# Personally Identifiable Information (PII)

**Internal Audit Report**

**October 28, 2019**

Orange County Public Schools
Internal Audit

Linda J. Lindsey, CPA, CGAP, Acting School Board Internal Auditor
Luis E. Aponte Santiago, CISA, IT Auditor

# Table of Contents

# EXECUTIVE SUMMARY

## Why We Did This Audit

According to NIST Special Publication 800-122 [1], security breaches involving PII have contributed to the loss of millions of records in recent years. Organizations that suffer breaches involving PII experience loss of public trust, legal liability and remediation costs. Management of PII was rated as a higher risk in the audit risk assessment and this audit was included in the 2019-2020 Annual Audit Plan.

Our objectives in this audit engagement were to:

- Evaluate internal controls over PII where access is provided to district employees and others.
- Determine whether policies and procedures are in place to assure the protection, confidentiality, and reporting of breaches, of PII data.
- Determine whether district personnel are monitoring agreements and procedures for compliance and whether any breaches have occurred and how they have been handled.
- Determine whether a PII data assessment has been performed and, if so, to determine the financial, operational, compliance and reputational impact of any possible loss, disclosure or inappropriate use or modification.

## Observations and Conclusion

| Audit Results at a Glance | | | |
|---|---|---|---|
| | Risk / Impact Rating | | |
| Results and Observations | Significant | Moderate | Minor |
| Source<br>IA - Internal Audit or<br>M - Management | IA - 2 | IA - 2 | IA - 0 |
| Observation Category<br>D - Deficiency or<br>O - Opportunity | D - 2 | D - 2 | D - 0 |

Most of the personnel we interviewed during this audit have some knowledge of what can be considered personally identifiable information.

Most business units have commendable, strong practices for the protection and securing of PII. This can be seen in the controls the schools have on student records, as they have a dedicated lockable room with lockable file cabinets where they store them and they have strong guidelines or in-house rules[2] on how these records should be accessed and managed.

The district's standard agreements and non-disclosure agreements don't have language addressing the protection and handling of personally identifiable information (PII) data.

## Results and Recommendations

We made four recommendations that, when implemented, should significantly improve the district's management of PII and reduce related risks. Those recommendations relate to:

- The need for a district-wide policy on PII
- Training for OCPS personnel on PII.
- The need for an inventory of all PII systems and/or applications.
- The inclusion of appropriate PII language in contract agreements

This report has been discussed with management and they have prepared their response which follows.

[1] Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

[2] All the records should be examined either at that room or school premises. If you took a record out, it should be taken back to the "records vault", as some schools call it.

**DEFINITIONS:**

**Risk / Impact Ratings**

| | |
|---|---|
| Minor | Low risk with a financial impact of less than one percent and/or an isolated occurrence limited to local processes (low impact and low likelihood) |
| Moderate | Slight to moderate risk with a financial impact between one and five percent and/or a noticeable issue that may extend beyond local processes (low impact and high likelihood or high impact and low likelihood) |
| Significant | High risk with a financial impact greater than five percent and/or a significant issue that occurs in multiple processes (high impact and high likelihood) |

**Observations Categories**

| | |
|---|---|
| Deficiency | A shortcoming in controls or processes that reduces the likelihood of achieving goals related to operations, reporting and compliance |
| Opportunity | A process that falls short of best practices or does not result in optimal productivity or use of resources |

**Criteria for Observations Sourced to Management**

- Internal audit was informed of the issue prior to starting detailed testing
- Management identified, evaluated, and communicated the issue to appropriate levels of the district
- Management has begun corrective action with clear, actionable plans and targeted completion dates

None of the observations resulting from this audit were sourced to management.

*None of the observations resulting from this audit were sourced to management.*

**BACKGROUND:**

Personally Identifiable Information (PII) includes, but is not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number;
- Address information, such as street address or email address;
- Personal characteristics, including photographic image (especially of face or other identifying characteristic) fingerprints, handwriting, or other biometric date (e.g., retina scan, voice signature, facial geometry); and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

*PII includes more than one might think.*

The National Institute of Standards and Technology (NIST) has established best practices for PII including collecting, classifying, inventorying, safeguarding and responding to data breaches. NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information was used as criteria for this audit.

