INFORMATION TECHNOLOGY

User Standards and Guidelines Manual

April 6, 2016

Division of Information Technology

http://www.palmbeachschools.org/it/security.asp

Table of Contents

1. Introduction 3
2. General Security Standards 4
   2.1. District Responsibilities 4
      2.1.1. Security Objectives 4
   2.2. User Responsibilities 4
   2.3 Limited Expectation of Privacy 5
   2.4. Employee Biometric Record Standards 6
   2.5 Encryption Standards 7
   2.6 E-Signatures 7
3. Acceptable Use Standards 8
   3.1 Email and Calendaring System Acceptable Use 9
   3.2 Software and Hardware Acceptable Use 9
   3.3 Personal Technology on School District Property 10
   3.4 Unacceptable Uses of Technology Include: 10
4. World-wide Web Standards and Guidelines 11
   4.1 Safe Surfing Guidelines 11
      4.1.1 Protect Your Confidential Personal Information 11
      4.1.2 Use Anti-Virus and Anti-Spy ware Software and a Firewall 11
5 Email AND OTHER ELECTRONIC COMMUNICATION Standards And Guidelines 12
   5.1 Spam 12
   5.2 User Responsibilities 13
      5.2.1 Public Records Law Adherence 13
      5.2.2 Standards for Retention of Email and Other Electronic Messages 14
   5.3 Email and Calendaring Privacy 14
   5.4 Shared Accounts 15
   5.5 Accessing another User's Email 15
   5.6 Backup and Restoration of Email Messages 15
   5.7 Technology Process for Exiting Employees 15
   5.8 Technology Process for Exiting Third Parties 15
6. Network Use Standards and Guidelines 16

6.1 Network Authentication 16
6.2 Network Inactivity 16
6.3 Approved Network Devices 16
7. Password Standards and Guidelines 17
7.1 Password Expiration 17
7.2 Password Confidentiality 18
7.3 Compromised Passwords 18
7.4 Enforcement 18
7.5 Password Construction Guidelines 18
7.5.1 Password Length 18
7.5.2 Composition 19
8. Wireless Network Standards and Guidelines 19
8.1 Approved Wireless Access Points 19
8.2 Authenticated Access 19
8.3 Encryption 19
8.4 Network Monitoring 19

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

Appendix 2 **PBSD 1664 – Employee Technology 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, 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

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. *Furthermore, nothing in these guidelines and standards should be construed to prohibit protected activity under the law.*

2. 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.

2.1. District Responsibilities

2.1.1. 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.

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.

2.2. 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 District.
- 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.
- 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 by contacting the District's Information Technology Service Desk and opening a work order.
- 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.

2.3 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 the District's Inspector General's office, IT Security and/or School Police may monitor District information resources. The District's Inspector General office's, IT's and School Police's monitoring must be reasonable in scope and 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;
- Investigating an allegation of theft of time;

- 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. 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.

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.

2.4. Employee Biometric Record Standards

It is the responsibility of all users that have access to employee 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.

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

2.5 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 email, encrypting a desktop work file, protecting a personal private key or digital certificate, or encrypting a saved email.

- Encryption keys shall 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 shall be performed over an encrypted communications session.

2.6 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 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 Statue, rule, or regulation are met.

3. 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, in violation of the provisions of the School Board's technology policies, 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.

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. *Furthermore, nothing in these guidelines should be construed to prohibit protected activity under the law.*

3.1 Email[1] and Calendaring System Acceptable Use

Unacceptable uses of the District's email and calendaring system include but are not limited to:

- Violating the conditions of the Florida State Board of Education's Administrative Rules dealing with students' rights to privacy (SB6A-1.0955).
- Using obscene language.
- 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.

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

[1] **Note: these standards also apply to text messaging, instant messaging and other forms of electronic messaging.**

Users are forbidden from making unauthorized copies of software.

