

# INFORMATION TECHNOLOGY

---

## User Standards and Guidelines Manual May 2010



Division of Information Technology  
<http://www.palmbeachschools.org/it/security.asp>

## Table of Contents

1.	Introduction .....	4
2.	Definitions .....	5
3.	General Security Standards .....	14
3.1.	District Responsibilities .....	14
3.1.1.	Security Objectives.....	14
3.2.	User Responsibilities .....	14
3.4.	Biometric Record Standards.....	16
3.5	Encryption Standards .....	17
3.6	E-Signatures .....	17
4	Acceptable Use Standards .....	19
4.1	Applicable Policies and Standards .....	19
4.2	E-mail and Calendaring System Acceptable Use .....	21
4.3	Software and Hardware Acceptable Use .....	21
4.4	Examples of Unacceptable Uses of Technology .....	22
5	World-wide Web Standards and Guidelines .....	23
5.1	Safe Surfing Guidelines.....	23
5.1.1	Protect Your Personal Information .....	23
5.1.2	Know Who You Are Dealing With .....	23
5.1.3	Use Anti-Virus and Anti-Spy ware Software and a Firewall.....	23
5.1.4	Setup Your Software Properly and Update Them Regularly .....	23
5.1.5	Protect Your Passwords.....	23
5.1.6	Back Up Important Files.....	23
5.1.7	Contact IT Security If Something Goes Wrong Online .....	24
6	E-mail AND OTHER ELECTRONIC COMMUNICATION Standards and Guidelines .....	25
6.1	Spam .....	25
6.2	User Responsibilities .....	25
6.2.1	Public Records Law Adherence .....	25
6.2.2	Standards for Retention of E-mail and Other Electronic Messages .....	26
6.3	E-mail and Calendaring Privacy.....	28
6.4	Shared Accounts .....	28
6.5	E-mail Distribution Lists .....	29
6.5.	Accessing another User's E-mail.....	29
6.6.	Backup and Restoration of E-mail Messages.....	29
6.7.	E-mail Guidelines .....	29
6.7.1.	Suggestions for Effective Use.....	29
6.7.2.	Capacity and Conservation of Resources .....	30
6.9	User Account Termination .....	30

# IT User Standards and Guidelines Manual

---

7. Network Use Standards and Guidelines.....	32
7.1. Network Authentication.....	32
7.2. Network Inactivity.....	32
7.3. Approved Network Devices.....	32
8.1. Password Expiration.....	34
8.2. Password Confidentiality.....	34
8.3. Compromised Passwords.....	34
8.4. Enforcement.....	35
8.5. Password Construction Guidelines.....	35
8.5.1. Password Length.....	35
8.5.2. Composition.....	35
8.5.3. Password Examples.....	35
9. Wireless Network Standards and Guidelines.....	37
9.1. Approved Wireless Access Points.....	37
9.2. Authenticated Access.....	37
9.3. Encryption.....	37
9.4. Network Monitoring.....	37

**Appendix 1**      **NOTICE OF CONDITIONS FOR STUDENT USE OF DISTRICT TECHNOLOGY**

**Appendix 2**      **PBSD 1664 – Employee Internet/Intranet Services Acknowledgement and Consent**

**Appendix 3**      **PBSD 2359 – Third Party Internet/Intranet Services Acknowledgement and Consent**

## 1. INTRODUCTION

The Division of Information Technology (IT) for the School District of Palm Beach County (District) supports a large countywide information network to provide high-speed access to the District's information resources, including internal educational and business systems and access to the Internet. These systems are critical and vitally important resources for the District to accomplish its mission and achieve its goals.

Despite the educational and business benefits of information technologies, there are risks associated with their use. Internet users face the risk of exposure to material that is sexually explicit or offensive, hateful or violent, or contains malicious software that can harm information resources. The District's firewall and filtering systems attempt to block these risks but access of such material may occur inadvertently through searching for educational content about people, places or issues. Other risks include cyber bullying, sexting, unreliable information, identity theft, spam, viruses and spy ware.

In an effort to minimize these risks to students, the first and most important standard relating to students is that all student activity on the Internet shall be supervised by a teacher, administrator, or other designated District employee.



The IT User Standards and Guidelines Manual (Manual) provides a framework for a *safe computing environment* for the District's information resource and technology users. Following the standards within this Manual will minimize the threats to the District's information resources and protect its users. To be effective, information security must be a team effort involving the participation and support of everyone, including parents, students, teachers, third parties, and administrators. A single unauthorized exception to security measures can jeopardize other users and systems, even outside organizations that share information resources with the District. The interconnected nature of information resources and technology requires that all users observe these standards to create an effective and enjoyable computing experience.

Included in this document are Acceptable Use Standards and General Security Standards, along with more specific standards for web, e-mail, passwords, and network access.

These guidelines and standards shall be interpreted consistently with the provisions of the United States, and Florida Constitutions, Florida and federal law, and federal and state rules and regulations.

## 2. DEFINITIONS

These definitions apply to terms within this Manual, as well as the School Board policies that incorporate this Manual by reference.

<b>Access</b>	To enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information technology resources.
<b>Access Control</b>	The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.
<b>Access Unit</b>	A physical user/end user interface to an information system. For example a workstation, terminal, and laptop
<b>Account</b>	See User ID.
<b>Asset</b>	See Information Asset/Resource/Technology.
<b>Asymmetric Cryptosystem</b>	See Key Pair.
<b>Attack</b>	An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to violate the security of a system.
<b>Attribution</b>	An explicit or formal acknowledgment of ownership or authorship.
<b>Authentication</b>	The process that verifies the claimed identity or access eligibility of a station, originator, or individual as established by an identification process.
<b>Authorization</b>	A positive determination by the information resource/data owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the resource/data owner's permission to access the resource.
<b>Automated Transaction</b>	A transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.
<b>Best Practice</b>	A technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success.
<b>Biometric Data</b> <b>Biometric Record</b>	A record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an

## IT User Standards and Guidelines Manual

---

individual. For purposes of this Manual and the policies, biometrics (unless prohibited by federal or Florida law) is limited to only fingerprints or a technology that utilizes an automated touchpad to recognize a person based on finger image or template. With the latter technology, biometrics will use a point on the finger for the image and will not utilize actual fingerprints.

---

<b>Blog</b>	Blog is an abbreviated version of "weblog," which is a term used to describe web sites that maintain an ongoing chronicle of information. A blog is a frequently updated, specialized website featuring diary-type commentary and links to articles on other Web sites. Blogs range from the personal to the political, and can focus on one narrow subject or a whole range of subjects.
<b>Certificate</b>	A computer-based record which: identifies the certification authority, identifies the subscriber, contains the subscriber's public key, and is digitally signed by the certification authority.
<b>Certification Authority</b>	A person or entity who issues a certificate.
<b>Client</b>	A system entity that requests and uses the service provided by another system entity called a "server".
<b>Computer Program</b>	A set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.
<b>Computer Security</b>	measures that implement and assure security in a computer system, particularly those that assure access control; usually understood to include functions, features and technical characteristics of computer hardware and software, especially operating systems.
<b>Confidential Information</b>	Information that cannot be disclosed pursuant to Statute and is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g., the Florida Public Records Act.
<b>Confidentiality</b>	The state that exists when confidential information is held in confidence and available only to a limited set of authorized individuals pursuant to applicable law. Confidentiality is the security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads.
<b>Control</b>	Any action, device, policy, procedure, technique, or other measure that improves security.

