LAFAYETTE DISTRICT SCHOOLS

Information & Instructional Technology

Policies and Procedures

TABLE OF CONTENTS

Lafayette County School Board Information and Instructional Technology Policies and Procedures **3**

Information & Instructional Technology Services **3**
- Organizational Chart **3**
- Job Descriptions **3**

Ownership and use of Information & Instructional Technology Resources **3**
- Technology Equipment **4**
- Software **4**

Technology Resources **4**

Security **5**
- User Accounts **5**
- Passwords **6**
- Administrator rights **6**
- Data Loss Prevention Program **7**
- Disaster Recovery Plan **7**
- Security Incident Response Plan **7**

Unacceptable Use **7**
- System and Network Activities **8**
- Email and Communications Activities **9**

Web Pages **9**

Purchasing **9**

Technology Committee **10**

Training **10**

Enforcement **10**

Revisions **10**

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

All users agree to comply with the LCSB Information & Instructional Technology Policies and Procedures with applicable state and federal laws dealing with appropriate, responsible and ethical use of information technology. It is the responsibility of the user to be aware of the existing policies and to adhere to their guidelines. Non-compliance is a serious breach of the Lafayette County School Board's standards and may result in legal and/or disciplinary action for all users, employees and students.

These policies are applicable to all LCSB technology resources and are global in scope. No department and/or school may override the guidelines and restrictions contained within this technology policy.

INFORMATION AND INSTRUCTIONAL TECHNOLOGY SERVICES

The organizational chart for LCSB Information & Instructional Technology Resources is located in **Appendix A**.

Job descriptions for all personnel assigned to LCSB Information & Instructional Services is located in **Appendix B**.

OWNERSHIP AND USE OF INFORMATION TECHNOLOGY RESOURCES

The Information & Instructional Technology resources provided and maintained by IIS Services are intended for LCSB related purposes including the support of the LCSB mission, its administrative and instructional functions and activities within the user community. Appropriate use of computing resources includes respecting the privacy of other users and their accounts, using only those resources you are authorized to use, respecting the finite capacity of these resources so as not to limit their accessibility by others and abstinence from using any of these resources for personal gain or commercial use not related to LCSB business. Unauthorized and/or inappropriate use of these resources is prohibited and may result in disciplinary and/or legal action. Unauthorized or fraudulent use of LCSB telecommunications resources can result in felony prosecution as provided for in Florida Statutes. Resource areas are defined as follows:

Technology Equipment

Technology equipment may include but is not limited to workstations, laptops, mobile communication devices, tablets, servers and network devices such as routers, patch panels, switches and wireless access points. LCSB may require users of computing equipment to limit or refrain from specific uses of that equipment if their activities are destructive or interfere with LCSB technology operations or resources. No unauthorized user may connect to any LCSB network resource that provides access to the internal network of the District. They may connect to the LCSBGuest network under the provisions of the District's Bring Your Own Device (BYOD) program as explained in **Appendix C.** An LCSB computer may be loaned upon request with 48 hours notice to sales representatives, consultants, trainers or others as needed for network access. This computer may not leave District property. The Director of Information & Instructional Services has the authority to approve specific contracted services to access the network with their own equipment when such connection can be done securely and safely. Examples of possible connection consideration would include auditors with the Auditor General Office, Meridian Healthcare, installation engineers with specific approved applications and similar services.

All employees assigned a mobile device, such as a laptop, must have a Lafayette District Schools Technology Equipment Sign-Out Form on file in the Information & Instructional Technology Services office. A copy of this form is in **Appendix I.**

Software

For the purpose of this policy and procedures manual, the term software will include not only applications installed directly on individual computers but also applications installed on any technological device of LCSB or that is accessed by said devices from cloud based resources.

Software owned by the Lafayette County School Board will be installed on computers set up for the end users by an LCSB technology support technician. All software installed on LCSB computers must be properly licensed and authorized.

All software, hardware or applications for use on or with LCSB technology equipment, beyond normal repair operations, must be approved by the principal of the affected school who will refer it to the Director of Information Technology for review to ensure compatibility with existing hardware/software. Any changes or additions to existing software may also be brought to the attention of the Technology Coach assigned to their respective school for referral.

TECHNOLOGY RESOURCES

It is a general policy of the Lafayette County School Board for the network to be used in a

responsible, efficient, ethical, and legal manner in accordance with the mission of the District. Failure to adhere to policies and guidelines may result in legal and/or disciplinary action.

Employees are required to (at the start of each academic year) sign and abide by the Lafayette District Schools Employee Acceptable Use Policy (see **Appendix D**). The signed form will be on file in the Information & Instructional Technology Services office.

Students are required to sign and abide by the Lafayette District Schools Employee Acceptable Use Policy (see **Appendix E**). The signed form will be on file in the students individual cumulative folder.

SECURITY

The network system of Lafayette District Schools is available for use by employees, students, and other authorized users to provide access to the computing resources which serve public education. No expectation of privacy or confidentiality in the content of electronic communications including, but not limited to, computer files, electronic messaging, facsimile or other transmissions sent, received through or stored on the communication resources of Lafayette District Schools should be expected by users. Such information is subject to review, monitoring and archiving.

