmaster.

The principal has sole editorial responsibility for the content appearing on their school's Web site. The principal may designate a Web manager to oversee the day-to-day operation and monitoring of the Web site; however, in the event that the principal does delegate the Web manager responsibilities, the principal and Web manager will meet at least once every semester to review the school Web site.

**4. Security and Editorial Control of Content on School Web Sites**

Unless individually denied at the discretion of the school principal, all instructional employees may post content to their school's Web server without prior editorial review of that content by the principal or the principal's designated Web manager. However, it is the responsibility of the principal, as the editor of their school's Web site, to inform and reiterate to all instructional employees that a signed agreement to comply with the provisions of the Guidelines for Acceptable Use of District Information Systems is an annual prerequisite for continued employment by the District. Any variance from full compliance will constitute sufficient reason for the principal to suspend an instructional employee's right to post content without editorial review; suspend an instructional employee's right to post content under any circumstances; or to begin appropriate disciplinary action that is commensurate with the degree of the employee's violation.

Unless individually granted at the discretion of the school principal, all non-instructional school employees (and/or school volunteers) may not post content to their school's Web server without prior editorial review of that content by the principal or the principal's designated Web manager. If the school principal chooses to grant a non-instructional employee (and/or school volunteer) the right to post content to the school Web server

without editorial review, the attendant responsibilities and consequences of the principal and the non-instructional employee (and/or school volunteer) are the same as those pertaining to the principal and instructional employees as cited above.

School-based personnel (of all types) do not have a de-facto right to include online synchronous or asynchronous communication applications or social networking functions on their Web pages. These elements can only be included if the District restrictions as prescribed in Part Two – Student/Community Access, Section 2c - Synchronous and Asynchronous Online Communication and Social Networking Applications within the Guidelines for Acceptable Use of District Information Systems are observed (provided a legitimate instructional purpose is being addressed) or if permission is obtained to implement student access and usage of these applications and functions outside of the prescribed District restrictions through the process described in Part Three – District Web Site Guidelines, Section 1 – Content, within the Guidelines for Acceptable Use of District Information Systems.

Students who are working on Web page projects must submit the work to the appropriate teacher for posting. Under no circumstances will students be allowed to post files directly to the District Web server.

It is the responsibility of the principal to work with or without a school Web manager to establish a process for familiarizing school employees with District policies pertaining to operation of the school Web site in a manner that is compliant with the provisions of the Guidelines for Acceptable Use of District Information Systems.

## **5. Guidelines for Copyright Compliance for Construction of District Web pages and other works**

Users will not plagiarize material that they find on the Internet (will not present that material in an online, electronic, or hard copy format as if it were original to the user).

To the extent possible original work and/or lawfully acquired copyright and royalty free material (text, graphics, animation, music, etc) should be used on District Web pages.

When it is necessary to use copyright protected material on a District Web page, users will respect the rights of copyright owners and will not infringe on those rights (using copyrighted material only with permission of the copyright holder and by citing all copyrighted sources in proper form).

If a work contains language that specifies acceptable use of that work, the user will follow the expressed requirements. When in doubt, the user will consult their teacher, media specialist, or designated District level resource person for assistance.

**Addendum I**

**Denial of Permission Form  
Multimedia Release, Internet Usage, and Web Publishing**

Media

My student does not have permission to be photographed, videotaped, or interviewed by print or broadcast media and/or be identified by name regarding school-sponsored programs and activities. Parents and guardians are advised that students who do not have multimedia release will not be able to appear in any print or broadcast media outside the regular school setting.

I do not give my permission \_\_\_\_\_

Internet Usage

My student does not have permission to access the Internet and/or online services for educational purposes. Parents and guardians are advised that students who are not permitted to use the Internet will not be able to access any online instructional resources.

I do not give my permission \_\_\_\_\_

Web Publishing

My student does not have permission to publish school-authorized work and graphics on any Escambia County School District Web site. Parents and guardians are advised that students who do not have permission to publish school-authorized work and graphics will not be able to produce any work for their school's Web site

I do not give my permission \_\_\_\_\_

My student's photograph may not be published on any District Web site even though information that identifies or locates students during the school day or at a school activity is not allowed to be published. Parents and guardians are advised that students who do not have permission to have the photographs published will not be included in photographs of school activities posted on their school's Web site.

I do not give my permission \_\_\_\_\_

Please sign this denial below. If you wish to exclude your child from any of the above activities, please circle and initial, "I do not give my permission." **This denial form will be effective from the date it is filed with the school until a new form is filed or a change of guardianship occurs.**

I, \_\_\_\_\_ the parent or guardian of

\_\_\_\_\_ do not give my permission for my child to participate in the above activities.