---

## IT User Standards and Guidelines Manual

---

<b>Custodian of an Information Resource Information System Owner</b>	Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, communications, protection controls, access controls, and output distribution for the resource; a person responsible for implementing owner-defined controls and access to an information source. The custodian is normally a provider of services. Entity identified by the Superintendent/designee as having responsibility for the maintenance of the confidentiality, availability and integrity of that asset. The asset owner may change during the lifecycle of the asset. The owner does not normally or necessarily have property rights to the asset.
<b>Data</b>	A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means.
<b>Data Integrity</b>	The condition existing when the data is unchanged from its source and has not been accidentally, intentionally, or maliciously modified, altered or destroyed.
<b>Data Security</b>	The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized.
<b>Denial of Service</b>	The prevention of authorized access to a system resource or the delaying of system operations and functions.
<b>Digital Signature</b>	A type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.
<b>Domain (Active Directory)</b>	A domain contains a group of computers that can be accessed and administered with a common set of rules.
<b>Domain Name</b>	The official name of computer (host) connected to the Internet.
<b>Domain Name Service (DNS)</b>	A database system that translates a network address into a domain name.
<b>Electronic</b>	Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
<b>Electronic Agent</b>	A computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.
<b>Electronic Record</b>	A record created, generated, sent, communicated, received, or stored by electronic means.

## IT User Standards and Guidelines Manual

---

<b>Electronic Signature E-Signature Electronic Acknowledgement E-Acknowledgemen</b>	An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
<b>Emergency</b>	An emergency is defined as an imminent threat to the health, safety, or welfare of an individual.
<b>Emergency</b>	An emergency is defined as an imminent threat to the health, safety, or welfare of an individual.
<b>Encryption</b>	Cryptographic transformation of data (called “plaintext”) into a form (called “cipher-text”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption”, which is a transformation that restores encrypted data to its original state. Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: a key value that varies the transformation and, in some cases, an initialization value that establishes the starting state of the algorithm.
<b>End User User</b>	A system entity, usually an individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes. This encompasses only District employees, students, and third parties (as defined in this Manual) in a part-time or fulltime capacity.
<b>Environment</b>	The aggregate of physical, organizational, and cultural circumstances, objects, or conditions surrounding an information resource.
<b>Generic User ID</b>	A User ID shared by multiple individuals used for a specific function. An example of a generic User ID would be “third_grade_student”.
<b>Global Positioning System GPS</b>	A satellite-based radio-navigation system which allows users to determine their location anywhere in the world at any time of the day. A GPS unit receives data transmitted from GPS satellites then interprets the data to provide information on longitude, latitude and altitude.
<b>Governmental Agency</b>	An executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of this state, including a county, municipality, or other political subdivision of this state and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.
<b>GPS Tracking</b>	Monitoring the location of people and/or assets by using GPS-enabled devices.

## IT User Standards and Guidelines Manual

---

<b>Guidelines</b>	The suggested method(s) or action(s) to comply with technology policies in the absence of an applicable standard.
<b>Harmful to Minors</b>	<p>Any reproduction, imitation, characterization, description, exhibition, presentation, or representation, of whatever kind or form, depicting nudity, sexual conduct, or sexual excitement when it:</p> <p>(a) Predominantly appeals to a prurient, shameful, or morbid interest;</p> <p>(b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material or conduct for minors; and</p> <p>(c) Taken as a whole is without serious literary, artistic, political, or scientific value for minors.</p>
<b>Host</b>	A computer that acts as a server for other computers on a network. See Server.
<b>Information</b>	Data, text, images, sounds, codes, computer programs, software, databases, or other similar representations of knowledge.
<b>Information Owner Information System Owner</b>	Entity identified by the Superintendent/designee as having responsibility for the maintenance of the confidentiality, availability and integrity of that information. The information owner may change during the lifecycle of the asset. The owner does not normally or necessarily have property rights to the asset.
<b>Information Resource Information System</b>	Includes databases; archives and data files; software; hardware; communication equipment; storage media; and the associated supporting personnel, services and infrastructure, tools and utilities, manuals and documentation, plans and procedures.
<b>Information Processing System</b>	An electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.
<b>Instant Messaging</b>	Exchanging text messages or files in real time between two or more people logged into a particular instant messaging (IM) service.
<b>Integrity</b>	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

## IT User Standards and Guidelines Manual

---

<b>Key Card Smartcard</b>	Usually a plastic card with a magnetically coded strip that is scanned in order to operate a mechanism such as a door or other locking system.
<b>Key Pair</b>	A private key and its corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key creates. An "asymmetric cryptosystem" is an algorithm or series of algorithms which provide a secure key pair.
<b>Logon</b>	See User ID.
<b>Monitor or Monitoring</b>	To watch, keep track of, or check usually for a special purpose
<b>Networks or Networking</b>	Networks provide design, programming, development and operational support for local area networks ("LANs"), wide area networks ("WANs") and other networks. Networks support client/server applications, telephony support, high-speed or real-time audio and video support and may develop and/or utilize bridges, routers, gateways, and transport media.
<b>Obscene</b>	<p>The status of material which:</p> <p>(a) The average person, applying contemporary community standards, would find, taken as a whole, appeals to the prurient interest;</p> <p>(b) Depicts or describes, in a patently offensive way, sexual conduct as specifically defined herein; and</p> <p>(c) Taken as a whole lacks serious literary, artistic, political, or scientific value.</p>
<b>Password</b>	A protected word or string of characters which serves as authentication of a person's identity and may be used to grant or deny access to private or shared data.
<b>Person</b>	An individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.
<b>Personal Identifier</b>	A data item associated with a specific individual, that represents the identity of that individual and may be known by other individuals.
<b>Platform</b>	The foundation technology of a computer system. The hardware and systems software that together provide support for an application program and the services they support.
<b>Port</b>	This is a number that indicates what kind of protocol a server on the Internet is using. For example, Web servers typically are listed on port 80.

## IT User Standards and Guidelines Manual

---

<b>Private Key</b>	See Key Pair.
<b>Provider</b>	See Third Party.
<b>Proxy</b>	A network device that retrieves web pages that have been requested by District users and applies filters in accordance to School Board Policy 8.125.
<b>Private Key</b>	See Key Pair.
<b>Public Records Act</b>	Florida Statutes Chapter 119.
<b>Public Records</b>	All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. Fla. Stat. Sec. 119.011 (12).
<b>Record</b>	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form, including public records as defined in <u>s. 119.011</u> .
<b>Remote Access</b>	The ability to connect to a computer from a remote location and exchange information or remotely operate the system.
<b>Review</b>	A formal or official examination of system records and activities that may be a separate agency prerogative or a part of a security audit.
<b>Risk</b>	The likelihood or probability that a loss of information resources or breach of security will occur.
<b>Risk Management</b>	Decisions and subsequent actions designed to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.
<b>Security Audit</b>	An independent formal review and examination of system records and activities to determine the adequacy of system controls, ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any indicated changes in any of the foregoing.
<b>Security Controls</b>	Hardware, software, programs, procedures, policies, and physical safeguards that are put in place to assure the availability, integrity and protection of information and the means of processing it.
<b>Security Incident or Breach</b>	An event which results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or deliberate

## IT User Standards and Guidelines Manual

---

<b>Security Procedure</b>	A procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.
<b>Security Risk Analysis</b>	The process of identifying and documenting vulnerabilities and applicable threats to information resources.
<b>Security Standard</b>	A set of practices and rules that specify or regulate how a system or organization provides security services to protect critical system resources.
<b>Security Vulnerability Assessment</b>	An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to: identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.
<b>Separation of Duties</b>	A security principle that prevents any part of the computer system from being under the control of a single person. Every duty or transaction therefore requires multiple people to be involved, with tasks being split among them.
<b>Server</b>	A server delivers information to computers that connect to it. When users connect to a server, they can access programs, files, and other information from the server. Common servers are Web servers, mail servers, and LAN servers. A single computer can have several different server programs running on it.
<b>Session</b>	The time during which two computers maintain a connection and are usually engaged in transferring data or information.
<b>Sexting</b>	The sending, taking, or possessing of explicit, indecent, or pornographic nude or semi-nude pictures of anyone using digital devices (including phones)
<b>Spam</b>	Unsolicited Bulk E-mail (UBE) or Unsolicited Commercial E-mail (UCE).
<b>SmartcardSpoofing</b>	See KeycardForging e-mail addresses to obscure the sender's identify.
<b>Standards</b>	The uniform method(s) or action(s) to support and comply with technology policies that are required to be followed.
<b>Storage or Computer Storage</b>	The holding of data in an electromagnetic form for access by a computer processor; the process of storing information in computer memory or on a magnetic tape or disk.