In accordance with the Children's Internet Protection Act (CIPA) filtering technology will be utilized to limit students access to prohibited material. Employees will be filtered only to the extent of protecting the security and integrity of the Lafayette District Schools network. Any use of the network or associated technological tools for illegal, inappropriate or obscene purposes, or in support of such purposes is prohibited.

User Accounts

General network accounts will be managed through Active Directory or other managed authentication systems (Google Gmail) for employees and students. When access is required for a new employee, access will only be granted after submission of an email request by the employee's supervisor to the Director of Information Technology and signing the Acceptable Use Policy. When employment is terminated the user account will be disabled or altered to prevent further access. Access will terminate effective 4:00 PM of the date of departure in lieu of unique circumstances. It is the responsibility of an individual's supervisor to inform the Director of Information Technology of a change in employment status.

Volunteers, non-school/district staff and non-permanent substitutes are not permitted access to LCSB network resources. In situations of long-term substitutes or other unique situations, the school principal or department head may request an access waiver to the Director of Information Technology.

At the end of each academic year or prior to the start of the next academic year, a complete audit of all active directory and email accounts will take place. This audit will be conducted with input from members of the Administrative Staff as required. Any account that cannot be reconciled during this audit will be locked immediately.

Passwords

Upon approval of access to the LCSB network a user ID and temporary password will be assigned. This initial password will be set to require a password change at first login to the network. Passwords will be kept secure and not provided to others. If a user password is required for the purpose of troubleshooting a technology problem, a mandatory password change will be initiated upon completion of the troubleshooting.

All passwords:

1. Must be a minimum of eight characters.
2. Must include a minimum of three of the
   following: Upper case letters
   Lower case letters
   Numbers
   Symbols
3. Must be changed every ninety days.
4. Must have a minimum password age of one day.
5. Must lock after five unsuccessful attempts at logging on.
6. Must not be repeated until four unique passwords have been used.
7. Will lock after sixty minutes of workstation inactivity, requiring the reentry of the user's password.

Administrator Rights

Administrative passwords for the network, servers, computers, switches, access points, firewall, controller, or any other electronic device utilized for security or maintaining the Lafayette District network will be kept strictly confidential. Network administrative access will be limited to the Director of Information Technology, Instructional Technology Specialist, Technology Aides (if necessary for their duties) and no more than two NEFEC technology support personnel.

Employees (or students) utilizing Lafayette District School devices will not be grant administrative rights to those devices.

Data Loss Prevention Plan

The Data Loss Prevention Plan for Lafayette District Schools is located in **Appendix F** of these

Policies and Procedures.

Disaster Recovery Plan

The Disaster Recovery Plan for Lafayette District Schools is located in **Appendix G** of these Policies and Procedures.

Security Incident Response Plan

The Security Incident Response Plan for Lafayette District Schools is located in **Appendix H** of these Policies and Procedures.

UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services). Exemption can only be authorized by the Director of Information Technology or the Superintendent of Schools.

Under no circumstances is an employee, student, or guest of Lafayette County Schools authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Lafayette County School-owned resources, to include the network and Internet.

Attempts to circumvent or defeat mechanisms put in place by the Lafayette County School District IT staff to manage the network is strictly forbidden.

Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Lafayette County School District.

Unauthorized copying of copyrighted material including, but not limited to, digitization

and distribution of photographs from magazines, books or other copyrighted sources; copyrighted music; and the installation of any copyrighted software for which Lafayette County School District or the end user does not have an active license is strictly prohibited.

Exporting software, technical information, encryption software or technology.

Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a Lafayette County School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any Lafayette County School District account.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purpose.

Port scanning or security scanning unless prior notification and approval is received from the Director of Information Technology (except as required by the duties of the Network Specialist).

Executing any form of network monitoring unless prior notification and approval is received from the Director of Information Technology (except as required by the duties of the Network Specialist).

Circumventing user authentication or security of any host, network or account.

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network connectivity, via any means, locally or via the network/Internet.

Providing information about, or lists of, Lafayette County School District’s students or

employees to parties outside the Lafayette County School District without prior permission from the Superintendent of Schools.

Unacceptable Use: Email and Communications Activities

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited email originating from within Lafayette County School District's networks or of other internet/network service providers on behalf of, or to advertise, any service hosted by Lafayette County Schools or connected via Lafayette County School's network.

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

WEB PAGES

The Director of Information Technology has responsibility for oversight of all web pages created in or for the Lafayette District School System. Content for Lafayette Elementary and Lafayette High Schools web pages are the responsibility of the respective principals.

PURCHASING

The Department of Information Technology is responsible for seamless integration of any hardware or software into the existing technology system of Lafayette District Schools and maintaining an inventory of all such items. When considering the purchase or addition of any technology related item, prior approval from Information & Instructional Technology Services is required. A verbal consent is not acceptable.

TECHNOLOGY COMMITTEE

Lafayette District Schools will maintain a Technology Committee comprised of the Director of Information Technology, other technology staff as necessary, other District level Administrators as necessary, LES Principal, LHS Principal, and Instructional Technology Coach.

The Purpose of the Technology Committee is:

1. To provide a forum to discuss issues, concerns, and/or interests of the teachers and administrators at each school with the Information & Instructional Technology Services Department.
2. To assist in promoting the efficient use of technology in schools, including creating standards for the management and application of technology.
3. To serve as a resource for Lafayette County Schools in helping all employees understand technology in schools and how to use it properly and efficiently.
4. To assist in planning for and evaluating classroom technology (such as model classrooms and educational software).
5. To assist in planning professional development activities related to technology.
6. To assist in other activities as deemed appropriate.