*NIST Publication 800-122 was used as criteria for this audit.*

Safeguarding PII against loss, theft or misuse is necessary to comply with laws and regulations,[3] to protect the owners of the PII, and to reduce risks to the district's finances and reputation, among many other reasons. Safeguards can include:

- Administrative safeguards – training personnel on PII best practices;
- Physical safeguards – ensuring paper and electronic records are secured and access is controlled; and
- Technical safeguards – encrypting emails and electronic transmission of data, and requiring user access and login restrictions.

*Safeguarding PII protects the district, its students and their families, employees, vendors, and community members.*

Recovering from a breach can be costly in terms of time spent by key staff coordinating and executing appropriate responses. If a loss of PII constitutes a violation of relevant law, the organization and/or its staff

*Breaches can be costly and damaging to an organization's reputation.*

[3] Florida Statutes 501.171, Security of confidential personal information

may be subject to criminal or civil penalties, or it may have to agree to government scrutiny and oversight. Another risk to organizations is that their reputation could be damaged and public confidence may be lost, potentially jeopardizing the organization's ability to achieve their mission.

Much of the PII we collect is at our schools, which is used for student enrollment. But we also gather PII from our vendors, employees and persons that use our facilities.

*Much of the PII collected by the district relates to students.*

## OBJECTIVES, SCOPE AND METHODOLOGY:

### Objectives

The objectives of this audit were to provide OCPS assurance on the PII data it collects on the following:

- To evaluate internal controls over PII where access is provided to district employees and others.
- To determine whether policies and procedures are in place to assure the protection, confidentiality, and reporting of breaches, of PII data.
- To determine whether district personnel are monitoring agreements and procedures for compliance and whether any breaches have occurred and how they have been handled.
- To determine whether a PII data assessment has been performed and, if so, to determine the financial, operational, compliance and reputational impact of any possible loss, disclosure or inappropriate use or modification.

### Scope

All District departments and systems, excluding the new Student Information System (Skyward) since it was still in an implementation status.

*Our scope included all district departments and systems, excluding the new Student Information System (Skyward) since it was still in an implementation status.*

### Methodology

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal

Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the audit objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

*This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.*

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. We also offer suggestions to improve controls or operational efficiency and effectiveness.

To perform this audit we:

- Surveyed most of the district's business units including 35 schools and 59 individuals in 48 departments under the following functions: Finance, Facilities, Communications, Operations, Human Resources and Employment Services, Chief Academic Office and Deputy Superintendent. We received 88 out of 94 initial surveys sent. A copy of the survey form is at Appendix 1.

*We conducted surveys of most of the district's business units.*

- Interviewed 63 staff at 35 sites which included schools, Finance, Facilities, Communications, Operations, Human Resources and Employment Services, Chief Academic Office, Deputy Superintendent and ITS, and observed handling of PII at those work locations.

*We visited 35 district sites and interviewed 63 employees regarding PII.*

- Reviewed Laws, Regulations and Guidelines regarding PII such as:

    a. Family Education Rights and Privacy Act (FERPA) Regulations
    b. NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
    c. Office of Management and Budget Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information
    d. Office of Management and Budget Memorandum M-10-23: Guidance for Agency Use of Third-Party Websites and Applications
    e. Federal Information Processing Standards (FIPS) Publication 199: Standards for Security Categorization of Federal Information and Information Systems

- Assessed the level of knowledge and awareness regarding PII (site walkthroughs, and follow-up meetings).
- Documented and evaluated processes regarding PII data.

Our audit results and recommendations are in the next section of this report.

*We conducted assessments to determine the level of knowledge and awareness regarding PII (site walkthroughs, and Follow-Up meetings).*

## RESULTS AND RECOMMENDATIONS

**1) There are no district-wide policies and procedures that define PII and provide guidance about how to handle it.** ***Significant Risk / Internal Audit***

Best Practice:
Comprehensive policies and procedures that outline the expectations of management in the classification and safeguarding of PII are essential in meeting requirements and managing associated risks.