## IT User Standards and Guidelines Manual

---

<b>System Control Data</b>	Data files such as programs, password files, security tables, authorization tables, etc., which, if not adequately protected, could permit unauthorized access to information resources.
<b>Technology Resources</b>	Includes databases; archives and data files; software; hardware; communication equipment; storage media; and the associated supporting personnel, services and infrastructure, tools and utilities, manuals and documentation, plans and procedures.
<b>Third Party</b>	Volunteer, contractor, vendor, governmental entity, individual or private organization transacting business with or providing or providing products, services or support to the District or other person or entity who is considered part of the School District.
<b>Transaction</b>	An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, insurance, or governmental affairs.
<b>Unauthorized disclosure</b>	A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
<b>User</b>	See End User.
<b>User ID</b>	A name that is assigned to an individual for the purpose of identification and authorization to access District technology. Typically used with a password.
<b>User Identification Code</b>	See Personal Identifier.
<b>Virtual Private Network or “VPN”</b>	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.
<b>Vulnerability</b>	A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security.
<b>Wireless</b>	Wireless includes any data communication device (e.g., personal computers, cellular phones, PDAs, laptops, etc.) that is connected to any network. This includes any form of Wireless communications device capable of transmitting packet data.
<b>Wireless Access Point (AP)</b>	The hub of a wireless network; the central transmitter and receiver, with antennas, attached to a wired network.

## 3. GENERAL SECURITY STANDARDS

The General Security Standards create a base framework that assures the most effective protection of the District's information resources and users.

### 3.1. *District Responsibilities*

#### 3.1.1. Security Objectives

Information Technology (IT) Security's responsibility to establish the following security objectives:

- **Integrity** – IT Security should ensure that all electronic information and transactions are free of errors and irregularities of any kind.
- **Availability** – IT Security should ensure that all information resources and data are available and protected from disruptions.
- **Confidentiality** – IT Security should ensure that all information resources are protected from unauthorized use or accidental disclosures, errors, fraud, sabotage, privacy infringement, and other actions that may cause harm.



The District employs various measures to protect its network and information resources and its users; however, the District cannot guarantee that security incidents will not happen. The District accepts no responsibility for harm caused directly or indirectly by the use of its network and information resources.

District's technology resources shall be auditable. IT shall audit the use of technology using available logging and monitoring facilities to ensure these security objectives are met.

### 3.2. *User Responsibilities*

Every information resource user must comply with all information security related policies, standards and procedures, including:

- Users must utilize the District's information resources and technology only for purposes specifically approved by the owner of the information resource or technology.
- Users must not interfere with the normal and proper operation of the District's information resources. User actions that would adversely affect the ability of other users to use the resources are not permitted. User actions that would reasonably be considered harmful or offensive to other users are not permitted.
- Users must not circumvent District security systems, including firewalls, filters and proxies.

## IT User Standards and Guidelines Manual

---

- Users must not attempt to expose information security vulnerabilities or compromise a District information resource without prior consent of the Department of Information Technology Governance.
- Users must report all incidents, where they believe an information security vulnerability or violation may exist, to the Department of Information Technology Governance.
- Any user failing to comply with any information security policy, procedure or standard may be subject to disciplinary action and civil or criminal liability. IT has the authority to take reasonably necessary immediate actions to protect District technology resources.
- The willful and knowing unauthorized use, modification, alteration, dissemination, or destruction of District information resources or technology is considered a violation of this Policy and the District may impose consequences. As to employees, these consequences may include discipline, up to and including termination. The Supervisor, through District procedures, may request reimbursement to the District from the employee. If the employee does not make payment, the School Board may institute a civil action for damages to hold the employee liable. Moreover, this conduct may constitute a computer-related crime punishable under Chapter 815, Florida Statutes.

### ***3.3. Limited Expectation of Privacy***

There is only a limited expectation of privacy to the extent required by law related to use of the District's technology resources. Except as stated below relating to a school's ability to monitor student use, only IT Security and/or School Police may monitor District information resources. IT's and School Police's monitoring must be for lawful and good cause purposes, including, but not limited to:

- Ensuring that their use is authorized;
- For management of the system;
- To respond to a records request;
- To facilitate protection against unauthorized access;
- Verifying security procedures, survivability and operational security;
- Compliance with School Board policies;
- A possible security incident; or
- Computer performance.

An employee's supervisor may request monitoring that employee's use of District resources but only when there is reasonable suspicion of misuse, to obtain information needed for the District's mission, or to respond to a

records request. Monitoring includes active attacks by authorized District entities to test or verify the security of the District's information resources. A teacher may monitor a student's use of District resources.

During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this resource may be monitored.

Use of District information resources and technology, authorized or unauthorized, constitutes consent to monitoring of this resource and/or technology. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. IT will monitor District computers and emails and employees shall be notified of this practice.

Employees, students and third parties are advised that many District technology resources, including but not limited to laptops and desktops, may contain input systems such as web cameras and microphones which can be remotely controlled to turn them on and off. The District will not utilize any such input systems remotely unless it is consistent with law.

This Section is not intended to prohibit or impede a school's ability to monitor student use of District technology to ensure proper usage.

### ***3.4. Biometric Record Standards***

It is the responsibility of all users that have access to biometric data to hold this information in confidence at all times. Biometric information should be disclosed only for a required business purpose. The School District shall design adequate processes and procedural standards to protect biometric information held and/or used in accordance with this Manual. Such standards, requirements and responsibilities shall include, but not be limited to, the following:

The Superintendent/designee shall determine the users who have authorization to access biometric information based on District needs. The must:

- i. Keep secure and confidential all biometric information.
- ii. Maintain biometric information in a "secure" environment limited to only designated users.
- iii. Restrict access to biometric data and processing to appropriate and authorized users.

- iv. Ensure that all biometric data is protected against fraud, unauthorized use or other compromise.
- v. Restrict access to biometric information to the minimum number of people possible, including only to the appropriate personnel. These persons are defined as needing access in order to perform their day to day responsibilities.
- vi. Not release biometric information in any form unless there is a legitimate business purpose as provided herein or if required by law.

The District will be responsible for maintaining biometric data pursuant to the District's records retention schedule.

The Superintendent, or designee, is further authorized to impose further standards, requirements and responsibilities in administrative procedures and guidelines established to implement these standards.

An Employee's failure to comply with this Policy or the associated, required administrative procedures will be deemed a violation of this standard and subject the employee to personnel action up to and including termination. Other users who violate this standard are subject to consequences for the District, including terminating access to this information.