TRAINING

The procedures contained in this Information & Instructional Technology Policies and Procedures manual will be included in the annual training for employees at a time determined by the Superintendent of Schools. It will also be made available on the Lafayette District web site with email references to all employees on a periodic basis.

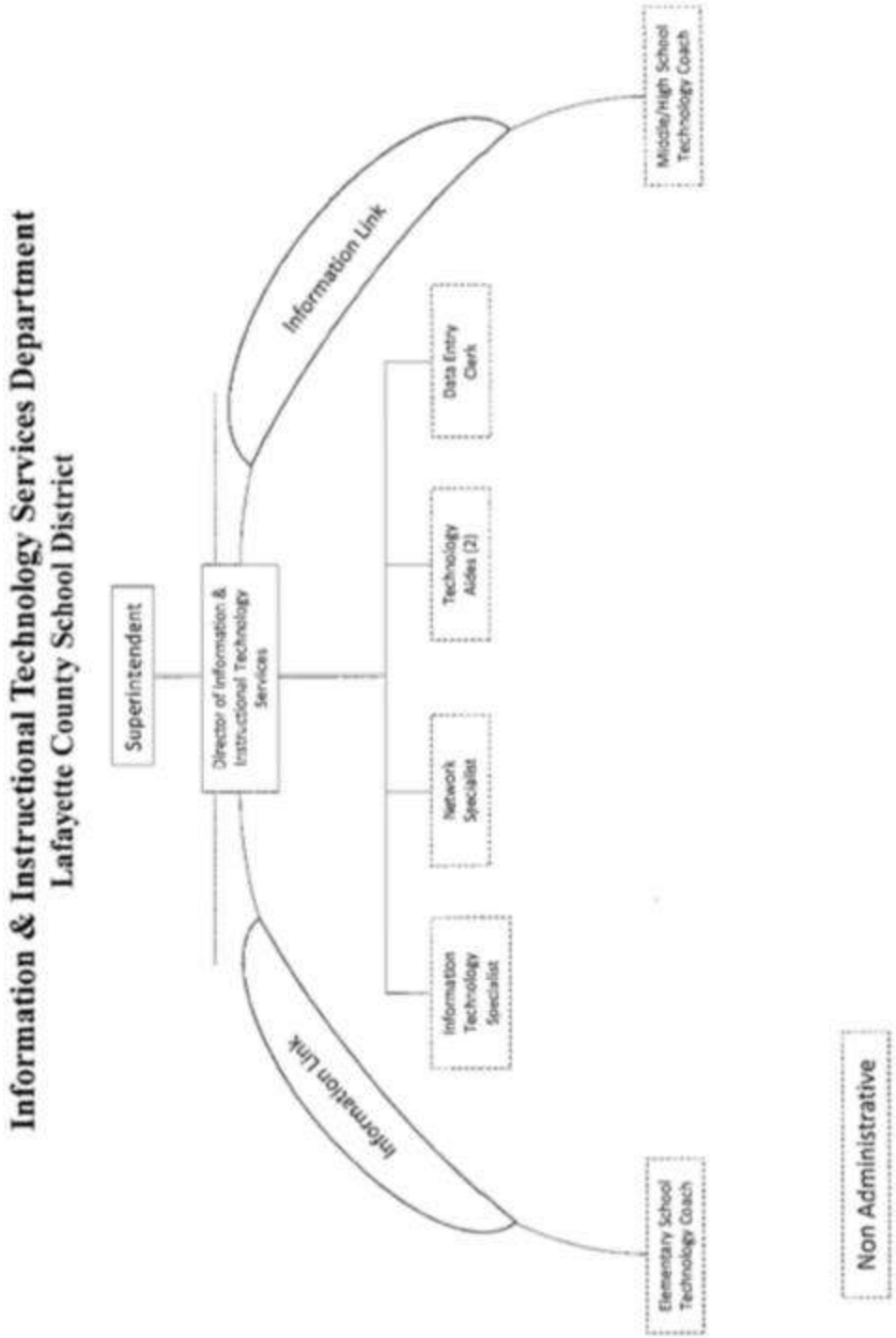
ENFORCEMENT

Failure to adhere to these policies and procedures may result in suspension or revocation of the offender's privileges or access to the District's technology resources and/or other disciplinary or legal action.

REVISIONS

The Lafayette County School Board reserves the right to change these Policies and Procedures at any time to ensure the operability and safety of the District's network and the users thereof.

Information & Instructional Technology Services
APPENDIX A
Organizational Chart



Information & Instructional Technology Services
APPENDIX B Job Descriptions

To be developed.

Information & Instructional Technology Services
APPENDIX C
BRING YOUR OWN DEVICE (BYOD) PROGRAM

This is still needing to be written.