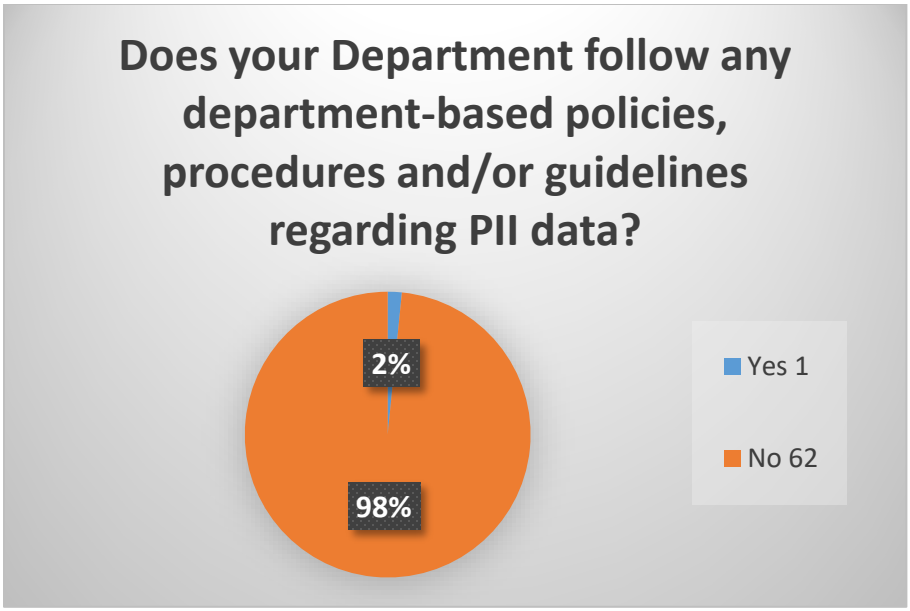
Audit Result:
During our site visits, we asked whether the different business units followed their own approved policies, procedures and/or guidelines regarding the collection, handling, management, storing and disposal of PII data. All interviewed personnel said that they follow the district's School Board Policies and Management Directives regarding the collection, handling, management, storing and disposal of PII data. However, they couldn't identify which School Board Policies and/or Management Directives they followed.

*All interviewed personnel said that they followed the district's School Board Policies and Management Directives regarding the collection, handling, management, storing and disposal of PII data.*

In fact, only one Management Directive comes close to addressing PII. *MD A-15, Employee Responsibility in the Proper Use of Sensitive Data*, is specifically for Social Security Numbers and is derived from School Board Policy CDG, Social Security Number Protection Policy, adopted by the School Board on October 9, 2012.

*Management Directive A-15 is specifically for social security numbers, but does not address the many other forms of PII.*

The chart on the next page summarizes our results with regard to policies and procedures.




Recommendation:

Develop comprehensive, policies and procedures defining PII and outlining the expectations of employees in the control and protection of this data. They should address the classification and safeguarding of PII and provide guidelines for handling a data breach.

*Develop policies and procedures defining PII and outlining expectations of employees.*

**2) OCPS personnel haven't been formally trained on how to manage or handle PII.** ***Significant Risk / Internal Audit***

*There is no PII training.*

Best Practice:

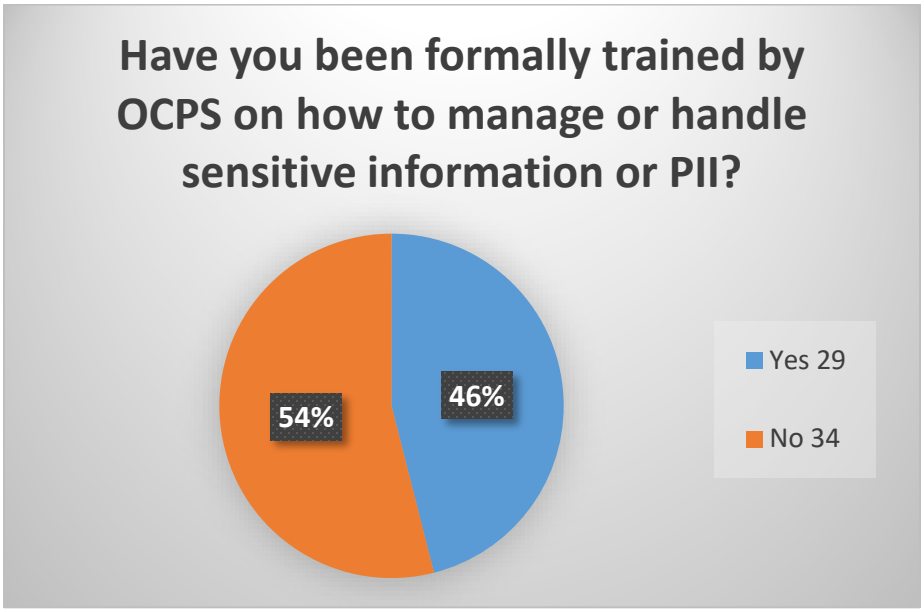
To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals should receive appropriate training before being granted access to systems / records containing PII.