### ***3.5 Encryption Standards***

Activities storing or transmitting confidential or exempt information shall require encryption processes approved by IT to ensure that the information remains confidential. Individual users must use IT approved encryption products and processes for sending an encrypted e-mail, encrypting a desktop work file, protecting a personal private key or digital certificate, or encrypting a saved e-mail.

- Encryption keys should not be stored on the same electronic storage device as the information that has been encrypted using the keys. Access to encryption keys should be restricted to authorized users and authorized processes using an access control mechanism.
- Remote administration of hardware, software, or applications should be performed over an encrypted communications session.

### ***3.6 E-Signatures***

The Superintendent/designee has the authority to determine that online or e-record forms or documents are to be utilized to meet the best interests of the District. In those instances and when the e-record is available and the employee has the authority as approved by the Board or in accordance with Board Policy, the employee shall execute these documents by means of an e-signature. If the

## IT User Standards and Guidelines Manual

---

person is acting on behalf of the District and has the authority to enter into an agreement, the person can bind the District with an e-signature following this procedure.

As to third parties and parents of a student, when the online or e-record is available and the Superintendent/designee has authorized its use, the School Board will accept an e-signature from that parent or a person authorized on behalf of the third party to execute the document by an e-signature. If the person is acting on behalf of a third party and has the authority to enter into an agreement, the person binds that party with an e-signature following this procedure. Parents will also bind themselves with an e-signature following this procedure.

The employee/third party/parent thereby agrees that for these transactions he/she intends to be and will be legally bound by his/her e-signature on these documents. The transaction shall be conducted through the employee/third party's/ parent's District account or the third party's or parent's account with another entity approved by the District that can attribute the signature to that person through the security and password procedures stated within this Manual and other IT security policies.

The employee/third party/parent must be afforded an opportunity to retain or access a copy of the electronic record.

To the extent the Superintendent/designee has determined that students may complete e-record forms or documents, students may execute those documents, if they are available, by e-acknowledgement. The student thereby agrees that for these transactions, he/she intends to be and will be bound by his/her e-acknowledgement on these documents. The transaction shall be conducted through the student's District account that can attribute the acknowledgement to that student through the security and password procedures stated within this Manual, School Board Policy 8.123, and other IT security policies.

If a law, State rule, or School Board policy requires a signature or record to be notarized, acknowledged, verified, or made under oath, the notarization requirement is satisfied if the conditions within Fla. Stat. §§ 668.50 (11) or 117.021 and any other applicable Statute, rule, or regulation are met.

**4 ACCEPTABLE USE STANDARDS**

The objective of the Acceptable Use Standards is to outline the acceptable use of technology that is used in the District. These standards are in place to protect the District’s information resources and technology and the users that must use these resources. Inappropriate use exposes the resources and users to risks including virus attacks, identity theft, denial of services, loss of data, and misuse of resources and information.

The District’s information resources and technology must be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of The School District of Palm Beach County. Users must acknowledge their understanding of all applicable policies and standards as a condition of receiving an account to use the District’s information resources and technology, and that the user will be responsible for his/her actions when using these resources.

The use of District information resources and technology for any activity that violates, or constitutes an attempt to violate, any local, state, federal or international law, order, rule or regulation, or to engage in tortious conduct, is strictly prohibited.

**4.1 Applicable Policies and Standards**

Students, employees and third parties shall find their applicable information security policies and standards in the table below:

**Table 1: Applicable Policies and Standards for Users.**

User	Applicable Policies and Standards
All Users	<p><b>School Board Policy 8.125</b> – District Review and Filtering of Web Sites.  <b>School Board Policy 2.501</b>—Information Security –Access Control Policy  <b>School Board Form PBSB 1664</b> — Website Review.  <b>Information Technology (IT) User Standards and Guidelines Manual</b> (this document).  <b>Public Records Rules:</b> The Florida Statutes in Chapter 119 defines public records as: “all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or <b>other material, regardless of the physical form, characteristics, or means of transmission</b>, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.”</p> <p>Emails and voice recordings have been determined to be subject to the Public Records Law. Treat instant messages, text messages, and tweets as public records. Public records are subject to inspection by the public unless a statutory exemption exists.  Public records must be retained pursuant to the District’s retention schedule located at:  <a href="http://www.palmbeachschools.org/records/documents/RecordsRetentionScheduleAugust012010.pdf">http://www.palmbeachschools.org/records/documents/RecordsRetentionScheduleAugust012010.pdf</a> and any records holds.</p>

## IT User Standards and Guidelines Manual

---

User	Applicable Policies and Standards
	<p>A <b>student's educational records</b> are confidential and exempt from public records disclosure under 20 U.S.C. 1232g ("FERPA"), and 34 C.F.R. Part 99, and Florida Statutes Sections 1002.22 and 1002.221. Subject to that confidentiality, any information generated through a computer, stored on hard disks, electronically mailed, or handled as e-mail, if it meets the definition of a public record, is subject to the District's retention schedule and Florida law concerning public records, as explained in School Board Policy 2.041.</p>
<b>Students</b>	<p><b>School Board Policy 8.123</b> – Technology Acceptable Use Policy for Students.</p> <p>Students shall not use any District technology resource for private business, personal use or gain and student use must be related to the curriculum, the academic development of the student, or a school extracurricular activity, as defined in Fla. Stat. § 1006.15(2) and as provided within School Board Policy 5.60. Student use of wireless devices and cellular phones is also governed by School Board Policy 5.183.</p>
<b>Employees</b>	<p><b>School Board Policy 3.29</b> – Employee Use of Technology.</p> <p>The District authorizes employees to use District technology resources, including its information and data systems for assigned responsibilities, when allowed by an appropriate District representative. Employees shall use these resources to enhance job productivity in performance of District business. Access to data files and programs shall be limited to those individuals authorized to view, process, or maintain particular systems. Confidential or exempt information shall be accessible only to personnel who are authorized by the District on the basis of the performance of responsibilities or as authorized by law.</p> <p>Employees shall not conduct a private enterprise using District technology resources.</p> <p>Except as stated within section (7) of School Board Policy 3.29, employees shall not use District technology resources, including, but not limited to computers, networks, copiers, and communication devices such as cell and office phones, personal digital assistants (PDAs) and facsimile machines, for a private business or for the benefit of private, "for profit," or "not for profit" organizations unless the use of the technology will benefit the District or, as to "not for profit" organizations, if the organization benefits the children, schools or community and is not for religious or political purposes.</p> <p>An employee may utilize District technology resources outside of the employee's paid duty hours to use the Internet for the employee's personal and professional growth provided no additional costs are incurred to the District, the District's Internet and network resources are not negatively impacted, and firewall and network configurations are not altered to allow different services that are not usually allowed during the employee's paid duty hours allowed during the employee's paid duty hours. This provision is not intended to restrict or limit an employee's ability to utilize District technology during the employee's paid duty hours for professional development when the professional development is related to the employee's responsibilities for the District, certification, or license, such as District or professional organization training vodcasts, power points, or breeze presentations related to one's duties. Employees are encouraged to use these facilities for personal and professional growth, which must not be confused with</p>

# IT User Standards and Guidelines Manual

---

User	Applicable Policies and Standards
	financial gain, and engaging in activities for financial gain is prohibited. Creation by an employee of any District blogs and/or social networking sites must be authorized by the Superintendent/designee and be for a public, purpose. The use of the blog must be compliant with District policies, including but not limited to those involving public records retention, student privacy, and copyright laws.
<b>Third Parties</b>	<b>School Board Policy 2.50 – Third Party Acceptable Use of Technology.</b> See provisions within Policy.