Information & Instructional Technology Services
APPENDIX D
Employee Acceptable Use Form

EMPLOYEE NAME _____ DATE _____/_____/_____

Lafayette School District views the use of computers and retrieval of information from the Internet in the same manner as information retrieval from reference materials identified by the school (i.e. library). Specifically, Lafayette School District supports those materials which will enhance the research and inquiry of the learner with directed guidance from faculty and staff. However, on a global network (the Internet) it is impractical to control all materials; users may discover inappropriate information. Teachers and other staff using the Internet should abide by the same high standards in their use of the Internet. Inappropriate Internet information and use is considered to be, but not limited to, the following:

1. The retrieving and viewing of any information that is pornographic in nature.
2. The disclosing of personal information without that person's consent.
3. Using profanity, obscenity, or other language that may be offensive.
4. Copying commercial software in violation of copyright laws.
5. Using the Internet for financial gains or for any commercial or illegal activity.
6. "Surfing" with no educational objective in mind.
7. Downloading and playing of games and/or music that are of no direct educational value
8. Engaging in "Bullying" or solicitation of any type.
9. Any other activity that may bring embarrassment to the Lafayette District School System.

Inappropriate device (computer, tablet, etc.) use is deemed to be, but not limited to the following:

1. Failure to keep personal passwords confidential, to include allowing others access under your username and password. (This includes Teacher's assistants.)
2. Using profanity, obscenity, or language that may be offensive in the creation of any documents, to include the naming of files.
3. Rendering the computer or peripheral devices (mouse, printers, keyboard, etc.) inoperative.
4. "Tampering" with programs or files, to include unauthorized deleting.
5. Unauthorized installation of programs or files.
6. Any use that violates the copyright laws.
7. Any use that violates established policies of the Lafayette District Schools System.
8. Physical damage to computers or peripheral devices.
9. The sending or forwarding of emails containing inappropriate materials, personal emails or "chain" emails.
10. The District LAN is considered a public network and as such there is no reasonable expectation of privacy beyond that stated by Florida law (student information and certain personnel information).

An employee who is aware of any infraction of these requirements, by an employee or student, is required to report such infraction to their immediate supervisor, who, in turn, will notify the IT Department. Failure to comply with the above or any other item deemed necessary by the administration will result in the loss of computer privileges and/or possible disciplinary actions. The employee is required to apply the same confidentiality standards to sensitive information in the use of the Internet and any technology devices as are required in the normal course of their work. Anyone accessing computers or the internet must have a current, signed internet/computer use form on file with the District IT Department. The signature below indicates agreement, understanding, and compliance with the policy stated herein.

_____ _____

Signature Date

STUDENT NAME _____ GRADE _____ DATE OF BIRTH _____/_____/_____

Lafayette High School Acceptable Use Policy

Lafayette Schools views the use of computers and access of the Internet as essential to the learning environment. The District fully supports those materials that will enhance the research and inquiry of the learner with directed guidance from faculty and staff. However, it is impractical to control *all* materials on the internet and users may discover inappropriate information. This AUP outlines the guidelines and behaviors users are expected to adhere to. The guidelines contained within are not intended to be an exhaustive list. Users should use their own good judgement when using school technologies.

I will:

- Treat school resources carefully, and alert staff if there is any problem with its operation.
- Use school technology at appropriate times, in approved places, and as advised by teachers for educational purposes.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Recognize the use of school technologies as a privilege and treat it as such.
- Keep my password and personal information confidential and notify my teacher if I believe it has been compromised.
- Communicate with the same appropriate, safe, mindful, and courteous conduct as offline.

I will **not:**

- Attempt to find or access inappropriate content or try to circumvent school safety measures and filtering tools.
- Use inappropriate language or engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Install software, change inappropriate settings, or any other activity not approved by an appropriate staff member.
- Engage in criminal activity, violate copyright, hack, or any activity that may bring embarrassment to the school district.
- Use my district owned device or accounts for any purpose other than education.

We would like to inform you that we wish to create individual email accounts for students to login to their chromebooks and receive assignments from their teachers. We feel this is an essential step in our move to a more digital curriculum and to prepare students for computer based testing. These email accounts may be monitored through the use of classroom management software. The use of email for children ages 13 and under is not permissible without consent from a parent or guardian. By signing this form, you are agreeing to the creation of a student email account for your child. If you have any concerns, please contact school administration before signing.

Lafayette County Staff will have the ability to monitor all district owned accounts and any traffic flowing in or out of the school network. Failure to comply with the above or any other activity deemed inappropriate by Lafayette staff will result in disciplinary action by the school district. Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act. Student information will be protected as required by FERPA and HIPPA. Lafayette schools will not be responsible for unauthorized transactions conducted over the school network, or any damage or harm to persons, files, data, or hardware.

Access to computers and the Internet through the Lafayette School District will only be granted with a dated student and parent/guardian signature below. These signatures indicate agreement, understanding, and compliance with the policies stated herein.

_____ _____ _____
Student Signature Printed Student Name Date

_____ _____ _____
Parent Signature Printed Parent Name Date

*If your student does not have permission to appear on Lafayette District web pages or other media, initial here _____.

Lafayette District Schools
Information and Instructional Technology Services

Appendix F
DATA LOSS PREVENTION PROGRAM (Revised 5/23/13)

Protection of data accessed via the network resources of Information & Instructional Technology Services is foremost in importance to Lafayette District Schools. The purpose of this policy is to comply with federal regulations governing privacy and security of information and to protect confidential data from loss or theft. The Family Education Rights and Privacy Act of 1974 (FERPA) is a federal guarantee of the privacy of educational records for students and their parents/guardians. Other privacy and security laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA) may also apply.