Audit Result:

OCPS personnel haven't been formally trained on how to manage PII. Many had minimal awareness of their responsibility to safeguard PII. One of the schools we visited was using a student as an assistant to work in a room similar to a "records vault", managing folders that contained personal information of other students. Without the proper training and/or experience handling this type of information, errors or

*We observed a student working in a room containing student records that included PII.*

mistakes could expose it. The chart below shows the results of our survey on the subject of PII training.




Recommendation:
Develop and implement training focused on PII with employees attesting to their understanding of PII and the safeguarding requirements. Require annual updates and refresher training as a reminder.

*Develop and implement training focused on PII.*

**3) Compile an inventory of all PII systems and/or applications.**
***Moderate Risk / Internal Audit***

Best Practice:
Keeping an updated inventory of all systems and/or applications that are used to collect personal information and the type of data collected provides management with a wider look of where, what and from whom we are collecting this information.

*One needs to know what systems handle PII in order to manage it properly.*

Audit Result:

At the start of our audit, we requested a list of all systems and processes, manual or electronic that gather, process, or store PII. No such list was available. During the course of our audit, we noted 20 different applications and/or systems that contain PII. Because we did not visit all sites and address every system, the actual list is likely much longer. It is difficult to effectively manage something like PII without knowing where it all is.

*We noted these systems that contain PII:*

- *CampusVue*
- *Carma*
- *Community Meeting*
- *Donor Perfect (CRM)*
- *Formatta*
- *Franklin*
- *iCIMS*
- *MS Excel*
- *MS Outlook*
- *MS Word*
- *MyGov*
- *Qualtrics*
- *QuickBooks*
- *Skyward*
- *SwissMango*
- *Teacher tix*
- *Transfleet*
- *Transit 4 U*
- *Vendorlink*
- *Google Forms/Docs*

Recommendation:

Develop and maintain an inventory list of all PII systems the District uses, requiring the location of the systems, what type of data is collected and what type of system (in-house or third party).

**4) Include PII language in the district's standard agreement template & non-disclosure agreements (NDA).** ***Moderate Risk / Internal Audit***

Best Practice:

Agreements should contain clear definitions of PII and specific responsibilities of the parties that handle it. They should include restrictions on further sharing of the information, requirements for notification to each party in the case of a breach, minimum security controls, and other relevant factors for access to or transfer of PII data. Also, Interconnection Security Agreements (ISA) should be used for technical requirements as necessary. These agreements ensure that the partner organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's PII.

Audit Result:

During the course of the audit, we reviewed the agreement template and NDA that are used when formalizing contracts with vendors and other entities with access to PII. After reviewing both documents we noted that they don't contain specific language for the protection and handling of personally identifiable information (PII) data.

As part of the audit process, we met with the Legal Department and they told us that they use Data Sharing Agreements for entities that will have access to student records. These agreements are required by

FERPA regulations. These Data Sharing Agreements contain appropriate language regarding PII and the responsibilities of the parties as it relates to PII.

Recommendation:
Include in the standard agreements, NDAs and any other templates used to formalize agreement language to clearly establish what type of personal information we want to protect when engaging in a contractual agreement with a vendor or other party.

*Include in the standard agreements and NDAs language to clearly establish what type of personal information we want to protect.*

We wish to thank the many staff members from various schools and departments for the cooperation and assistance we received in the course of this audit.