## ***4.2 E-mail<sup>1</sup> and Calendaring System Acceptable Use***

Acceptable uses of the District's e-mail and calendaring system are activities that support the employee's job assignment within the standards and policies of the District, the Florida Department of Education, and the laws of the State of Florida. Users are encouraged to make full use of the E-mail and Calendaring System in the pursuit of their District jobs and assignments, provided such use complies with School Board Policy 3.29 "Employee Use of Technology".

Unacceptable uses of the District's e-mail and calendaring system include:

- Violating the conditions of the Florida State Board of Education's Administrative Rules dealing with students' rights to privacy (SB6A-1.0955).
- Using profanity, obscenity or other language that may be offensive to another user.
- Using the system illegally, including sexting.
- Copying commercial software or other copyright protected material in violation of copyright law.
- Using these electronic services for financial gain or for any commercial or illegal activity.
- Time-wasting activities that do not adhere to the District's mission.

## ***4.3 Software and Hardware Acceptable Use***

No purchase or use of software or hardware on District computers/systems shall occur unless it is authorized by the District as follows. This includes public domain software downloaded from the Internet. Users shall utilize only hardware and licensed software that has been approved by the Superintendent/designee after submission of a completed PBSO 2199 to the Technology Clearinghouse Committee (TCC). Software and hardware installed prior to July 1, 2009 are grandfathered in, but if they are upgraded or replaced, they are subject to Superintendent/designee approval following submission to TCC.

Users must strictly adhere to software license agreements and copyright holders' notices.

Users are forbidden from making unauthorized copies of software.

---

<sup>1</sup> **Note: these standards also apply to text messaging, instant messaging and other forms of electronic messaging.**

### ***4.4 Examples of Unacceptable Uses of Technology***

- The purchase of technology for use within the District that has not been approved by the Technology Clearinghouse Committee.
- Posting or otherwise transmitting any content that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, pornographic, libelous, invasive of another's privacy, harmful to minors, hateful, of malicious intent, or racially, ethnically or otherwise objectionable.
- Impersonating any person or entity, or falsely stating or otherwise misrepresenting your affiliation with a person or entity.
- Reposting clearly personal communications without the author's prior consent, absent a student/public records request.
- Forging /spoofing e-mail addresses or otherwise manipulating network identifiers in order to disguise the origin of any content transmitted through the network.
- Intentionally transmitting any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- Transmitting any unsolicited or unauthorized advertising, promotional materials, "junk mail," "bulk mail", "spam," "chain letters," "pyramid schemes," or any other form of solicitation.
- Attempting to access any domain, network, service, port, system, host, computer, or device without the specific prior permission, authorization, or approval of the controlling entity or to impair or damage the operations of computers, networks, terminals or peripherals devices.
- Copying or otherwise transmitting any content in violation of patent, trademark, trade secret, copyright law, confidentiality laws or agreements, court orders, or other protected material.
- Using the network for personal financial gain or for any unauthorized commercial or illegal activity. This includes, but is not limited to: offering for sale any products or services and soliciting for advertisers or sponsors.

### 5 WORLD-WIDE WEB STANDARDS AND GUIDELINES

There are vast amounts of information available on the internet and worldwide web. The District has a website for teachers, students, parents and the community that helps find appropriate educational information on the web. The site, Learning Village, <http://lv.palmbeach.k12.fl.us>, is maintained by the District's Department of Educational Technology.

#### ***5.1 Safe Surfing Guidelines***

The Internet, and the anonymity it affords, can give online scammers, hackers, and identity thieves' access to your computer, personal information, finances, and much more. Users must be aware of these threats and follow the following steps to be safer and more secure online.

##### **5.1.1 Protect Your Personal Information**

Users should not share their personal information unless they know how it will be used and protected. Users should not reply to or click on any links in any e-mails asking for personal information.

##### **5.1.2 Know Who You Are Dealing With**

Users shall not download files from untrustworthy web sites. Many downloaded files come with spy ware that can compromise the security of your computer.

##### **5.1.3 Use Anti-Virus and Anti-Spy ware Software and a Firewall**

Users shall not disable or turn off District anti-virus or anti-spy ware software. Users shall not circumvent the rules of District firewalls or filter set forth in Policy 8.125 to access sites that would otherwise be blocked.

##### **5.1.4 Setup Your Software Properly and Update Them Regularly**

District computers accessing the Internet shall have the most current system software image available from IT.

##### **5.1.5 Protect Your Passwords**

Don't share your passwords with anyone. Keep your passwords in a secure place, and out of plain view.

##### **5.1.6 Back Up Important Files**

No system is completely fail proof. Important files stored on your computer should be backed-up and stored in a secure location.

### **5.1.7 Contact IT Security If Something Goes Wrong Online**

Contact IT Security to report any security incidents that have occurred. IT Security will respond appropriately to stop any attacks and prevent them from reoccurring.

### 6 E-MAIL AND OTHER ELECTRONIC COMMUNICATION STANDARDS AND GUIDELINES <sup>2</sup>

All employees receive the E-mail and Calendaring Service with their Employee User ID account. Employees are expected to use the District's e-mail and calendaring service only for activities appropriate to the business and educational objectives of the District. Employee's usage and communications should reflect well on the employee and on the District. E-mail may not be used to endorse a political candidate or distribute a political candidate's campaign information. District technology may be used in relation to "Calls for Action" pursuant to School Board Policy 2.591 as allowed by the Superintendent or designee.

For more information about Employee User IDs and e-mail accounts, visit the IT Security web site at <http://www.palmbeachschools.org/it/security.asp>.

Some third parties are also provided this service when the District has determined that these services are in the best interests of the District.

Students may be provided or have access to electronic mail if authorized by the Superintendent/designee for educational or learning purposes.

The Division of Information Technology shall provide spam and virus protection services for the District's e-mail and calendaring system.

#### 6.1 *Spam*

Despite all of the precautions taken to block spam, some spam does make it through to the District's e-mail system. In order for IT Security to block spam messages, the message must be forwarded to [abuse@palmbeach.k12.fl.us](mailto:abuse@palmbeach.k12.fl.us) as an attachment. This preserves the information that is needed to report the spammer so that future posts may be blocked. Detailed instructions are available at <http://www.palmbeachschools.org/it/security.asp>.

#### 6.2 *User Responsibilities*

The e-mail account owner is responsible at all times for proper usage. Users should be aware of Florida public record laws and recognize that their e-mail messages may be considered a public record.

##### 6.2.1 **Public Records Law Adherence**

If E-mail messages, are created or received in the transaction of official School District business, they would be considered public records, open to public inspection according to provisions in Chapter 119, Florida Statutes. Depending on the content and topic of a particular message, it may or may not be exempt from public inspection under Florida's Public Records Law.

---

<sup>2</sup> **Note: Where applicable, these standards govern not only to emails but also text messaging, instant messaging and other forms of electronic messaging.**

To the extent the District has not archived one's E-mails, or if one's E-mail is subject to long term retention, each user is individually responsible for maintaining the public accessibility of his/her own incoming and outgoing E-mail messages that are official records as required by the Public Records Law. Questions relating to whether or not the content of a particular E-mail message constitutes a public record should be directed to the District's Public Affairs Office.