Backup Strategy:
All protected data will be backed up on a regular basis of no less than once per week. Backups may be in the form of virtual server snapshots/images, individual file backups and/or database backups. Copies will be stored in a secured environment outside of the building housing the original data. Backups are the responsibility of the Network Specialist.

Physical Security:
All district level servers and storage will be housed in a secured area. The offices of Information & Instructional Technology Services (where the Master Data Facility or MDF is located) will be kept locked when technology personnel are not present. Key access will be limited to those working inside the offices, one emergency responder (resource officer), one facilities technician (with air conditioner responsibility), and the Superintendent of Schools. These offices will be protected with camera security as well as with excessive heat and fire protection.

The resources in the MDF are protected through battery backups and an auxiliary power generator. All servers are protected in either a RAID 5 configuration or RAID 1 configuration with a hot spare hard drive.

IIT Services will monitor Lafayette District owned devices (computers, servers, tablets, etc.) to ensure they are being properly used and have not been compromised.

IIT Services will ensure non-Lafayette District Schools wireless routers, access points and/or “hot spots” are not in use on Lafayette District property. NOTE: this does not include 3G and/or 4G carriers as is commonly used by cell phones, except as such a device is being utilized as a “hot spot” to circumvent Lafayette District policies.

IIT Services will ensure policies are in place to prevent personally owned equipment (commonly referred to as BYOD) from accessing the Lafayette District School internal LAN and such equipment remain on the LCSBGuest wireless network (unless otherwise authorized by IIT). A wireless controller for detection of “rogue” devices with the ability to contain any threats that could compromise Lafayette District Schools data will also be utilized.

Confidential Information:
Information protected by statutes, regulations or Lafayette County School Board Policy are designated as Confidential. Any disclosure of confidential data must be authorized by the Lafayette County Superintendent of Schools or designee. By way of illustration only, examples of confidential data include the following:

1. Medical records,
2. Student records and other non-public student data,
3. Social security numbers,
4. Student Psychological Records,
5. Personnel and/or payroll records,
6. Individualized Education Plans (IEPs),
7. Credit card or bank account numbers,
8. Facility or technology security procedures and processes,
9. Information specifically exempt from public information by LCSB Policy
10. Any data identified by government regulation to be treated as confidential or sealed by order of the court of competent jurisdiction.

Storage Classification:
The protection of all resources is an important function of Information & Instructional Services. It is also important to identify data storage that contains confidential information and develop more rigorous processes to protect the data.

Due to the confidential and mission critical information housed with the District’s Student Information, Human Resources and Finance/Business Management Systems they are

classified as sensitive data. As this data is housed within the Skyward System of the North East Florida Education Consortium (NEFEC) all responsibility for security, backups, etc. for this data, will be under the responsibility of NEFEC.

Sentry File

Lafayette District Schools is undertaking the process of converting all hard copy confidential and sensitive records to digital format. These files will be stored in the Sentry File system under the control of NEFEC. Access to this system is via SSL and restricted to only those personnel with a valid need.

Current hard copies are stored in the District's records room, LHS records room and LES records room. Access to these locations are only by individuals with valid job related need (business personnel, guidance, etc.) Control of these areas are the responsibility of the respective Director or Principal.

As the Sentry File process continues and is more thoroughly defined this policy will be revised to accommodate the required changes.

Health records are controlled by the Florida Department of Health with all electronic communication via SSL. Hard copies are secured in locked containers with access by health personnel only (in compliance with HIPAA laws).

Application: Filemaker Pro

The Filemaker Pro software application includes data used to create, record, track, manage and warehouse Individual Education Plans (IEPs) for students receiving or have received exceptional educational services. Permission to access IEPs rest with the manager of exceptional Education and the Superintendent of Schools.

FileMaker Pro as used for IEPs may not be accessed outside of the Lafayette District Schools LAN. Internal access is granted only to those personnel directly involved with the ESE Program. Any hard copies of records for IEPs, IAPs and 504 Plans must be kept secure. Responsibility for ESE record security is the responsibility of the Director of Teaching & Learning Services and respective Principals.

Data Classification and Handling Policy

Purpose

The purpose of this policy is to establish a framework for classifying and handling LCSD data based on its level of sensitivity, value and criticality to the LCSD as required by the LCSD's Information Security Plan. Classification of data will aid in determining baseline security controls for the protection of data.

Scope
This policy applies to all LCSD employees who access, process, or store sensitive LCSD data.

Definitions
Confidential Data- Generalized term that typically represents data classified as confidential, according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.

Data Owner- An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, school, or administrative unit of the LCSD.

Data Custodian - Employee of the LCSD who has administrative and/or operational responsibility over information assets.

Institutional Data- All data owned or licensed by the LCSD

Information Assets- Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the LCSD

Non-public Information- Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

Sensitive Data - Generalized term that typically represents data classified as Confidential according to the data classification scheme defined in this document.

Data Classification
Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the LCSD should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels (tiers), or classifications:

Tier1-Confidential Data

Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the LCSD or its affiliates. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the LCSD who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Tier 1 Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Confidential/Restricted data include official student grades and financial aid data, social security and credit card numbers, and individuals' health information.

Tier 2-Internal/Private Data

Data should be classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the LCSD or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal/Private data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the LCSD should this information not be available when needed is typically moderate. Examples of Internal/Private data include official LCSD records such as financial reports, human resources information, some research data, unofficial student records, and budget information.

