DISTRICT OF COLUMBIA
OFFICE OF THE STATE SUPERINTENDENT OF
EDUCATION

Data Incident Response Plan: Policies and Procedures

Updated February 1, 2019

The goal of this document is to define a data incident and establish policies and procedures for OSSE staff and contractors to follow in the event of an unauthorized disclosure or re-disclosure of data. This plan covers any disclosure of confidential data including inadvertent sharing involving personally identifiable information (PII) for which OSSE is responsible as well as when OSSE becomes aware of a data incident committed by a third party for which OSSE is not responsible.[1] This plan addresses OSSE's obligations under DC code and federal law. Whenever confidential information is inadvertently disclosed, there is a risk to the privacy of individuals as well as the agency as a whole. For this reason, this plan is intended to prepare OSSE employees. Our commitment to the protection of and service to DC students, residents and employees compels OSSE to maintain a constant awareness of the trust our work entails.

Definitions

A data incident involving PII occurs when there is suspicion of an unauthorized disclosure, consisting of either a release of or access to PII or other information not suitable for public release.[2] Examples of unauthorized disclosures include but are not limited to:

- Lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.) or hard copy documents that contain PII;
- Unauthorized system access (e.g., an employee leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, poor user management policies, URL hacking, etc.);
- Hackers gaining access to data through a malicious attack;
- Sharing un-redacted documents or data files.

OSSE is responsible for ensuring that its contractors, vendors and any other third parties with access to or receipt of confidential information, including PII, keep this information private and secured. Therefore, this plan applies to data incidents that occur at OSSE or any of the third parties with access to its confidential information. This means a data incident committed by an authorized representative of OSSE is equivalent to OSSE committing a data incident. OSSE staff should be

[1] Generally adapted from SLDS Technical Brief #2 (National Center for Education Statistics, November 2010) and Guide to Protecting the Confidentiality of PII (National Institute of Standards and Technology, April 2010).
[2] PTAC-CL, September 2012, http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf.

aware that any third party data access or sharing requires a contract or data sharing agreement (Memorandum of Agreement, or MOA) that outlines these responsibilities. The *Data Incident at LEAs, CBOs, or associated third parties* section of this plan details OSSE's response when a data incident is committed by a third party for which OSSE is not responsible.

Personally identifiable information (PII) is information that, alone or in combination, can be linked to a specific student, including but not limited to:

- Name of student, parents, or other family members.
- Address of student, parents, or other family members.
- Personal identifier, such as a Social Security Number, unique student identifier (such as OSSE's USI), or biometric record.
- Indirect identifiers, such as date of birth, place of birth, or mother's maiden name.

Aggregate data (for example, at the school, LEA or state level) generally does not include PII. Sometimes, however, the sample underlying aggregate data is so small and/or narrowly-defined that the recipient could easily identify a student from it. Examples include but are not limited to:

- Special education data about a school with only a small number of special education students.
- Certain types of aggregate counts of zero students or percentages of 0 or 100.
- Two separate files that when combined can be used to link information to a student.

Data Incident Management Team

Every data incident reported to OSSE will be investigated by an incident management team including members of DAR, OGC, CIO and OSSE leadership. This team will hold expertise in data systems, legal obligations, organizational management, and strategic planning. The team will also bring in content experts among OSSE staff and contractors as needed. This skill set will allow for both immediate issue resolution and long-term prevention. The responsibilities of this team include maintaining the confidentiality of the individual that reports the incident, as well as recusing team members whose participation might present conflicts of interest in conducting an investigation and determining next steps. For example, any team member from a division being investigated will not conduct internal reviews independent of the incident management team's plan.

Data Incident Response Plan

When there is suspicion of an unauthorized disclosure of PII, the data incident response will consist of four phases:

- Reporting
- Investigation
- Containment
- Notification and Communication

Reporting

If a staff member, OSSE contractor, or authorized representative of OSSE becomes aware of a potential unauthorized disclosure, he/she should report the issue immediately to the incident

management team at OSSE.DataIncident@dc.gov. This alerts the data incident team responsible for leading the confidential investigation into the data incident.

All OSSE staff members and contractors are encouraged to report any known or suspected unauthorized disclosure of PII. [3] The act of reporting allows for OSSE to address any incident internally and strengthen our resolve to best serve DC students by protecting their privacy and data rights.

Reporting on a potential incident will not automatically put an employee at risk of disciplinary action or termination. Per DC Personnel Regulations, an investigation into a data incident will include the intent and scope of the occurrence into account.[4] Self-reporting is the safest and most expedient method of alerting the data incident management team.

Reporting should contain the following elements:

- Summary of incident including
    - Nature of incident
        - e.g. system wide, lost equipment, paper records, electronic document
    - Storage medium from which information was compromised
        - e.g. standalone document/spreadsheet, technical equipment like flash drive or computer, or access to a secure data storage system
    - Description of information suspected to be lost or compromised, including the number of affected records
    - Source of the data involved (if known)
        - e.g. data software including name of system and possible interconnectivity with other systems
    - Actions taken since the incident discovery
        - e.g. Lost item is found, remote log off, system suspension, data spread further
    - Any additional information relevant to the incident
        - e.g. the disclosure has (not) been accessed outside of OSSE, the media was alerted, LEA has taken steps to alert others
- Date and time incident was discovered
- Date and time incident happened (if known)
- Best contact information of person reporting the incident
    - e.g. phone or email

Because the investigation is confidential, the staff member should not share the details of the incident until the investigation is completed. This includes any solicited communication from LEAs, the media, or additional staff members or contractors. See Appendix A for examples of data incident reports.