- a. Persons are allowed to communicate by e-mails through services provided by the District but are prohibited from engaging in text messaging, instant messaging, tweeting and other methods of instant electronic communication if the messages must be retained as public records in accordance with the District's Retention.
- b. Treat instant messages, text messages, tweets, and other instantaneous messages as public records. Public records are subject to inspection by the public unless a statutory exemption exists.
  - c. Public records must be retained pursuant to the District's Retention Schedule located at: <http://www.palmbeachschools.org/records/RecordsRetention.asp> and any records holds.  
See Section 6.2.2 below.

### **6.2.2 Standards for Retention of E-mail and Other Electronic Messages**

If, according to State mandated records retention schedule, the content of an e-mail message possesses long term business value and is an official record, to the extent the District has not archived one's e-mails, or if one's E-mails are subject to long term retention, employees are required to retain the message and either immediately or eventually move and archive the e-mail message to a personal folder on the computer's hard drive or print the message and place it in the proper paper file for further retention.

Four record categories are described below to assist users in determining the retention requirement of E-mail and other electronic messages. It is important to note that many e-mail or other electronic messages typically fall under the categories of non-record materials, notices with no business value, or transitory messages and therefore should be deleted by both the sender and receiver immediately after the administrative value is lost. For these messages, users are encouraged to delete messages on a daily basis, immediately after reading, replying, or taking other action concerning a particular message.

Yet, if a records hold exists, e-mails and other electronic communications relating to those issues must be retained irrespective of the retention schedule until the records hold is released. Records holds are requests to retain all documents until further notice when

potential or pending litigation exists, when an audit is being conducted, or when an investigation is occurring.

Further, if the employee is aware of pending or potential litigation and no records hold request has yet been made, the employee or his/her supervisor must notify the Office of Chief Counsel. The e-mails relating to those issues must be retained irrespective of the retention schedule until advised by the Office of Chief Counsel or per the District's retention schedule, whichever period of time is longer. Additionally, if the employee is aware of an audit or pending investigation and no records hold request has yet been made, the emails must be retained until the audit or investigation have been completed or per the District's retention schedule, whichever period of time is longer.

Absent a records hold or the employee is aware of pending or potential litigation, audit or investigation, the following retention principles apply:

### **6.2.2.1 Non-Record Materials**

Delete at will.

The following examples are materials (not records) that may not be appropriate for E-mail and may be deleted at any time:

- Lost jewelry/keys notice.
- Birth/death/funeral announcements.
- Party announcements (baby shower, wedding shower, retirement, etc.).
- Any e-mail not received or created in the course of District business.

### **6.2.2.2 Notices with No Business Value**

Delete at will.

This category includes information with no business value after receipt and review. Examples include internal office announcements such as:

- "Joe Smith called, please call back"
- "Is this afternoon's meeting still on?"
- "Tomorrow's staff meeting location has been changed to room #202."

### **6.2.2.3 Transitory Messages**

Delete after administrative value is lost.

The Florida Department of State, Division of Library and Information Services' most recent publication of the General Records Schedule for Local Government Agencies (GS1-L) [PDF file] includes a record series category that may cover a large percentage of typical E-mail messages. The category title is "Transitory Messages", which has the following definition:

"This records series consists of those records that are created primarily for the communication of information, as opposed to

communications designed for the perpetuation of knowledge. Transitory messages do not set policy, establish guidelines or procedures certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to the communication that might take place during a telephone conversation or a conversation in an office hallway. Transitory messages would include, but would not be limited to: E-mail messages with short-lived or no administrative value, voice mail, self-sticking notes, and telephone messages."

The retention requirement for all transitory messages is "retain until obsolete, superseded or administrative value is lost."

### 6.2.2.4 Official Records

Retain as required.

**E-mail messages that pertain to a particular District business transaction, project/case file, board action, or student/personnel issue must be retained as long as all other documentation that pertains to the same transaction/project/case/action/issue.**

The Palm Beach County School District Records Retention Schedule,

<http://www.palmbeachschools.org/records/documents/RecordsRetentionScheduleAugust012010.pdf> must be referenced to determine the specific retention requirement for E-mail messages that fall under this category. Questions relating to which record series are applicable for a particular E-mail message should be directed to the Records Management section of Information Technology.

## 6.3 *E-mail and Calendaring Privacy*

All E-mail messages sent and received by the District's e-mail and calendaring system are the property of the District. Never consider electronic communications to be private. Email users have only a limited expectation of privacy to the extent required by law (see section 3.3, above). Treat electronic communications the same as written hard copy communications with regard to propriety and openness. The District reserves the right to review all electronic correspondence that uses District systems and facilities.

## 6.4 *Shared Accounts*

Except as to certain students as allowed by School Board Policy 8.123, there will be no shared accounts; all accounts will be used by a single individual. E-mail distribution lists should be used when the same information is to be distributed to several users.

### **6.5 E-mail Distribution Lists**

Distribution lists are a very useful tool when sending the same message to a group of users.

There are two types of distribution lists:

- 1) Generic distribution lists created by IT (i.e., All Principals, All Data Processors, All High Schools, etc.); and
- 2) User created distribution lists.

The following rules shall be adhered to when using distribution lists:

- Maintenance and update of end user created distribution lists is the responsibility of the user that created the list;
- Think carefully before using a large distribution list. The employee should consider, "Do all E-mail users on this distribution list really need to know this information?"

### **6.5. Accessing another User's E-mail**

Where appropriate, users may delegate access to their e-mail and calendar to other secondary/delegated users. This should only be done in situations where the delegated user might also handle the primary user's paper mail. In all cases, this should be done by means of the e-mail and calendaring system's delegation facilities, not by giving the delegate access the primary user's user ID and password.

### **6.6. Backup and Restoration of E-mail Messages**

For disaster recovery purposes, Information Technology will backup E-mail for offsite security storage. These backups are not designed to meet records retention requirements. See "Guidelines for Retention of E-mail Messages" for information on user responsibilities and compliance to E-mail retention requirements.

Restoration of E-mail messages may be possible through Information Technology depending upon the age of the e-mail and the District's archival system.

When the District migrates to Google email, Google archiving will capture and store all email based on pretermind configurations.

### **6.7. E-mail Guidelines**

#### **6.7.1. Suggestions for Effective Use**

The following suggestions will increase the effectiveness of E-mail:

- Make subject headings as descriptive as possible.
- Restate the question or issue being addressed in a response unless the text of the original message(s) is included in the current message.
- Include the most important fact/idea/issue first or very near the top of the message.

- Avoid misunderstandings by keeping in mind that electronic text is devoid of any context clues that convey shades of irony, sarcasm, or harmless humor.
- Proofread/edit each message and use the system's spell check prior to sending a message.
- Check the facts in your message before sending it; do not spread rumors via E-mail.
- Acknowledge requests for read receipts.

### **6.7.2. Capacity and Conservation of Resources**

Users must be aware of the finite capacity of the e-mail and calendaring system and must cooperate with Information Technology to conserve resources. The storage of documents and other items uses system resources that are finite and limited; failure to use these resources wisely could result in system outages and thus deprive others from getting their work done.

Users should:

- Open their E-mail on a regular basis (at least daily, if possible), delete unneeded items, and file items needed for future reference appropriately so as not to fill up their incoming mail file (in-basket). Failure to do so will result in that user ID being deleted from the system along with all associated files and records including all unopened E-mail. If the employee is absent and another employee has access to that employee's email (such as an assistant, although the employee's password shall not be shared), ask the assistant to scan the e-mails to acknowledge or respond to time-sensitive matters
- Delete unneeded items from their mail logs on a regular basis and keep mail logs organized so that they can be easily maintained.
- Send E-mail to concerned parties only.
- Use the E-mail system's delegation or forwarding facilities (whichever is available and/or appropriate, such as the office assistant feature) whenever they are out for extended periods of time. Passwords are never to be shared with anyone.
- Review intended recipients appearing on e-mail before sending to make sure persons with similar names and/or unintended addressees are not listed.