\_\_\_\_\_  
(Parent or Guardian's Signature)

\_\_\_\_\_  
(Date)

## **Addendum II**

### **Guidelines for Sponsorships or Advertisements appearing on District Web pages**

The District will not allow sponsorships or advertisements on its Web pages, which include but are not limited to any of the following categories:

#### **Direct Response/Call to Buy**

Advertising which directly solicits opportunities to purchase goods or services. This does not preclude all click-through messages, only those which are overly-aggressive in their exhortations to buy now.

#### **Excessive Distractions:**

Advertising such as contests, sweepstakes, coupons, promotions, free offers, or promises of instant downloads, which excessively detract or distract from the educational environment.

#### **E-Commerce:**

Advertising that promotes online transactions of products that do not have in place an 18 years old and over requirement as part of their purchase process.

#### **Pornography:**

Products, or the advertising of any products that contain material intended to be sexually arousing or erotic.

#### **Sex:**

Products, or the advertising of any products that contain images or descriptions of sexual activity.

#### **Nudity:**

Products, or the advertising of any products that contain bare or visible genitalia, pubic hair, buttocks, female breasts, etc. (this includes models in swimwear, especially swimwear photos.)

#### **Violence:**

Products, or the advertising of any products containing graphic images or written descriptions of wanton violence or grave injury (mutilation, maiming, dismemberment, etc.). Includes graphically violent games.

#### **Illegal Activity:**

Products, or the advertising of any products advocating, promoting, or giving advice on carrying out acts widely considered illegal. This includes lock-picking, bomb-making, fraud, breaching, computer security (“hacking”), phone service theft (“phreaking”), pirating software, or evading law enforcement.

#### **Gambling:**

Products, or the advertising of any products relating to gambling services, or information relevant primarily to gambling.

#### **Profanity/Language:**

Products, or the advertising of any products that contain crude, vulgar, or obscene language or gestures.

#### **Tasteless/Gross:**

Products, or the advertising of any products that contain reference to bodily functions as well as tasteless humor, graphic medical photos, and some extreme forms of body modification (cutting, branding, genital piercing).

#### **Lingerie:**

Products, or the advertising of any products that contain models in lingerie, (except those that qualify for Nudity).

#### **Murder/Suicide:**

Products, or the advertising of any products containing information on committing murder or suicide.

Hate/Discrimination:

Products, or the advertising of any products advocating discrimination against others based on race, religion, gender, nationality, or sexual orientation.

Drugs:

Products, or the advertising of any products advocating or promoting recreational use of any controlled substance.

School cheating:

Products or the advertising of any products that promotes plagiarism or similar cheating among students (such as by offering term papers, exam keys, etc.).

Alcohol:

Products, or the advertising of any products advocating or promoting recreational use of alcohol.

Tobacco:

Products or the advertising of any products advocating or promoting recreational use of tobacco.

Personals:

Products, or the advertising of any products containing personal advertisements, including “mail-order” brides.

Weapons:

Products, or the advertising of any products containing information on use of weapons, weapon collecting, or weapon making.

## **Addendum III**

### **Use of Personally Owned and Individually Issued Computing Devices (devices capable of Internet connectivity) and Peripheral Equipment**

#### **Part I: Personally Owned Computing Devices and Peripheral Equipment**

##### **Documentation of Permission for On District Premises Usage and/or at District Sponsored Events Usage**

Computing devices and peripheral equipment owned by individual students or individual District employees can be sanctioned for use on District premises and/or at District sponsored events at the discretion of the pertinent school principal or supervising District administrator (and with notification of the sanctioned usage to the Information Technology Department). A District “Usage Permission Form” must be completed by the owner of the computing device or peripheral equipment and by the issuing principal or supervising District administrator before a personally owned computing device or peripheral can be used on District premises and/or at District sponsored events. The form will specify the sanctioned uses of the device or peripheral, the responsibilities of the owner of the device or peripheral (including the responsibilities of the parent or guardian in the case of sanctioned student usage, as acknowledged by a witnessed signature), the responsibilities of the school or District department sanctioning the District usage, and the serial#, model#, and manufacturer of the device or peripheral (see detailed explanation of these responsibilities and sanctioned usages in the language below). A copy of the District “Usage Permission Form” appears at the end of this addendum.

The original District “Usage Permission Form” will be kept on file at the issuing school or District department, and a copy will be provided to the recipient/equipment owner.