Tier 3-Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the LCSD and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. The appropriate Data Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level 3 Public data not be available is typically low, (inconvenient but not debilitating). Examples of Public data include directory information, course information and research publications.

Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Confidential even though the student's name and address may be considered Public information.

Determining Classification

The goal of information security is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the LCSD if confidentiality, integrity or availability of the data is compromised.

	Potential Impact		
Security Objective	LOW	MODERATE	HIGH
Confidentiality- *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity- *Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability- *Ensuring timely and reliable access to and use of information.*	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Predefined Types of Confidential/Restricted Information Assets

Based upon state, federal, and contractual requirements that Lafayette School District is bound by, the following information assets have been predefined as Level 1 or Level 2 data and must be protected:

Personally Identifiable Education Records-Covered under FERPA

Personally Identifiable Education Records are defined as any education records that contain one or more of the following personal identifiers:

- Grades, GPA, Credits Enrolled
- Social Security Number
- Race/Gender
- A list of personal characteristics or any other information that would make the student's identity easily traceable

Personally Financial Identifiable Information (PIFI) - Covered under GLBA

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data

elements:

- Social security number
- State-issued driver's license number
- Date of Birth
- Financial account number in combination with a security code, access code or password that would permit access to the account

Payment Card Information- Covered under PCI DSS

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Protected Health Information (PHI) - Covered under HIPAA

PHI is defined as any "individually identifiable" information that is stored by a Covered Entity, and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual.

PHI is considered "individually identifiable" if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone/Fax numbers

- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered "individually identifiable" and; as a result, would not be considered PHI.

Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability. The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Tier 3 – Public	Tier 2 – Internal	Tier 1 – Confidential
Access Controls	No restriction for viewing Authorization by Data	Viewing and modification restricted to authorized	Viewing and modification restricted to authorized

	Owner or designee required for modification; supervisor approval also required if not a self-service function	individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access	individuals as needed for business-related roles Data Owner or designee grants permission for access, plus approval from supervisor Authentication and authorization required for access
Copying/Printing (applies to both paper and electronic forms)	No restrictions	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know Data should not be left unattended on a printer/fax May be sent via LCSD Mail	Data should only be printed when there is a legitimate need Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement Data should not be left unattended on a printer/fax Copies should be labeled “Confidential” Must be sent via Confidential envelope; data should be marked “Confidential”
Network Security	May reside on a public network Protection with a firewall recommended IDS/IPS protection recommended Protection only with router ACLs acceptable	Protection with a network firewall required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data should not be visible to entire Internet May be in a shared network server subnet with a common firewall ruleset for the set of	Protection with a network firewall using "default deny" ruleset required IDS/IPS protection required Protection with router ACLs optional Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless

		servers	networks Must have a firewall ruleset dedicated to the system The firewall ruleset should be reviewed periodically
System Security	Must follow general best practices for system management and security Host-based software firewall recommended	Must follow LCSD-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended	Must follow LCSD-specific and OS-specific best practices for system management and security Host-based software firewall required Host-based software IDS/IPS recommended
Virtual Environments	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Should not share the same virtual host environment with guest virtual servers of other security classifications	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	System must be locked or logged out when unattended Host-based software firewall recommended	System must be locked or logged out when unattended Hosted in a secure location required; a Secure Data Center is recommended	System must be locked or logged out when unattended Hosted in a Secure Data Center required Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	No restrictions	Access restricted to local network or VPN Remote access by third party for technical support limited to authenticated,	Restricted to local network or secure VPN group Unsupervised remote access by third party for technical support

		temporary access via direct dial-in modem or secure protocols over the Internet	not allowed Two-factor authentication recommended
Data Storage	Storage on a secure server recommended Storage in a secure Data Center recommended	Storage on a secure server recommended Storage in a secure Data Center recommended Should not store on an individual's workstation or a mobile device	Storage on a secure server required Storage in Secure Data Center required Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption Encryption on backup media required Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	No restrictions	No requirements	Encryption required (for example, via SSL or secure file transfer protocols) Cannot transmit via e-mail unless encrypted with a password
Backup/Disaster Recovery	Backups required; daily backups recommended	Daily backups required Off-site storage recommended	Daily backups required Off-site storage in a secure location required
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	No restrictions	Recycle Reports; Wipe/erase media	Shred reports Destruction of electronic media
Training	General security awareness training recommended	General security awareness training required Data security training required	General security awareness training required Data security training required Applicable policy and regulation training required

Auditing	Not needed	Logins	Logins, access, and changes
Mobile Devices	Password protection recommended; locked when not in use	Password protected, locked when not in use	Password protected, locked when not in use
Electronic Storage Locations	n/a	n/a	Skyward, NEFEC sftp server, Performance Matters, OneCallNow, Filemaker Pro Server, FLDOE, Achieve3000, Discovery Education, Edgenuity, Hapara, Pearson, Reading Eggs,
Hard Copy Storage Locations	n/a	n/a	Designated Testing Rooms, Storage Vaults, District Server Room, District Storage Room
Downloading	n/a	n/a	Files should only be downloaded on district hardware by authorized personnel and should otherwise meet specifications in the data storage section.