3.3 Personal Technology on School District Property

The use of personal devices on District property by employees and other persons acting on behalf of the District, when conducting District business, must comply with all applicable laws, Board Policies, School and Department directives and procedures, rules, and regulations as if it were a District owned device. The following conditions apply:

- Employees and third parties with District email accounts are discouraged from using personal email accounts to conduct official District business. If their personal or non-District email accounts are used to transact official District business and the District needs access to these emails for good cause, the employees and third parties voluntarily consent to provide these emails timely to the District upon request. If the employees or third parties fail to provide them to the District, they agree that the District has the authority to contact the online carrier/service provider to retrieve these emails.
- District business communications remain the property of the District including when using employee's personal technology or devices.
- Employees are responsible for removing or wiping District files off of personal technology when disposing of the devices and upon the employee's separation from the District. If there is an official record that is being removed that is required to be retained as required by the District Records Retention Schedule, it must be stored in a District repository, such as a District Google Drive or a District server.
- The School Board/School District will not be responsible for loss, theft, or damage of personal devices brought onto District property.
- Employees must immediately report the loss of any personal technology that contains District data or confidential information.
- Information Technology (IT) does not support personal devices.
- Personal devices shall not be used to circumvent the District firewalls or the filter to access websites for display to students that would otherwise be blocked from delivery to students. An example of prohibited use would be using a personal cellular hot-spot to show blocked material to a student or class.

3.4 Unacceptable Uses of Technology Include:

- 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, threatening, harassing, defamatory, obscene, pornographic, libelous, invasive of another's privacy, harmful to minors, of malicious intent, or racially or ethnically 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 email 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.

4. 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.

4.1 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.

4.1.1 Protect Your Confidential Personal Information

Users shall not share their confidential personal information unless they know how it will be used and protected. Users shall not reply to or click on any links in any emails asking for confidential personal information.

4.1.2 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. Contact IT Service Desk to Report Security Incidents.

Contact the IT Service Desk to report any security incidents that have occurred. The Service Desk will contact the IT Security team, who will respond appropriately to resolve any security incidents including cyber-attacks and will work to prevent them from reoccurring.

5 Email And Other Electronic Communication Standards And Guidelines [2]

All employees receive the Email and Calendaring Service with their Employee User ID account. Employees are expected to use the District's email 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. Email 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 email 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 for educational or learning purposes.

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

5.1 Spam

Despite all of the precautions taken to block spam, some spam does make it through to the District's email system. Employees should utilize the SPAM reporting feature within the District's email system.

[2] Note: Where applicable, these standards govern not only to emails but also text messaging, instant messaging and other forms of electronic messaging.

5.2 User Responsibilities

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

5.2.1 Public Records Law Adherence

a. Public records are subject to inspection by the public unless a statutory exemption exists. If Email 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. Treat emails, instant messages, text messages, tweets, and other instantaneous messages that involve official School District business as public records.

b. The District maintains an email archive system. If one's Email is subject to long term retention, each user is individually responsible for maintaining the public accessibility of his/her own incoming and outgoing Email messages that are official records as required by the Public Records Law. Questions relating to whether or not the content of a particular Email message constitutes a public record should be directed to the District's Department of Communications.

c. District employees must retain communications generated through a computer or electronic device that meets the definition of a public record. Retention is required subject to the District's Records Retention Schedule[3], records holds, and Florida law concerning public records, as explained in School Board Policy 2.041. These communications include but are not limited to email, text messages, instant messages, tweets, and similar instantaneous methods of communication. Employees shall not communicate in text messaging, instant messaging, tweeting or other methods of instant electronic communication if the messages cannot be retained as required by the District's Retention Schedule. Employees are allowed to communicate through transitory messages, as defined in the District's Records Retention Schedule.

[3] This Schedule is located on the District's Records Management Department website at: http://www.palmbeachschools.org/records/documents/RecordsRetentionSchedule.pdf .

5.2.2 Standards for Retention of Email and Other Electronic Messages

If, according to State mandated records retention schedule, the content of an email message possesses long term business value and is an official record, to the extent the District has not archived one's emails, or if one's emails are subject to long term retention, employees are required to retain the message and either immediately or eventually move and archive the email 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.

If a records hold exists, 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 General Counsel. The emails relating to those issues must be retained irrespective of the retention schedule until advised by the Office of Chief General 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.

The Palm Beach County School District Records Retention Schedule, must be referenced to determine the specific retention requirement for Email messages. Questions relating to which record series are applicable for a particular Email message should be directed to the Records Management section of Information Technology. Within this Schedule:

See Electronic Communications – Pages 1 and 30.

See Transitory Messages - Pages 1, 30 and 87.

See Records Hold – Page 1

5.3 Email and Calendaring Privacy

All email messages sent and received by the District's email and calendaring system are the property of the District. Email users have only a limited expectation of privacy to

the extent required by law (see section 3.3, above). The District reserves the right to review all electronic correspondence that uses District systems and facilities.

5.4 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. Email distribution lists should be used when the same information is to be distributed to several users.

5.5 Accessing another User's Email

Where appropriate, users may delegate access to their email and calendar to other secondary/delegated users. This shall be done by means of the email and calendaring system's delegation facilities, not by giving the delegate access the primary user's user ID and password.