##### **Requirements and Guidelines for On District Premises and/or at District Sponsored Events Usage**

All sanctioned usage must facilitate legitimate instructional and/or business tasks or duties. The sanctioned usage granted by the pertinent school principal or supervising District administrator may be reviewed by the Information Technology Director and the District Technology Advisory Committee on behalf of the Superintendent and Board to determine if the subject computer and/or peripheral (or a class of device types) is capable of efficient and secure usage within the District’s technology work environments; efficient and secure transition between the District’s technology work environments and off District premises technology work environments; and operation within the guidelines contained in the District Acceptable Use Policy (Acceptable Use of District Information Systems document). The sanctioned usage granted by the pertinent school principal or supervising District administrator may also be reviewed by the Information Technology Director and the District Technology Advisory Committee on behalf of the Superintendent and Board to determine if a legitimate instructional and/or business task or duty is being facilitated by the sanctioned usage and if the subject computer and/or peripheral (or a class of device types) is being used in an appropriate manner (a manner that is compliant with the guidelines contained in the School Board Rules and Procedures Manual, Acceptable Use of District Information Systems document, and the Student Rights and Responsibilities Handbook). District sanctioned usage can be withdrawn at any time at the discretion of the pertinent school principal or supervising District administrator or through the above referenced review processes.

Use of personally owned computing devices and/or peripheral equipment, while on District premises, to access private wireless network accounts and/or privately purchased services are

explicitly excluded from sanctioned usage. Student use of voice services available on sanctioned student owned computing devices is restricted to the usage times pertaining to cellular phones as described in the Student Rights and Responsibilities Handbook. Employee usage of voice services available on sanctioned employee owned computing devices is restricted to reasonable levels of personal and professional usage as determined by the pertinent school principal or supervising District administrator. Sanctioned usage of personally owned computing devices and/or peripheral equipment, while on District premises, is explicitly restricted to use with District sanctioned networks and systems. In the case of computing devices and/or peripheral equipment owned by individual students, sanctioned usage is explicitly restricted to areas and times under the direct supervision of instructional and/or administrative personnel and those devices and equipment must be turned off in all other areas and at all other times. Sanctioned usage of student owned computing devices and/or peripheral equipment explicitly excludes use while on a school bus at any time and such devices and equipment must be turned off for the duration of any bus transportation.

Use of personally owned computing devices and/or peripheral equipment, while at District sponsored events that occur off of District premises and without connectivity to the District network, to access private wireless network accounts and/or privately purchased services is allowable if the access facilitates legitimate District instructional and/or business tasks and the access is stated as part of the owner's sanctioned usage in the District "Usage Permission Form" on file with the subject school or District department.

Minimum Hardware Specifications are posted on the District Web site to assist principals and District administrators in determining if personally owned computing devices are adequately equipped for effective and secure usage. Specific peripherals and/or classes or manufacturers of computing devices may be determined to be ineligible for sanctioned usage based on the above described review process. Principals and District administrators should consult their School Technology Contact and/or their assigned District Technical Support personnel for assistance in determining the appropriate setup of any personally owned computing device they are considering for sanctioned usage. This setup may include, but is not limited to installation of the standard District desktop and network operating systems and filtering and security components. The District prescribed setup must take place before any personally owned computing device is used on District premises to access District sanctioned networks and systems or at District sponsored events. Any attempt, by the owner of a sanctioned computing device or peripheral, to remove and/or defeat any District setup component will result in the immediate withdrawal of the sanctioned usage status.

Personally owned computing devices and peripheral equipment sanctioned for usage by the District are subject to all District policy and guidelines documents governing technology usage and ethical conduct, including but not limited to the School Board Rules and Procedures Manual, the District Acceptable Use Policy (Acceptable Use of District Information Systems document), and the Student Rights and Responsibilities Handbook. Violation of any technology usage rules and/or ethics rules related to technology usage contained in the referenced documents can result in, but is not limited to withdrawal of the sanctioned usage status, disciplinary and/or legal actions as defined within those documents, and possible confiscation of the subject computing and/or peripheral equipment for examination to determine if disciplinary and/or legal action is warranted. All content stored on privately owned computing devices and/or peripherals sanctioned for usage by the District is subject to public records law, and there can be no expectation of privacy on the part of the equipment owner except in cases where legal rights to privacy are involved (i.e., issues related to employee and student HIPAA and FERPA

compliance). Reasonable supervision and examination will be conducted to ensure use compliant with the terms of the Acceptable Use of District Information Systems document and the Student Rights and Responsibilities Handbook.