REFERENCES:
Sumter District Schools Network & Instructional Technology Policies & Procedures
Microsoft Security Monitoring and Attack Detection
National Institute of Standards and Technology Information Security (NIST)

Lafayette District Schools
Information and Instructional Technology Services

Appendix G DISASTER RECOVERY PLAN

The purpose of the Disaster Recovery Plan is to ensure a plan is in place and active for continuing operations of the Lafayette District School's Information and Instructional Technology Services in the event of a major hardware or software failure.

Critical applications are considered to be data stored in the Skyward System of the North East Florida Education Consortium (NEFEC), the Active Directory, firewall, and primary switch stack. It is noted the most critical data for continued operation of the Lafayette District School system is the Skyward system and in the event of local equipment loss access to Skyward is available in adjoining school districts. Such access is under the control of the Superintendent and/or School Board of the adjoining district. Should access be denied the resources of the North East Florida Education Consortium will be utilized.

The Active Directory is maintained on two domain controllers allowing for continued login activities in the event of a controller failure. The firewall is recognized as a single point of failure, however we still have the previous model on the shelf in the event our new firewall fails. The primary switch is in a stack of four switches. Should the primary switch fail operations will automatically be assumed by one of the remaining operational switches.

In the event of a natural disaster, the assumption is made that no online testing (CBT) will be conducted, therefore , priority for restoration will be in the following order: (1) Skyward access; (2) email access; (3) Firewall rules; (4) Active Directory; (5) Web content filter; (6) classroom connectivity (connectivity for students cannot be restored until a filtering capability is in place).

For all data stored on servers under the control and/or ownership of Lafayette District Schools, the following procedures will be adhered to.

1. All servers and data equipment located in the Lafayette District Schools Master Data Facility (MDF) will be connected to an uninterrupted power source of a sufficient VA rating to ensure continued operation for a minimum of five minutes. The UPS units will also be connected to an external emergency generator set to automatically come on line after

detection of a power loss lasting longer than 30 seconds.

2. All data located on servers in the MDF will be backed up to a locally hosted storage server (NAS) with backups being conducted as a minimum of once per week. Data being duplicated off site (such as Discovery Education) need not be replicated to an NAS.

3. All programing data for the MDF Firewall, Primary (OSI Layer 3) Switch, Wireless Controller, external DNS, and Active Directory will be copied to a text file and stored off site.

All personnel and student records are part of the Skyward System under control of North East Florida Education Consortium (NEFEC). Disaster recovery for all Skyward data at that facility is the responsibility of NEFEC.

The physical act of recovering data in an emergency will be by all available members of the Lafayette District Schools Information and Instructional Technology Services with assistance from NEFEC personnel as needed or required. Services will be restored based upon the priorities listed above.

REFERENCES:

NIST Contingency Planning Guide for Federal Information Systems

Lafayette District Schools
Information and Instructional Technology Services

Appendix H INCIDENT RESPONSE PLAN

The purpose of this Plan is to establish a rapid response to data security incidents, to improve incident reporting and related communications, to mitigate any potential damages caused by incidents, and to improve overall data security systems.

Lafayette County School District (LCSD) will maintain guidelines and procedures to provide the basis for appropriate responses to incidents that threaten the security, confidentiality, integrity, and/or availability of information assets, information systems, and/or the networks that deliver the information. A Critical Incident Response Team will be maintained to manage security incidents. Data security guidelines and procedures will be reviewed routinely and updated as necessary.

GUIDELINES AND DEFINITIONS

This procedure applies to all information systems and services of the Lafayette County School District (LCSD). An incident is any event that threatens the security, confidentiality, integrity, or availability of LCSD information assets, information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include:

- Unauthorized entry
- Security breach
- Unauthorized scan or probe
- Denial of service
- Distributed Denial of Service
- Malicious code or virus
- Networking system failure (widespread)
- Application or database failure (widespread)
- Others as defined by critical incident response teams

For the purpose of this procedure, **Personal Information** is used as defined in Florida Statute 817.5681(5): "Personal Information" means an individual's first name, first initial and last

name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

(a) Social security number.

(b) Driver's license number or Florida Identification Card number.

(c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Critical Incident Response Team (CIRT) membership could include:

Director of Information Technology (chair)
Director of Financial Services
Student Information Systems Specialist
Instructional Technology Specialist
Technology Aide
School Discipline Officer
Appropriate Personnel from NEFEC

Participation by individual members and other employees will vary by incident as appropriate. Members of the critical incident response team are expected to respond immediately and fully when called upon. Responding to a critical incident, in general, takes precedence over all other work. If a member is unavailable at the time the team is assembled, a substitute member may be named by the chair or the Superintendent.

An incident is deemed critical when so declared by the Superintendent, Director of Information Technology, or Director of Financial Services.

Procedures

Upon discovery or suspicion of an incident, Lafayette County School District employees shall notify the Director of Information Technology in a prompt and effective manner through direct contact, email, or telephone call to ext. 4293.

Within four business hours of receipt of notification or suspicion of an incident, the Director of Information Technology (or designee in the case of absence) will consult with the Superintendent/designee; remove the risk, if possible; and begin an investigation of the incident, including notification to the critical incident response team. The Director of Information Technology will keep a log of all activity related to the investigation.