## **6.9 User Account Termination**

All user accounts will be disabled immediately upon a user's termination of employment with the District.

The employee's supervisor is responsible for:

- Notifying Information Technology of the user's termination of relationship; and

## IT User Standards and Guidelines Manual

---

- Requesting access to the former employee's stored E-mail to review for required retention of any official record material.

Upon the termination of any user's employment with the District, the user shall no longer attempt to access the system.

## 7. NETWORK USE STANDARDS AND GUIDELINES

The District's data network is the backbone of its information resources. The countywide network includes almost 200 remote locations with 120,000 nodes interconnected with high speed IP network links. The network connects schools with educational resources available throughout the world. Network Use Standards ensure only authorized and authenticated users can access the District's network resources, and that the resources are available and safe to use.

Wireless networks are provided at many locations and users should follow these standards when connecting to one of the wireless networks.

### 7.1. *Network Authentication*

Except for certain students as allowed by School Board Policy 8.123:

- All users must be positively identified, by using a UserID and password, prior to being able to use any network or information resource.
- Users are prohibited from using a UserID that is assigned to another user.
- Users are prohibited from using an anonymous or guest UserID, although generic accounts may be allowed with the permission of IT-
- Users must-logoff or lock their computer when leaving it unattended for any period of time.

### 7.2. *Network Inactivity*

In order to reduce the potential for unauthorized access to information, all network devices, including user computers, should invoke inactivity timeouts that will lock the device after no longer than thirty minutes of inactivity. The user will be required to re-authenticate to regain access to the device.

### 7.3. *Approved Network Devices.*



All devices that are connected internally to a SDPBC network must be approved by the District's Chief Information Officer Director of IT Infrastructure, or designee. These devices include, but are not limited to, servers, workstations, modems, wireless access points, routers, switches or hubs. Any unauthorized devices will be immediately disconnected from the District network. These restrictions do not apply to authorized Web access from external locations or equipment if allowed by law. This procedure does not prohibit or restrict public access to inspect data and information on publiclypublicly available District technology resources.

## IT User Standards and Guidelines Manual

---

All networked computers *must* join the District's Active Directory domain - ADMIN.

All devices must have:

- All available software and operating system updates, patches and hot fixes installed.
- District approved anti-virus software installed and operational with current virus signatures.

### 8. PASSWORD STANDARDS AND GUIDELINES

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the District's entire information network. As such, except for certain students as allowed by School Board Policy 8.123:

- a. All District information resource and technology users (including contractors, vendors and volunteers) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
- b. These users of District information resources shall be assigned by IT a unique personal identifier or user identification.
- c. User identification shall be authenticated with the user's password before access is granted.

#### 8.1. *Password Expiration*

The Superintendent or designee will set password expiration limits based on the user's roles and responsibilities relating to the extent of access of the user and the security risk.

Students must change their passwords at least once every 120 days. Other users must change their passwords at least once every 90 days except for technical system administrators whose passwords must be changed at least once every 30 days.

#### 8.2. *Password Confidentiality*

Except for certain students as allowed by School Board Policy 8.123:

Passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user's responsibility for actions that the other party takes with the password.

If someone demands the user's password, the user must refer that person to this document and/or call IT Security. It is considered a violation of School Board policy, as expressed within this Manual, for a person to demand the password of another person.



Users are responsible for all activity performed with their user accounts. User accounts shall not be utilized by anyone but the individuals to whom they have been issued. Users shall not allow their user accounts to be used by others.

Users are forbidden from performing any activity with user accounts belonging to other users.

#### 8.3. *Compromised Passwords*

All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

### 8.4. *Enforcement*

IT enforces all password rules set forth by this policy within the scope of their capability, and conducts periodic compliance audits.

IT Security or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

### 8.5. *Password Construction Guidelines*

Passwords are used for various purposes at the District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Except for certain students as allowed by School Board Policy 8.123, all users must be aware of how to select strong passwords.

#### 8.5.1. **Password Length**

All passwords must be eight (8) or more characters in length. The user must use the maximum password length allowed on systems that do not support password lengths of at least eight (8) characters.

#### 8.5.2. **Composition**

All passwords must contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and special characters ( , @\$% ^&\*+\_).

Passwords should be difficult to guess. Words in a dictionary, derivatives of a userID, and common character sequences such as "123456" must not be used. Personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. Proper names, geographical locations, common acronyms, and slang must not be used.

Users should not construct passwords by combining a set of characters that do not change, with a set of characters that predictably change. Characters that change are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not use passwords like "X34JAN" in January, "X34FEB" in February, etc.

#### 8.5.3. **Password Examples**

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.

## IT User Standards and Guidelines Manual

---

- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#\$%^&\*()\_+|~-=\`{}[]:;'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

**NOTE: Do not use any of these examples as passwords!**

### 9. WIRELESS NETWORK STANDARDS AND GUIDELINES

The objective of these standards is to prohibit unauthorized access to the District information resources via unsecured wireless communication methods. This standard covers all wireless data communication devices wired to the District's network.

A non-secure public wireless network is provided for visitors at school and administrative locations to access District information resources and technology without having to logon to the network and/or domain. Public wireless access is very limited and should not be used for accessing non-public information resources.

#### 9.1. *Approved Wireless Access Points*

All wireless access points (AP) that are to be used to access District information resources, including the Internet, must be approved, managed and configured by IT based on IT's current technology standards. Use of unapproved access points, known as rogue APs, is not allowed. Any unapproved access points that are discovered to be connected to the District network will be disconnected or otherwise rendered unusable by IT.

#### 9.2. *Authenticated Access*

All non-public wireless systems must support and utilize strong user authentication.

#### 9.3. *Encryption*

All non-public wireless data communication must be encrypted with secure protocols such as WEP or any future protocol that may offer stronger encryption.

#### 9.4. *Network Monitoring*

IT should utilize operational support tools to monitor continually the District airspace for rouge APs and other security vulnerabilities.

#### **NOTICE OF CONDITIONS FOR STUDENT USE OF DISTRICT TECHNOLOGY**

The following notice must be read by, or read and/or explained to, the student. Also it is available to be read by, or explained to, the student's parent(s) or legal guardian(s) (unless the student is emancipated). The student registration form, PBSB 0636, which is required to be reviewed, completed and signed by the parent/legal guardian/emancipated student annually, will contain language providing them notice of Policy 8.123 and that the students must abide by its terms.

Student access to District technology resources, including access to the Internet, is to support the District's educational responsibilities and mission. The specific conditions and services being offered will change from time to time. In addition, the District makes no warranties with respect to network or Internet service, and it specifically assumes no responsibilities for:

1. The content of any source on the Internet, or any costs, liability, or damages caused by the way the student chooses to use his/her network or Internet access.
2. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District.