### **Property Control Procedures for On District Premises Usage**

The District is not liable for accidental or willful damage, accidental or willful destruction, or theft of personally owned computing devices and peripheral computing equipment (absence of District liability pertains to hardware, software, and data). The owner uses this equipment at his or her own discretion and risk. Willful and criminal destruction, damage, or theft of personally owned computing devices and peripheral computing equipment will be treated as any other malicious or criminal act taking place on District premises or at District sponsored events.

## **Part II: Individually Issued District Computing Devices and Peripheral Equipment**

### **Documentation of Permission for Off District Premises Usage**

District computing devices and peripheral equipment issued to individual students or individual District employees can be sanctioned for off District premises usage at the discretion of the pertinent school principal or supervising District administrator. A District “Usage Permission Form” must be completed by the recipient and by the issuing principal or supervising District administrator before an individually issued device or peripheral can be taken off District premises. The form will specify appropriate uses of the device or peripheral, the responsibilities of the recipient of the issued District device or peripheral (including the responsibilities of the parent or guardian in the case of sanctioned student usage, as acknowledged by a witnessed signature), the responsibilities of the school or District department issuing the District device or peripheral, and the serial#, model#, and manufacturer of the District device or peripheral (see detailed explanation of these responsibilities and sanctioned usages in the language below). A copy of the District “Usage Permission Form” appears at the end of this addendum.

The original District “Usage Permission Form” will be kept on file at the issuing school or District department and a copy will be provided to the recipient/equipment owner.

### **Requirements and Guidelines for Off District Premises Usage**

All sanctioned off District premises usage of individually issued computing devices and peripheral equipment must facilitate legitimate instructional and/or business tasks or duties. The sanctioned usage may be reviewed by the Information Technology Director and the District Technology Advisory Committee on behalf of the Superintendent and Board to determine if the subject device and/or peripheral (or a class of device types) is capable of efficient and secure usage within the District’s technology work environments; efficient and secure transition between the District’s technology work environments and off District premises technology work environments; and operation within the guidelines contained in the District Acceptable Use Policy (Acceptable Use of District Information Systems document). This sanctioned usage can be withdrawn at any time at the discretion of the pertinent school principal or supervising District administrator or through the above referenced review process. The sanctioned usage may also be reviewed by the Information Technology Director and the District Technology Advisory Committee on behalf of the Superintendent and Board to determine if a legitimate instructional and/or business task or duty is being facilitated by the sanctioned usage and if the subject computer and/or peripheral (or a class of device types) is being used in an appropriate manner (a manner that is compliant with the guidelines contained in the School Board Rules and Procedures Manual, the District Acceptable Use Policy (Acceptable Use of District Information Systems document), and the Student Rights and Responsibilities Handbook. This sanctioned

usage can be withdrawn at any time at the discretion of the pertinent school principal or supervising District administrator or through the above referenced review process.

Use of individually issued computing devices and/or peripheral equipment, while on District premises, to access private wireless network accounts and/or privately purchased services is explicitly excluded from sanctioned usage. Sanctioned usage of individually issued computing devices and/or peripheral equipment, while on District premises, is explicitly restricted to use with District sanctioned networks and systems. In the case of computing devices and/or peripheral equipment issued to individual students, sanctioned usage is explicitly restricted to areas and times under the direct supervision of instructional and/or administrative personnel, and those devices and equipment must be turned off in all other areas and at all other times. Sanctioned usage of computing devices and/or peripheral equipment issued to individual students explicitly excludes use while on a school bus at any time, and such devices and equipment must be turned off for the duration of any bus transportation.

Use of individually issued computing devices and/or peripheral equipment, while at District sponsored events that occur off of District premises and without connectivity to the District network, to access private wireless network accounts and/or privately purchased services is allowable if the access facilitates legitimate District instructional and/or business tasks and the access is stated as part of the owner's sanctioned usage in the District "Usage Permission Form" on file with the subject school or District department.

Minimum Hardware Specifications are posted on the District Web site to assist principals and District administrators in determining if individually issued computing devices are adequately equipped for effective and secure usage. Principals and District administrators should consult their School Technology Contact and their assigned District Technical Support personnel for assistance in the proper setup of any individually issued computing device or peripheral that they are considering for sanctioned off District premises usage. This setup may include, but is not limited to installation of the standard District desktop and network operating systems and filtering and security components. This setup must take place before any individually issued computing device or peripheral is used off District premises. Any attempt, by the assigned user of a sanctioned device or peripheral, to remove and/or defeat these District installed components will result in the immediate withdrawal of the sanctioned usage status.