5.6 Backup and Restoration of Email Messages

District email is archived off-site through the provider, including Disaster Recovery services.

5.7 Technology Process for Exiting Employees

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

The employee is responsible to provide and the employee's supervisor is responsible for obtaining:

- Email
- The return of District -owned equipment including but not limited to cellular phones, smart phones, iPads, computers, tablets and any other District-owned technology.
  - District process for property transfers must be followed for applicable items. See District form PBSD 0082.
- Access, including applicable passwords and any other authorizations needed, to any employee's District work files stored electronically. If needed, the Supervisor can contact the IT Service Desk for assistance using a service request in the District work order tracking system.

5.8 Technology Process for Exiting Third Parties

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

The Third Party is responsible to provide and the District's supervising department is responsible for obtaining:

- The return of District -owned equipment including but not limited to cellular phones, smart phones, iPads, computers, tablets and any other District-owned technology.
  - District process for property transfers must be followed for applicable items. See District form PBSD 0082.

Access, including applicable passwords and any other authorizations needed, to any Third Party's District work files stored electronically on District resources, and elsewhere if contract allows. If needed, the Supervising Department can contact the IT Service Desk for assistance using a service request in the District work order tracking system.

6. Network Use Standards and Guidelines

The District's data network is the backbone of its information resources. 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 all locations and users shall follow these standards when connecting to one of the wireless networks.

6.1 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.

6.2 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.

6.3 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, 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 publicly available District technology resources.

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.

7. 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.

7.1 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.

7.2 Password Confidentiality

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

Unless otherwise authorized by School Board Policy, 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.

7.3 Compromised Passwords

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

7.4 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.

7.5 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.

7.5.1 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.

7.5.2 Composition

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

8. Wireless Network Standards and Guidelines

Access to the District information resources via unsecured wireless communication methods is prohibited.

A non-secure guest 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. Guest wireless access is very limited and should not be used for accessing non-public information resources. The District shall not be liable for any loss or damage of whatever nature (direct, indirect, consequential, or other) whether arising in contract, tort or otherwise, which may arise as a result of the Public's or Guest's use of (or inability to use) the District network.

8.1 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.

8.2 Authenticated Access

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

8.3 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.

8.4 Network Monitoring

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

Appendix 1

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, PBSD 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:

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.

1. 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, defamatory, bullying, 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 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.
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, unless otherwise allowed by School Board policy, and the student will not disclose them to *any* third-parties.
12. The student acknowledges when accessing a commercial site or product they will first read the site's Terms of Service statement, Privacy Policy statement, and Contract or License for Use. The student will not use sites or products that can expose the student's personal information.
13. Students must use outside sites when required by the District or the State for educational purposes, or when the District contracts with third-party website operators to offer educational programs - for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. Students may use outside sites with written parental consent and if allowed by the school.

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.

Appendix 2

THE SCHOOL DISTRICT OF PALM BEACH COUNTY
INFORMATION TECHNOLOGY

Employee Technology Services Acknowledgement and Consent

This form must be completed and signed by each employee that wishes to use District technology, including but not limited to, Internet or intranet services, district e-mail, world-wide web access and other technology resources. Employees must agree to the conditions below to use District technology. Employees must read and be familiar with the **IT User Standards and Guidelines Manual** *(see link on page 2 of this form).*

Type the Employee ID number and press tab. If the employee information does not appear do not submit the form. Close and try later or call PX 44100.

Employee ID #	Employee First Name	Employee Middle Name	Employee Last Name
Job Title		School/Department Name	