Appendix 1 – Personally Identifiable Information (PII) Survey



# Personally Identifiable Information (PII) Survey

This survey was developed to obtain an understanding of the client's business environment, organizational characteristics and operating procedures, including a preliminary understanding of the internal controls and information systems controls for the safe management of Personally Identifiable Information (PII) data.

Also, to determine the level of knowledge and awareness of regulations and policies related to management of PII.

* Required

## Respondent Information

We will use this information as a contact reference in case we need more clarification.

1. **Full Name** *

2. **Title or Position** *

3. **Department** *

4. **Business Unit** *

## Survey Questions

These questions were developed to understand, from a departmental point of view, how OCPS collects, manages, stores and disposes of personally identifiable information (PII) data throughout the different business processes it has.

Some areas could perform the same actions as others in terms of handling their PII collection, storing and disposal. It is important to complete this assessment form, so we can have detect well-managed areas and those that need improvement.

If in some of the questions you think that an answer doesn't apply, write N/A (Not Applicable).

If you have any questions regarding this questionnaire, please give us a call at Internal Audit:
Luis E. Aponte Santiago - IT Internal Auditor, EXT. 2002420

5. **#1 - Are you familiar with or have heard about the following government regulations regarding PII?** *

*Check all that apply.*

- [ ] Family Educational Rights and Privacy Act (FERPA)
- [ ] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- [ ] Office of Management and Budget (OMB) Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- [ ] Office of Management and Budget (OMB) Memorandum M-10-23: Guidance for Agency Use of Third-Party Websites and Applications
- [ ] Federal Information Processing Standards Publication (FIPS PUB) 199: Standards for Security Categorization of Federal Information and Information Systems
- [ ] None of the above

6. **#2 - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, has defined PII as, among other things, "any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity". Also included in the SP are various examples of PII data that an organization may collect thru their processes. To your knowledge and working experience, does your department collect any of the following information: a) name, such as full name, maiden name, mother's maiden name, or alias?** *

*Mark only one oval.*

- ◯ Yes
- ◯ No

7. **b) Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number?** *

*Mark only one oval.*

- ◯ Yes
- ◯ No

8. **c) Address information, such as street address or email address?** *

*Mark only one oval.*

- ◯ Yes
- ◯ No

9. **d) Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people?** *

*Mark only one oval.*

- ◯ Yes
- ◯ No

10. **e) Telephone numbers, including mobile, business, and personal numbers?** *
*Mark only one oval.*

- ◯ Yes
- ◯ No

11. **f) Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)?** *
*Mark only one oval.*

- ◯ Yes
- ◯ No

12. **g) Information identifying personally owned property, such as vehicle registration number or title number and related information?** *
*Mark only one oval.*

- ◯ Yes
- ◯ No

13. **h) Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)?** *
*Mark only one oval.*

- ◯ Yes
- ◯ No

14. **#3 - If "Yes" to any options from question #2: what means does your department use to collect the information?** *
*Mark only one oval.*

- ◯ Systems/Applications (Computers, Tablets, Smartphones, or any other device)
- ◯ Manually (Documents/Forms)
- ◯ Mix of both (some Systems/Applications, some Documents/Forms)
- ◯ Not Applicable (do not collect PII data as defined by NIST SP 800-122)

15. **#4 - If you answered "No" to all options from question #2: are you sure that your department does not collect any PII data as defined on the NIST SP 800-122?** *
*Mark only one oval.*

- ◯ Yes
- ◯ No

16. **#5 - If answer to question #3 is "Systems/Applications": what is the name of the system/application used to collect the data? {Make sure you write and spell the correct name of the system/application for each piece of PII data that the department collects: e.g. - Microsoft Word for (type of PII collected); SAP for (type of PII collected); Kronos for (type of PII collected); etc.}** *

17. **#6-a) If answer to question #2 is "Yes" and to question #3 is "Systems/Applications": what is the storage procedure, as per your department and/or business unit, of the PII data collected?** *

18. **#6-b) What kind of controls does your department and/or business unit have in place to ensure the reliability, availability and protection of that PII data gathered through a system/application?** *