Individually issued computing devices and peripheral equipment sanctioned for off District premises usage are subject to all District policy and guidelines documents governing technology usage and ethical conduct including but not limited to: the School Board Rules and Procedures Manual, the District Acceptable Use Policy (Acceptable Use of District Information Systems document), and the Student Rights and Responsibilities Handbook. Violation of any technology usage rules and/or ethics rules related to technology usage contained in the referenced documents can result in, but is not limited to withdrawal of the sanctioned usage status, disciplinary and/or legal actions as defined within the referenced documents, and possible confiscation of the subject computing device and/or peripheral equipment for examination to determine if disciplinary and/or legal action by the District is warranted. All content stored on individually issued computing devices and/or peripherals sanctioned for usage by the District is subject to public records law, and there can be no expectation of privacy on the part of the equipment owner except in cases where legal rights to privacy are involved (i.e., issues related to employee and student HIPAA and FERPA compliance). Reasonable supervision and examination will be conducted to ensure use compliant with the terms of the Acceptable Use of District Information Systems document and the Student Rights and Responsibilities Handbook.

### **Property Control Procedures for Off District Premises Usage**

Willful damage and destruction or theft of individually issued computing devices and/or peripheral computing equipment will be treated as any other willful or criminal act resulting in damage, destruction, or loss of District owned equipment. Restitution and appropriate criminal penalties will be sought through legal action taken against the perpetrator. Accidental damage, destruction, or loss of individually issued computing devices and/or peripheral computing equipment, reported to the Risk Management Office or the District Information Technology Office through established property incident and repair request procedures, will result in the repair or replacement of the subject equipment through the District Risk Management fund or the District Technology Maintenance Contract. The issuing school or District department will be responsible for repair or replacement of the subject equipment in the event that District policy prohibits use of the Risk Management fund or the Technology Maintenance Contract to repair or replace the subject equipment. This situation could result if the circumstances of the destruction, damage, loss, or theft do not fall within Risk Management Guidelines or Technology Maintenance Contract proviso for replacement or repair or because established property incident reporting or repair request procedures were not followed. Regardless of the circumstances resulting in the damage, destruction, loss, or theft of individually issued computing devices; the issuing principal or supervising District administrator will be responsible for providing an explanation of the incident to the Superintendent and Board. That explanation will include a summary of the circumstances and events leading to the damage, destruction, loss, or theft as well as a description of measures that will be implemented to prevent a reoccurrence of similar incidents.

In the event that an individually issued computing device or peripheral is damaged, destroyed, lost, or stolen and due diligence in proper care or in following property incident reporting procedures was not exercised by the pertinent employee or parent, the issuing principal or supervising District administrator will decide whether to seek lawful restitution for the equipment or peripheral. If no implication of willful or criminal action is apparent on the part of the pertinent employee or parent, the first option for restitution sought by the District should be a claim against any applicable insurance coverage possessed by the pertinent employee or parent.

### **Appropriate Uses of Personally Owned and Individually Issued Computing Devices and Peripheral Equipment (appropriate uses may be restricted or expanded at the discretion of the Superintendent and Board)**

#### **Teacher Usage:**

- Personal Productivity (use of word processing, spreadsheet, database, grade-book, email, Web page and other Internet format editor, and database software to complete clerical and classroom management tasks associated with establishing and maintaining an effective instructional environment)
- Lesson Plan Development (use of Web browser, District sanctioned social networking, word processing, online digital textbook and reference volume, presentation, simulation, integrated learning system, instructional management system, Web page and other Internet format editor, and multimedia software to construct and technically enrich lessons and to extend the reach of the classroom)
- Professional Growth (use of Web browser, District sanctioned social networking, multimedia, collaboration, instructional management system, list serve, video and audio conferencing, and

ASP - application service provider professional development software to engage in online and electronically delivered professional development)

- Differentiation of Instruction (use of academic data mining, grade-book, integrated learning system, instructional management system, and other software associated with lesson development to tailor instruction to individual student needs)
- Research and Peer to Peer Collaboration (use of Web browser, District sanctioned social networking, search engine, online digital textbook and reference volume, email, instructional management system, Web page and other internet format editor, and list serve software to obtain targeted instructional and professional development resources)
- Internet Content Production (use of District sanctioned social networking functions and Web page and other Internet format editors to produce and post research information and projects for viewing by peers, parents, and community)