Acceptable Use and Non-Disclosure Statement

1. I have read, understand, and am responsible for actions described in **Board Policy 3.29**, **Acceptable Use of Technology by Employees** and the **IT User Standards and Guidelines Manual** (Manual) *(see links on page 2 of this form).*
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, including by GPS, as per the District's policy, 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.
3. I understand and acknowledge that District equipment and assets, including but not limited to, school buses, desktops, laptops, and mobile devices may be tracked for location by GPS and other technologies during my use and/or while in my possession. If the equipment is lost or stolen, I must immediately report it to my supervisor. I acknowledge that electronic device tracking may be used for disciplinary and or legal/actions against me and/or others for unauthorized movement of District equipment.
4. I acknowledge that before using the District's technology resources, I will be familiar with the District's employee Code of Ethics (**School Board Policy 3.02**) as well at **Fla. Admin. Code 6A-10.080 and 6A-10.081** including the provisions prohibiting harassment and discrimination, defamation, and libel, prohibiting matters that are obscene, hateful or harmful to minors, use of institutional privileges for personal gain, and improper disclosure of confidential information; and as stated in **Fla. Stat. §1123.313(8)**, 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".
5. I acknowledge that I will comply with all copyright laws and license agreements during my use of technology as set forth herein and in **School Board Policy 8.121** on the use of copyrighted materials. I further understand and acknowledge that I will not install, duplicate, and/or distribute software that is not in compliance with the license or copyright agreement.
6. District technology resources, including but not limited to, desktops, laptops, and mobile devices, applications, and databases, will be used only as stated in Policy 3.29 and its referenced IT manual.
7. All activities performed while using my District computer account will be attributed to me and no one else.
8. 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.
9. I acknowledge my intent to be bound by documents I sign electronically by the method described above in paragraph eight (8).

PBSD 1664 (Rev. 2/12/2016) ORIGINAL - Division of Human Resource/Customer Relations. Page 1 of 2

10. I acknowledge that I will conserve District resources by not storing personal files, documents, or other information in locations that are being backed-up, archived, or otherwise electronically saved by the District.
11. Unless allowed by a School Board Policy, all passwords assigned to me will be kept confidential and I will not disclose them to any third parties.
12. I acknowledge that for electronic mail communications, the District discourages that I use my personal email accounts to conduct official District business. If my personal email accounts are used to transact official District business and the District needs access to these emails for good cause, I voluntarily consent to provide these emails timely to the District upon request. If I fail to provide them to the District, I agree that the District has the authority to contact the online carrier/ service provider to retrieve these emails.
13. Non-compliance with any of the above conditions may result in disciplinary actions, including loss of privileges, suspension, or dismissal.
14. 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.

Links:

IT User Standards and Guidelines Manual

School Board Policies 3.02 and 3.29

Fla. Admin. Code Sections 6A-10.080 and 6A-10.081

Fla. Stat. § 112.313

Signature of Employee REQUIRED

Click to sign

After you sign the form click "Go" to submit.

PBSD 1664 (Rev. 2/12/2016) ORIGINAL - Division of Human Resource/Customer Relations Page 2 of 2

Appendix 3

THE SCHOOL DISTRICT OF PALM BEACH COUNTY

Third-Party Internet/Intranet Services Acknowledgement and Consent

This form is to be used by the third-parties to request access to Internet and intranet services through the networking facilities in the District. This form must be completed and signed by each third-party that wishes to use any Internet or intranet services, including district e-mail, world-wide web and other Internet services. Third-parties must agree to the conditions below to gain access to Internet or District intranet services. Third-parties must read and be familiar with the IT User Standards and Guidelines Manual available at *http://www.palmbeachschools.org/it/security.asp*.

Acceptable Use and Non-Disclosure Statement

1. I have read, understand, and am responsible for actions described in *Board Policy 2.50, Third-Party Use of District Technology at* http://www.palmbeachschools.org/it/security.asp 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 a third-party related to my use of District technology resources. District technology resources may be monitored for all lawful and good cause purposes, including GPS tracking. 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.
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 6A-10.080 and 6A-10.081, including the provisions prohibiting harassment and discrimination, defamation and libel, prohibiting matters that are obscene, hateful, or harmful to minors, 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 2.50 and its Manual.
5. I acknowledge that I cannot, by any means take, obtain, receive, acquire, or capture any District data, meta data, or information from any District system for any purpose without written consent from the District.
6. All activities performed while using my District computer account will be attributed to me and no one else.
7. 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.
8. I acknowledge my intent to be bound by documents I sign electronically by the method described above in paragraph 6.
9. All passwords assigned to me will be kept confidential and I will not disclose them to *anyone*.
10. I acknowledge that for electronic mail communications if I am provided a District email account, the District discourages that I use non-District email accounts to conduct official District business. If non-District email accounts are used to transact official District business and the District needs access to these emails for good cause, I voluntarily consent to provide these emails timely to the District upon request. If I fail to provide them to the District, I agree that the District has the authority to contact the online carrier/service provider to retrieve these emails.
11. Non-compliance with any of the above conditions may result in consequences, including loss of privileges, or termination of agreement.
12. 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 the law.

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.

Print Name of Third Party	*Signature of Third Party*	*Date*

PBSD 2359 (Rev. 2/12/2016) SBP 2.50 ORIGINAL- Department engaging hiring or using third party COPY - third party page 1 of 1