19. **#6-c) - What's the procedure, as per your department and/or business unit, on how you dispose of PII data that you no longer use?** *

20. **#7-a) If answer to question #2 is "Yes" and to question #3 is "Manually (Documents/Forms)": what's the storage procedure, as per your department and/or business unit, of the PII data collected?** *

21. **#7-b) What kind of controls does your department and/or business unit have in place to ensure the reliability, availability and protection of PII data gathered manually?** *

22. **#7-c) What is the procedure, as per your department and/or business unit, on how to dispose of PII data that you no longer use?** *

23. **#8 - What do you think the impact on OCPS would be if a PII data breach happens? a) Financial Impact** *

*Mark only one oval.*

- ◯ Low
- ◯ Moderate
- ◯ High

24. **#8-b) Operational Impact** *

*Mark only one oval.*

- ◯ Low
- ◯ Moderate
- ◯ High

25. **#8-c) Compliance Impact** *

*Mark only one oval.*

- ◯ Low
- ◯ Moderate
- ◯ High

26. **#8-d) Reputation Impact** *

*Mark only one oval.*

- ◯ Low
- ◯ Moderate
- ◯ High

| | |
|---|---|
| **Department / School Name** | **ITS, Legal, Teaching and Learning, Procurement Services** |
| **Administrator / Department Head** | Bridget Williams, Chief of Staff; Amy D. Envall, General Counsel; Dale Kelly, Chief Financial Officer; Roberto Pacheco, Chief Operations Officer; Robert Curran, Chief Information Officer |
| **Cabinet Official / Area Superintendent** | |

| Audit Result / Recommendation | Management Response Acknowledgement/ Agreement of Condition | Responsible Person (Name & Title) And Target Completion Date (MM/YYYY) | Management's Action Plan |
|---|---|---|---|
| **1) There are no district-wide policies and procedures that define PII and provide guidance about how to handle it.** ***Significant Risk / Internal Audit***<br><br>Recommendation:<br>Develop comprehensive, policies and procedures defining PII and outlining the expectations of employees in the control and protection of this data. They should address the classification and safeguarding of PII and provide guidelines for handling a data breach. | See attached narrative. | Bridget Williams, Chief of Staff<br><br>Amy D. Envall, General Counsel<br><br>07/2020 | ITS, Legal, Teaching and Learning, and Procurement Services will work together to review the documents governing PII to evaluate which documents need to be updated and to potentially develop a district-wide guidelines regarding the collection, maintenance, retention, and/or disclosure of PII. |
| **2) OCPS personnel haven't been formally trained on how to manage or handle PII.** ***Significant Risk / Internal Audit*** | See attached narrative. | Bridget Williams, Chief of Staff<br><br>Amy D. Envall, General Counsel<br><br>07/2020 | In addition to the regular training that is already conducted by the Office of Legal Services, ITS, Legal, Teaching and Learning, and Procurement Services will work together to develop a district-wide series of training seminars/videos for all employees who work with PII. |

| | | | |
|---|---|---|---|
| Recommendation:<br>Develop and implement training focused on PII with employees attesting to their understanding of PII. and the safeguarding requirements. Require annual updates and refresher training as a reminder. | | | |
| **3) Compile an inventory of all PII systems and/or applications.** ***Moderate Risk / Internal Audit***<br><br>Recommendation:<br>Develop and maintain an inventory list of all PII systems the District uses, requiring the location of the systems, what type of data is collected and what type of system (in-house or third party). | ITS will compile a list of known sites that collect PII data. | Teasha Williams, Sr. Director, ITS Applications, 07/2020 | ITS will work with Teaching and Learning to compile a list of known sites that collect PII data. |
| **4) Include PII language in the district's standard agreement template & non-disclosure agreements (NDA).** ***Moderate Risk / Internal Audit***<br><br>Recommendation:<br>Include in the standard agreements, NDAs and any other templates used to formalize agreement language to clearly establish what type of personal information we want to protect when engaging in a contractual agreement with a vendor or other party. | Procurement Services will collaborate with ITS, Legal Services, Teaching and Learning to draft agreement language for protecting PII. | Robert Waremburg, Senior Director, Procurement Services 07/2020 | Procurement Services will work with ITS, Legal, Teaching and Learning to draft agreement language for PII data and include the drafted language in all of the Procurement related contract template documents. |