#### **Student Usage:**

- Research (use of Web browser, District sanctioned social networking, Internet subscribing and collaboration, search engine, online digital textbook, and reference volume software to respond to assignments calling for students to obtain, analyze, synthesize, evaluate, and present information)
- Personal Productivity (use of word processing, spreadsheet, database, teacher moderated email and other teacher moderated Web-based communication systems, and presentation software to complete assignments and to construct collaborative and individual projects)
- Computer Assisted Instruction (use of a Web browser and other vendor specific client software to access introductory and remedial instruction in academic content areas and computer literacy)
- Multimedia Production (use of digital audio/video and graphics editing software to enhance the communicative quality of students' assignments and collaborative and individual projects)
- Internet Content Production (use of District sanctioned social networking functions and Web page and other Internet format editors to produce and post research information and projects for viewing by peers, parents, and community)

#### **District Level Employee Usage:**

- Personal Productivity (use of word processing, spreadsheet, email, terminal emulation, data mining, Web page and other Internet format editor, and database software to complete clerical, administrative, and management tasks associated with establishing and maintaining an effective District level office)
- Presentation and Information Dissemination (word processing, presentation, Web page and other Internet format editor, and multimedia software to construct professional presentations for delivery to District employees)
- Professional Growth (use of Web browser, multimedia, list serve, video and audio conferencing, vendor specific client, and ASP - application service provider professional development software to engage in online and electronically delivered professional development)

- Professional Development Delivery (use of academic data mining, learning management system, presentation, multimedia, Web page and other Internet format editor, video and audio conferencing, and other software to create and deliver targeted and sustained training to District employees)
- Research and Peer to Peer Collaboration (use of Web browser, District sanctioned social networking, search engine, online digital reference volume, email, Web page and other Internet format editor, and list serve software to obtain the clerical, administrative, and management resources associated with establishing and maintaining an effective District level office)

## Usage Permission Form

This form defines the terms of District sanctioned usage of personally owned and individually issued computing devices and/or peripheral equipment. The terms of this sanctioned usage are permissible as defined and permitted through the processes and criteria contained in the Acceptable Use of District Information Systems document and/or the Student Rights and Responsibility Handbook. This sanctioned usage can be withdrawn at any time as defined and permitted through the processes and criteria contained in those documents.

\_\_\_\_\_  
Date of Sanctioned Usage Issuance

\_\_\_\_\_  
Date of Withdrawal of Sanctioned Usage

Device/Equipment is:

Personally Owned \_\_\_\_\_

District Owned and Individually Issued \_\_\_\_\_

Manufacturer \_\_\_\_\_ Model Name/Number \_\_\_\_\_

Serial Number \_\_\_\_\_ MAC Address \_\_\_\_\_

District Property Number \_\_\_\_\_

\_\_\_\_\_  
School or District Department Sanctioning Usage

\_\_\_\_\_  
Principal or District Department Administrator Sanctioning Usage (print)

\_\_\_\_\_  
Employee or Student Granted Sanctioned Usage (print)

\_\_\_\_\_  
Parent/Guardian of Student Granted Sanctioned Usage (print)

Specific Types of Sanctioned Usage:

Only those Sanctioned Uses Defined as Appropriate in the Acceptable Use of District Information Systems, Addendum III \_\_\_\_\_

Sanctioned Uses in Addition to those Defined as Appropriate in Acceptable Use of District Information Systems, Addendum III \_\_\_\_\_

List of Additional Sanctioned Usages

- 1) \_\_\_\_\_
- 2) \_\_\_\_\_
- 3) \_\_\_\_\_

I have reviewed, understand, and agree with the information supplied above. I have reviewed, understand, and agree with the terms of liability and indemnification regarding personally owned and individually issued computing devices and/or peripheral equipment as defined in the Acceptable Use of District Information Systems, Addendum III.

\_\_\_\_\_  
Principal or District Department Administrator Sanctioning Usage (signature)

\_\_\_\_\_  
Employee or Student Granted Sanctioned Usage (signature)

\_\_\_\_\_  
Parent/Guardian of Student Granted Sanctioned Usage (signature, witnessed at school site)

## **Addendum IV**

### **Email Retention**

Electronic mail is subject to the same access and retention requirements as other public records covered by the Florida Public Records Law.

#### **Who Must Retain Electronic Mail**

In general, the sender is responsible for retaining **internally produced** messages. Messages received from sender within the School district are considered duplicates and can be deleted as desired. If the message is sent out in both electronic and paper copy, the sender only has to retain one copy. If an email message originates **outside the school district**, the recipient's copy is considered to be an original and thus it is the recipient's responsibility to keep the record.