Within three business days of receipt of notification, the Critical Incident Response Team will formulate a recommendation of whether the incident is critical or noncritical. Factors to be considered in this recommendation include, but are not limited to, whether data was inappropriately accessed, the nature and type of data accessed, and the extent of the data accessed. The CIRT will advise the Superintendent of the recommendation.

If the incident is determined to be non-critical, public notice of the incident is not required, but an appropriate response will be determined by the Superintendent of Schools; the response may include a change in procedure or practice, required training, targeted communications or further inquiry. The Director of Information Technology will submit to the Superintendent a brief description of the incident and the rationale for determining it to be non-critical. The procedures for a non-critical incident end at this step.

If the incident is determined to be critical, the Critical Incident Response team will follow all the below procedures. The team will review the incident, create an overall action plan and formulate an appropriate district or system response; this response may include but is not limited to:

- Selecting which CIRT members should respond;
- Assuming control of and containing the incident; involving appropriate personnel, as conditions require;
- conducting a thorough investigation of the incident, including establishing controls for the proper collection and handling of evidence, and keeping a log of all communications and actions related to the incident;
- protecting the rights of students, employees and others as established by law, regulations, and policies;
- determining whether or not to involve outside personnel, such as legal advice, law enforcement or computer forensic experts;
- drafting statements and materials for public notice as required by State law, including posting an incident report on the LCSB website;

• executing a remediation plan, possibly including repairing/rebuilding any damaged systems and considering any additional remedies for affected constituents;
• recommending any change in procedure or practice, required training, targeted communications or further inquiry;
• monitoring and revising the action plan as needed in the period directly following the incident;
• discussing, reviewing and documenting all actions and results, and particularly any lessons learned from the security breach.

Within four business days of receipt of notification, unless authorized for extended review by the Superintendent or designee, the Critical Incident Response Team will confirm with the Superintendent a preliminary course of action.

In accordance with Florida state law, the Critical Incident Response Team will send a Notification Letter to affected constituents without unreasonable delay. The notification may be provided by one of the following methods:

• direct notice to the constituent's residence,
• telephonic notice directly with the constituent and not through a prerecorded message, or
• electronic notice if address or phone information; electronic notice cannot request personal information and must conspicuously warn constituents not to provide personal information in response to electronic communications regarding security breaches.

The Critical Incident Response Team will conduct a post-incident critique and submit a summary report to the Superintendent including:

• a description of the incident
• a summary of lessons learned
• any suggested changes to existing policies or procedures
• any recommendations to protect against future incidents

Any disciplinary action considered in association with a critical incident shall follow procedures

set forth in the appropriate NCSD Board Rules and the District Student Code of Conduct Handbook.

If determined appropriate and necessary, the notification methods may include the following:

A Press Release will contain the following information:

1. What are you doing?
    Announcing a breach? A theft?
    Announcing that the case has been resolved? That notification has occurred?
2. Who is affected/not affected?
3. What specific types of personal information are involved?
4. What are the (brief) details of the incident?
5. No evidence to indicate data has been misused or what the evidence points to.
6. Expression of regret and concrete steps the District is taking to prevent this from happening again.
7. Major (re)actions taken.
8. Contact information for the District spokesperson for the incident.

A Notification Letter will contain the following components:

1. What happened?
2. When did the breach occur and/or when was it detected?
3. How was it detected?
4. What data was potentially compromised?
5. How much data was compromised?
6. For whom was data compromised?
7. Why you are being notified?
8. What steps are\were being taken?
9. Is any data known to be fraudulently used or is notification precautionary?
10. What steps should individuals take?
11. Apology or statement of commitment to security.
12. Anticipated next steps, if any.
13. Who to contact for additional information.
14. Signature.

An Incident Specific Web Site will contain the following components:

1. Most-recent-update section at top of page.
2. Basic facts (similar to what might appear in a notification letter):
    - Who was impacted
    - What data may have been involved
    - When compromise or discovery occurred
    - Where compromise occurred
    - Whether anyone believed to be negatively affected or not
    - Actions taken by the District to ensure more security in Future/Ongoing measures.
    - What should I do to be sure I'm unaffected?
    - Link to Identity Theft website/credit agencies.
    - FAQs.

In the event of a DDOS attack, we will work with our ISP to reduce the effects of the attack. If it is not quickly brought under control, any time sensitive jobs can be done from home, a local business, or another school district.

References:

--National Institute of Standards and technology
--Nassau County (Florida) School District
--Vermont State Colleges - Data Security Incident Response Procedure, October 5, 2006
--PASCO-HERNANDO Community College – Information Security Incident Response Plan, May 18, 2009
--The College of St. Scholastica - Information Technologies Incident Response Plan, July 17, 2007
--EDUCAUSE – Data Incident Notification Templates

Lafayette District Schools
Information and Instructional Technology Services

Appendix I

TECHNOLOGY EQUIPMENT SIGN-OUT FORM

PROPERTY NUMBER:_____

DATE:_____

This form is used for audit/property accountability. Signing below acknowledges this device is the property of Lafayette District Schools and must be returned to the IT Department if employment terminates for whatever reason.

Employee Last Name: _____ First Name: _____

Home telephone number:_____

Device type:_____

Serial Number:_____

Employee Signature:_____

Date Device Returned:_____

IT Signature Upon Return:_____

Upon return of property indicated on this form, make a copy with all signatures and return the original to employee.