Last updated: 1/10/20 ade

**RESPONSE TO #1 AND #2**
**RESULTS AND RECOMMENDATIONS**

**1 ) There are no district-wide policies and procedures that define PII and provide guidance about how to handle it.** ***Significant Risk / Internal Audit***

| Recommendation: |
| --- |
| Develop comprehensive, policies and procedures defining PII and outlining the expectations of employees in the control and protection of this data. They should address the classification and safeguarding of PII and provide guidelines for handling a data breach. |

There are a number of Management Directives, Board Policies, Principles, Florida Statutes, and Procedures provide guidance to employees regarding the handling of personally identifiable information (PII) – which includes both student information and employee information. These documents are all attached to this response.

**A. Management Directives.**

1. **A-15 Employee Responsibility in the Proper Use of Sensitive Data.** This Management Directive, last updated on May 4, 2017, governs the protection of social security numbers (SSNs) and ties directly to Policy CDG State and Federal Programs Administration (Social Security Number Protection Policy).

2. **A-9 Employee Use of Technology**. This Management Directive, last updated on May 4, 2017, governs the use of OCPS computing, network, information, or telephone systems. It specifically addresses electronic communication and requires encryption or secure transport when sending confidential information (including PII) via email.

**B. Board Policies.**

1. **Policy CDG State and Federal Programs Administration.** This policy, last revised on October 9, 2012, is the district's social security number protection policy (the title does not reflect this and should be changed accordingly for transparency purposes). The policy sets forth its purpose, the collection of SSNs from applicants or employees, the collection from students, the collection from volunteers, establishes regulations and procedures, provides notification guidelines, requires superintendent or designee review, and provides for the disclosure of SSNs.

2. **Policy EHBA Records Management (Public Records).** This policy, last revised on May 10, 2016, requires employees to comply with Florida's public records laws and state retention schedules for public records. The policy covers public records and inspection (including PII), retention of public records, responding to a public records request, types of public records requests, right to inspect or copy, coordination of responses to public records requests, fees for duplication, and special services charges. All public records requests are handled by Records Management so that redaction of confidential information (including PII) is consistent.

3. **Policy GBJ Personnel Records.** This policy, last revised on October 11, 2016, governs personnel files and names and address changes of employees. It requires the Superintendent to establish

written procedures for the maintenance of personnel files consistent with the provisions of Section 1012.31, Florida Statutes; these procedures have been established.

4. **Policy JRA Student Records.** This policy, last revised on June 11, 2019, governs the proper use of school records, legal names of students, discipline records, directory information (including PII), person standing in loco parentis to student, access to student records, right to contest the contents of student records, and release of student discipline records. These topics are governed by FERPA and Sections 1000.04, 1002.22, and 1002.221, Florida Statutes.

**C. Principles of Professional Conduct for the Education Profession**. An improper usage of personally identifiable information (PII) may result of discipline up to and including termination of employment. *See* The Principles of Professional Conduct for the Education Profession in Florida, Florida Administrative Code Rule 6A-10.081(2)(a)(9), which requires school personnel to "keep in confidence personally identifiable information obtained in the course of professional service, unless disclosure serves professional purposes or is required by law." A violation of the Principles of Professional Conduct is misconduct in office and just cause for termination.

**D. Florida Statutes.**

1. **Civil Liability**. Section 768.28(9)(a), Florida Statutes, makes employees liable civilly for "bad faith or with malicious purpose or in a manner exhibiting wanton and willful disregard of human rights, safety, or property."

2. **Criminal Liability**. As for criminal liability, Section 815.06(2)(a), Florida Statutes, provides: "A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization or exceeding authorization: Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner of use exceeds authorization;

**E. Other OCPS Procedures and Safeguards of PII.**

1. **OCPS PII Detection Software.** In the event an employee attempts to send PII in an unencrypted message outside the district, an email automatically responds to the employee letting him/her know that ITS Information Security has data loss prevention measures in place which prevent sensitive data from being transmitted in clear text to prevent any unauthorized access from malicious third-parties. An example of an automatic response is contained in the supporting documents attached to this narrative.