#### **How Messages Should Be Saved**

Messages can be saved in one of three ways:

1. Print a paper copy and file by subject and date.
2. Retain messages in an electronic subject folder in text format. These can be opened for viewing in most word processing programs. A unique file name must be assigned to saved email items. Attachments must be saved separately and may be saved in their original file format. They can be open and viewed by launching the program in which the file was originally created. Attachments can be saved using the original file name of the attachment.
3. Messages can be retained by archiving them in GroupWise, but this requires GroupWise software to access the stored documents and attachments.

It is best to print a hard copy of the message because these records can be stored with similar records having the same retention requirements, thus simplifying their disposal, and a build-up of saved email can inhibit the performance of your computer.

GroupWise users who are planning to retire, terminate employment with the district, or transfer to another school or department should review messages in their current Mailbox and Sent Items folders and print those required for records retention purposes. These should be filed with other records being stored for retention/audit purposes. Once these procedures are completed, the original email messages may be deleted.

#### **How Long Email Messages Must Be Saved**

The General Records Schedule GS1-SL for State and Local Government Agencies, November 1, 2006, and General Records Schedule GS7 for Public Schools Pre-K – 12 Adult & Vocational/Technical, June 1998, published by the Florida Department of State, Division of Library and Information Services, Bureau of Archives and Records Management, sets the guidelines for the retention of specific types of

records. The content of the electronic messages determines the disclosure and retention procedures. All schools have copies of these schedules on file, and the schedules may be downloaded from the following Website:  
<http://www.escambia.k12.fl.us/Master/Index.asp>.

**General Email Categories and Minimum Retention Requirements:**

Directory Information OSA\*

Job Announcements 180 days after expiration

Meeting Agendas OSA\*

Routine Correspondence Three Fiscal Years

\*Obsolete, Superseded, or Administrative value is lost. The custodian of the record determines when a record is OSA.

**Summary**

The majority of email may be deleted after its usefulness. Your main area of responsibility is to save what you send and what you receive from external sources, then use the above chart to decide how long the record should be retained.

## **Addendum V**

### **Escambia School District Data Access Guidelines**

The guidelines contained in this addendum govern employee use of District applications and/or functionalities to access and use all District data types while conducting the official business of the School District of Escambia County. The guidelines are compliant with, and by reference incorporate, all applicable District, state, and federal policies and guidelines regarding employee and student rights to privacy and confidentiality (including but not limited to FERPA and HIPAA). These guidelines are separate and distinct from District policy governing public access to information, but they are compliant with those policies.

#### **1) Compilation, Implementation, and Administration of Data Access and Usage Guidelines for All District Data Types**

- 1.1) The Superintendent, with the advisement of the District Technology Advisory Committee, will assign appropriate District Directors (designated as District Data Administrators) with the responsibilities for deployment of new data access applications and/or functionalities and with the responsibilities for compilation, implementation, and administration of the associated data access and usage guidelines (and when appropriate, for refinement of existing data access and usage guidelines and their implementation and administration).
- 1.2) District Data Administrators will compile new data access and usage guidelines and/or refine existing data access and usage guidelines based upon lessons learned, management priorities, and user requirements as employee access to all District data types broadens through deployment of new applications and/or functionalities.
- 1.3) The Superintendent, with the advisement of the District Technology Advisory Committee, will continuously review and approve new and/or refined guidelines as submitted by District Data Administrators for governing employee access and use of District data.

- 1.4) District Data Administrators will identify School and Office Data Administrators to provide training, account registration/activation, and management services for the users of data access applications and/or functionalities within individual schools and offices.
- 1.5) School and Office Data Administrator personnel will consist of school principals and germane District office supervisors, coordinators, and specialists.
- 1.6) School and Office Data Administrators will determine the best procedures for delivery of training, account registration/activation, and account management responsibilities based upon workflow, organizational structure, and job responsibilities in that school or office.
- 1.7) The user training, account registration/activation, and management procedures and processes established by School and Office Data Administrators will be compliant with the implementation and administrative guidelines defined for each of the District's data types as determined by the applicable District Data Administrator.
- 1.8) The user account management processes, administered by School and Office Data Administrators, will insure that user access privileges and accounts are kept current and in alignment with changes in personnel status and duty assignments within and among individual schools or offices.
- 1.9) School and Office Data Administrators will have the option to delegate training, account registration/activation, and account management responsibilities to a School or Office Data Coordinator. School and Office Data Coordinator personnel may be the school or office Technology Contact or any school or office-based employee with training/skills in the appropriate access and use of District data.
- 1.10) The Data Coordinator in an individual School or Office will report directly to the School or Office Data Administrator and will execute training, account registration/activation, and account management responsibilities according to the procedures established by the Data Administrator for that school or office.
- 1.11) Electronic archives of all information regarding user accounts will be maintained in a manner consistent with procedures used for other district level applications.
- 1.12) District Data Administrators will serve as the point of contact for audit reviews and other inquiries related to their assigned data access and usage responsibilities.
- 1.13) The Office of Information Technology will maintain the requisite hardware and system software (including appropriate encryption) associated with provision of access and use of the data types approved by the Superintendent.
- 1.14) All District data access and usage, through newly deployed applications and/or functionalities, will at a minimum require training of employee users in the operation of the application and/or functionality; awareness of District, state, and federal guidelines governing data access and use; and awareness of the statistical and/or ethical issues associated with appropriate data use.
- 1.15) Guidelines for access and use of specific District data types (i.e., various Finance, Human Resource, Payroll, Operations, Inventory, and Student data types) will be addressed by additional sections of this guidelines document that are specific to each data type. These specific guidelines sections will be compiled and/or refined by the appropriate District Data Administrator as defined above and will be supplemental to this general guidelines section.
- 1.16) The general and specific guidelines sections of this document are also supplemented by the procedures for delivery of training, account registration/activation, and account management established by the School and