The student agrees to the following terms:

1. The student's use of the District's technology resources must be consistent with the primary goals of the District, IT, and the school site.
2. The student will not use any District technology resources for illegal purposes of any kind.
3. The student understands that misuse of District technology resources may occur in many forms, including the issues described in this document and School Board Policy 8.123 and its referenced Manual.
4. The student will not use District technology resources to transmit materials that are harmful to minors, threatening, obscene, or harassing. The District will not be held responsible if the student participates in such activities or for any such behavior on the student's part.
5. The student will not use District technology resources to interfere with or disrupt network users, services, or equipment through the distribution of unsolicited advertising, propagation of computer viruses, using printers other than those designated at the student's school site for student use, and/or using the network to make unauthorized entry to any other machine accessible via the network or by any other means.
6. The student will not use District technology resources and information unless permission to do so has been granted by the owners or holders of the rights to those resources or information. It is assumed that information and resources accessible via District technology resources are private to the individuals and organizations which own or hold the rights to those resources and information unless specifically stated otherwise by the owners or holders of the rights.
7. The student has read or been informed of the provisions of School Board Policy 8.123 and its Manual and understands that the student is responsible for abiding by the provisions within *this policy relating to Student Use of Technology* at [http://www.palmbeachschools.org/policies/8\\_123.htm](http://www.palmbeachschools.org/policies/8_123.htm) and the IT User Standards and Guidelines Manual at <http://www.palmbeachschools.org/it/security.asp>.
8. The student acknowledges that only a limited expectation of privacy exists to the extent required by law for him/her as a student related to his/her use of District technology resources. District technology resources may be monitored for all lawful and good cause purposes. Use of these resources constitutes consent for the District to monitor these resources for these purposes. The student further acknowledges that the District may retrieve and/or disclose, as allowed by law, all messages stored by the District or an outside entity on its behalf.
9. The student's District computer account, if the student is authorized to do so, may be used by the student to electronically acknowledge District documents. The student's account may also be used to access and update the student's personal information in District information systems.

## IT User Standards and Guidelines Manual

---

10. The student acknowledges his/her intent to be bound by documents he/she acknowledges electronically by the method described above in paragraph 9 to the same extent the student would be bound if signing a hard-copy of the document.
11. All passwords assigned to the student will be kept confidential and the student will not disclose them to any third-parties.

The District makes no warranties of any kind, whether express or implied, for the services provided and will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the District's negligence or by user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through District network or Internet services. All users need to consider the source of any information they obtain and consider how valid that information may be.

In accordance with the Electronic and Communications Privacy Act of 1986, (18 USC Section 2510), all students are hereby notified that there are no facilities provided for sending or receiving private or confidential electronic communications. All messages may be considered readily accessible to the general public. Do not use this system for any communications which the sender intends only for the sender and intended recipients to read. By the student's use of the District network or Internet, the student agrees to hold harmless the District against any and all claims arising out of said use.

The student and his/her parent(s) or legal guardian(s) (the student alone if emancipated) are bound to the terms and conditions of this Notice. The student has discussed these rights and responsibilities with his/her parent(s) or legal guardian(s).

The student understands that any violations of the above provisions may result in disciplinary action, the revocation of the student's access privileges, and/or privileges, and/or appropriate legal action. The student also agrees to report any misuse of the information resources to the school site administrator, teacher, or technology representative. All the rules of conduct described in District or school site policies, procedures, and handbooks apply when the student is on the network.

*The parent or guardian of this student has been provided an opportunity to read this Notice and School Board Policy 8.123 and its referenced Manual. The parent or guardian understands the provisions and conditions of this document and the Policy and Manual and that Internet access via the District network is being provided solely for educational purposes related to the curriculum, the academic development of the student, or a school extracurricular activity. The parent or guardian understands that his/her child will abide by the provisions and conditions of this Notice and the parent or guardian understands that any violations of the above provisions may result in disciplinary action, the revocation of his/her child's access privileges, and/or privileges, and/or appropriate legal action. All the rules of conduct described in District or school site policies, procedures, and handbooks apply when his/her child is on the network.*

The parent or guardian further understands that it is impossible for the District to restrict access to all controversial materials, and the parent or guardian will not hold the District responsible for materials acquired on the District network or Internet. The parent or guardian also will report any misuse of any information resources or technology to the school site administrator, teacher, or technology representative. The parent or guardian accepts full responsibility for the supervision of his/her child should he/she use remote connections to the District network or Internet in a non-school setting.

The principal/designee agrees to promote the terms and conditions of this Policy with the student and to instruct the student on the acceptable use of the network and proper network etiquette. The principal/designee also agrees to report any misuse of any information resource or technology to the school site technology representative.

### **PBSD 1664 – Employee Internet/Intranet Services Acknowledgement and Consent**

District Form PBSD 1664 is available as a PDF document or an online web form at the District's Records Management Forms web site at

<http://www.palmbeachschools.org/forms/> A sample of the form is shown below:

#### **THE SCHOOL DISTRICT OF PALM BEACH COUNTY**

#### **Employee Internet/Intranet Services Acknowledgement and Consent**

This form is to be used by the employee to request access to Internet and intranet services through the networking facilities in the District. This form must be completed and signed by each employee that wishes to use any Internet or intranet services, including district e-mail, world-wide web and other Internet services. Employees must agree to the conditions below to gain access to Internet or District intranet services. Employees must read and be familiar with the IT User Standards and Guidelines Manual available at <http://itsecurity.palmbeach.k12.fl.us>.

#### **Acceptable Use and Non-Disclosure Statement**

1. I have read, understand, and am responsible for actions described in *Board Policy 3.29, Employee Use and Technology* at <http://www.palmbeachschools.org/policies/> and the IT User Standards and Guidelines Manual at <http://www.palmbeachschools.org/it/security.asp>.
2. I acknowledge that a very limited expectation of privacy exists to the extent required by law for me as an employee related to my use of District technology resources. District technology resources may be monitored for all lawful and good cause purposes. Use of these resources constitutes consent for the District to monitor these resources for these purposes. I further acknowledge that the District may retrieve and/or disclose, as allowed by law, all messages stored by the District or an outside entity on its behalf. I have been advised that many District technology resources, including but not limited to laptops and desktops, may contain input systems such as web cameras and microphones which can be remotely controlled to turn them on and off. The District will not utilize any such input systems remotely unless it is consistent with the law.
3. I acknowledge that before using the District's technology resources, I will be familiar with the District's employee code of conduct (School Board Policy 3.02) as well as Fla. Admin. Code Sections 6B-1.001 and 6B-1.006, including the provisions prohibiting harassment and discrimination, defamation, use of institutional privileges for personal gain, and improper disclosure of confidential information; Fla. Stat. § 112.313, including the duty to avoid improper use or disclosure of "information not available to members of the general public and gained by reason of [their] official position for [their] personal gain or benefit or for the personal gain or benefit of any other person or business entity", and School Board Policy 8.121 on the use of copyrighted materials.
4. District technology resources, applications, and databases will be used only for my assigned duties and responsibilities in performance of District business as stated in Policy 3.29 and its Manual.
5. All activities performed while using my District computer account will be attributed to me and no one else.
6. My District computer account may be used by me to electronically sign District documents and make binding legal obligations for transactions, if I am authorized to do so. My account may also be used to access and update my personal information in District information systems.
7. I acknowledge my intent to be bound by documents I sign electronically by the method described above in paragraph 6.
8. All passwords assigned to me will be kept confidential and I will not disclose them to any third-parties.
9. Non-compliance with the above conditions may result in disciplinary actions, including loss of privileges, suspension, or dismissal.

By signing below, I hereby acknowledge that I have read and understand the terms and conditions of this Acknowledgment and Consent, the statements are true and correct, and I agree to be bound by the terms and conditions.

## IT User Standards and Guidelines Manual

---

EMPLOYEE \_\_\_\_\_ ID # \_\_\_\_\_

\_\_\_\_\_  
SIGNATURE OF EMPLOYEE

\_\_\_\_\_  
DEPARTMENT

\_\_\_\_\_  
DATE