2. **Proofpoint**. The OCPS Proofpoint Secure Email FAQ provides employees with information regarding email encryption, why and when employees should encrypt emails, how employees use secure email, how employees encrypt messages, how secure mail recipient will receive encrypted messages, how long encrypted messages are available to a recipient, whether attachments can be sent, whether secure messages will be able to be read on a smartphone, and who employees can contact if they have questions about secure emails.

3. **SecureShare**. The district utilizes SecureShare in order to send large documents that may contain sensitive information (including PII).

4. **Public Records Request Process for Media Inquiries**. This flow chart shows the process by which Media Relations or Records Management respond to requests from the media that may result in the district producing public records responsive to the request that may need to redact confidential or exempt information (including PII).

5. **Guidelines for Managing a Data Breach**. In accordance with Policy EI Insurance Management, the district maintains a specialty risk policy that affects the security and privacy of confidential information whether stored electronically or by paper in the care, custody, and control of OCPS, including OCPS confidential information (including PII). Via an Interoffice Memorandum, dated October 25, 2019, the CIO and the Senior Director – ITS Security provided guidelines and reporting requirements in the event of an incident, threat, demand, or claim seeking remedy and/or alleging liability or responsibility on the part of OCPS from the operations of ITS or OCPS technology or records, no matter the cause.

| Management's Action Plan: |
| --- |
| ITS, Legal, Teaching and Learning, and Procurement Services will work together to review the documents governing PII to evaluate which documents need to be updated and to potentially develop a district-wide guidelines regarding the collection, maintenance, retention, and/or disclosure of PII. |

**2) OCPS personnel haven't been formally trained on how to manage or handle PII.** ***Significant Risk / Internal Audit***

| Recommendation: |
| --- |
| Develop and implement training focused on PII with employees attesting to their understanding of PII. |

There are two (2) categories of PII with which the district routinely is involved – student PII and employee/volunteer PII. All education records (student records) that contain personally identifiable information (PII) are subject to FERPA restrictions on access and disclosure. PII contained in education records can be disclosed with the consent of the parent or eligible student. Otherwise, generally, education records cannot be disclosed without consent of the parent or eligible student. However, an educational agency or institution may disclose PII from an education record without consent, if the disclosure meets one of the exceptions listed in 20 U.S.C. § 1232(g)(b) and (h)-(j) and 34 C.F.R. § 99.31. Employee/volunteer PII is generally handled in accordance with the applicable Florida Statutes and Board Policies, Management Directives, and procedures (see above items outlined in the response to #1).

In addition to those Board Policies, Management Directives, and procedures, there is a great deal of information that can be found by visiting the district's Records Management website located at https://www.ocps.net/cms/one.aspx?pageId=103666. Contained on this site is valuable information regarding public records and student records. Under the District and Personnel Records page, employees and visitors will find information on where to send subpoenas, public records requests, employee records requests, and employment verification requests. Under the Student Records page, employees and visitors will find information on how to request educational records. There are also some FAQs containing instructions and answers to frequently asked questions.

With respect to district-wide training, the Office of Legal Services provides various trainings throughout the year to a variety of groups of employees on public records and FERPA and Information Sharing. For instance, every summer, Principals and Assistant Principals go through legal training on a variety of different topics. The following training documents, containing the materials that were presented by the Office of Legal Services to Principals and Assistant Principals are attached to this response.

**A. 2017 Legal Trainings PowerPoint and Handouts**
**B. 2018 Legal Trainings eBook**
**C. 2019 Legal Training eBook**

In addition to the annual training for Principals and Assistant Principals every summer, the Office of Legal Services provides semi-annual trainings on the handling of student education records (including student PII) to employees involved in the threat assessment team process, the discipline process, and to all registrars and those who deal with attendance records.

Management's Action Plan:
In addition to the regular training that is already conducted by the Office of Legal Services, ITS, Legal, Teaching and Learning, and Procurement Services will work together to develop a district-wide series of training seminars/videos for all employees who work with PII.

Last updated: 1/10/20 ade