Office Data Administrators at individual schools and offices. Those individual schools' and offices' procedures are hereby referenced and formally incorporated into this document.

**2) Access and Usage Guidelines for Student Academic Achievement, Demographic, and Disciplinary data**

- 2.1) Prerequisites for individual access to and use of student achievement, demographic, and disciplinary data through District deployed applications and/or functionalities and the procedures for assurance that the prerequisites have been met are below.
  - 2.1.1) The user will complete the application and/or functionality training provided by the local School/Office Data Administrator and/or Data Coordinator.
    - 2.1.1.1) This includes instruction that will prevent inappropriate use of aggregated and disaggregated student data.
  - 2.1.2) The user will complete the online registration form.
  - 2.1.3) The School/Office Data Administrator and/or Data Coordinator will activate the individual accounts.
- 2.2. Appropriate student achievement, demographic, and disciplinary data access and usage contexts are cited below with departures from these cited contexts defined and approved by the School/Office Data Administrators (this is not intended to be an exhaustive list of appropriate usage contexts, other appropriate contexts will likely emerge as implementation proceeds).
  - 2.2.1) School and District office level individual access and usage of aggregated and/or disaggregated student achievement, demographic, and disciplinary data
    - 2.2.1.1) Routine teacher differentiation of instruction to address individual and group academic needs
    - 2.2.1.2) Parent conference
    - 2.2.1.3) Individual professional development planning, IPDP
    - 2.2.1.4) State and Federal reporting requirements, NCLB (Title I, EETT, AYP), ESE, etc.
    - 2.2.1.5) Construction of grant applications requiring aggregated data on ethnic, demographic, and academic performance sub-groups
  - 2.2.2) Use of a team (i.e., parents, teachers, counselors, ESE personnel, Alternative Education personnel, and administrators) to review and examine individual academic achievement, demographic, and disciplinary data for prescriptive action
    - 2.2.2.1) AIP
    - 2.2.2.2) IEP
    - 2.2.2.3) Placement in exceptional or alternative programs
  - 2.2.3) Use of a committee (i.e., SAC, SIP, Technology Committee) to review and examine aggregated and/or disaggregated academic achievement, demographic, and disciplinary data for data driven prescriptive action and planning
    - 2.2.3.1) School Improvement and planning processes
  - 2.2.4) School/Office Data Administrators define and approve additional appropriate usage contexts and context restrictions that are specific to their school and supplemental to District defined usage contexts. Additional contexts would likely, at a minimum, address the issues cited below.

- 2.2.4.1) Permitted locations for data access
    - 2.2.4.2) Permitted methods of data duplication and transmission, electronic, hard copy, e-mail, etc.
  - 2.3) Use of aggregated and/or disaggregated student achievement, demographic, and disciplinary data to facilitate professional growth
    - 2.3.1) Use of aggregated and/or disaggregated student achievement, demographic, and disciplinary data in the contractually prescribed teacher evaluation process is categorically prohibited
    - 2.3.2) Use of aggregated and/or disaggregated student achievement, demographic, and disciplinary data to determine a trend of effectiveness regarding specific types of pedagogy in order to prescribe appropriate professional development
- 3) **Potential Additional Data Types Requiring Specific Data Access and Usage Guidelines (potential data types list is intended to be illustrative not exhaustive)**
  - 3.1) Human Resources, Finance, Payroll, Operations, and Inventory