[3] 34 CFR §99.32
[4] DC Personnel Regulations 1607.2(a)(10)

Investigation

Reporting of a data incident will trigger an investigation to determine whether an unauthorized disclosure occurred. If the investigation concludes that there was not an unauthorized disclosure, the findings will be documented for future reference but no further action will be taken.

If the investigation reveals that an unauthorized disclosure occurred, the data incident team will take steps to contain the unauthorized disclosure (see below) while simultaneously documenting the data incident, including:

- When and how the incident occurred
- Who was involved in the disclosure, including internal staff and recipients
- Size and implications of the impact of the incident
- Scope of the incident, including containment and cataloging the lost data

Containment

As immediately as possible after learning of an unauthorized disclosure, the data incident team will determine the containment strategies which may include:

- Shut down applicable systems sharing data internally and externally to ensure no further disclosure
- Notify the entities / individuals that improperly received PII with information about their affirmative responsibility to destroy the data
- Determine responsibilities within any existing data sharing agreement that may pertain to the data and systems involved

Notification and Communication

Based on the investigation and a review of District law and policies, the data incident team will collaborate with appropriate members of OSSE's leadership team when an unauthorized disclosure has occurred to:

- Establish any necessary communication plans to keep those impacted by the incident informed
- Decide what notification about the disclosure to provide and to whom, including:
    - Contents of such notification
    - Means of notification
    - Whether public outreach is needed
- Involve the OAG and Office of the Mayor at designated intervals
- Establish hotlines for the public to remain informed
- Create credit monitoring systems for individuals who experienced information exposure
- Utilize existing and create new containment and response tools to address the incident immediately

Notification to LEAs, CBOs and other third parties will be determined after the investigation identifies whether any data were exposed and the extent of data exposure. The results of the investigation will conclude with a set of recommended practices to prevent a similar incident from occurring in the future.

Policy Resources

Training and Awareness

All OSSE staff and contractors receive training about the requirements of protecting PII, clear guidance about what constitutes a data incident involving PII, and what protocols to follow in the event of a suspected or known incident.

Agencywide policy governing access to PII

OSSE currently has the following policies about access to PII:

- OSSE Secure Data Transfer with Box
- FOIA Request Process Overview
- Accessing Student Education Records
- OSSE and Federal Privacy Laws

Federal Policy

While the Family Educational Rights and Privacy Act (FERPA) does not contain specific incident notification requirements, it protects the confidentiality of education records by requiring recordation of each incidence of data disclosure.

Pursuant to §99.67 of the FERPA regulations, if the U.S. Department of Education issues a final agency decision that a third party has re-disclosed PII from education records in violation of FERPA, or has failed to provide the notification required under §99.31(a)(9)(ii) pursuant to §99.33(b)(2) of the FERPA regulations, the state will adhere to the FERPA guidance to not allow the third party or individual team members, as appropriate, access to PII from education records for at least five years.

Data Incident at LEAs, CBOs, or other third parties

Staff members may become aware of unauthorized disclosures that occur within a local education agency, community-based organization, or other third parties. Should an OSSE staff member become aware of such an unauthorized disclosure, they are encouraged to report that to the data incident management team at OSSE.DataIncident@dc.gov who will document the unauthorized disclosure and provide assistance and resources to prevent future incidents. OSSE does not hold specific responsibilities for data incidents that occur outside of agency staff, contractors or vendors. However, as data stewards within the District, OSSE will take steps to assist in any incident involving student data.

For More Information

OSSE staff may contact OSSE.DataIncident@dc.gov for additional information on the technical processes that support this policy.

Appendix A: Data Incident Report Examples

Equipment Loss

1. Nature of incident: Lost Equipment
2. Storage medium: OSSE laptop (assigned to ---- Employee) last seen with Windows access locked, was located within (1050 First St. room 427)
3. Description of Information: Computer holds the following:
    a. Access to the – Drive
    b. Documents with Student PII saved on the C drive (including desktop)
    c. Employee currently logged into: Outlook, Google Drive, PeopleSoft, SLED, and XYZ QuickBase Application
4. Data Source: NA
5. Actions taken since the incident discovery: Lost item was discovered by a non-employee and delivered to the front office on the 3rd floor at approximately 3 p.m.
6. Any additional information relevant to the incident: It is unknown if the computer has been accessed by anyone in the time it was lost.
7. Date and Time Discovered: 1/1/2017, 1:30 p.m.
8. Date and Time Occurred: 1/1/2017, window between 1 p.m. and 1:30 p.m.
9. Contact Info of Reporter: John.Smith@dc.gov, 202-xxx-xxxx

Standalone Document

1. Nature of incident: Single electronic document
2. Storage medium: Excel spreadsheet without password protection or redactions was emailed to (123) LEA.
3. Description of Information: Spreadsheet document has aggregate data on (987) LEA including the following elements:
    a. Demographic Enrollment Breakdown
    b. PARCC Assessment Scores by Grade Level
    c. Attendance Records
4. Data Source: Unknown
5. Actions taken since the incident discovery: Team supervisor was alerted
6. Any additional information relevant to the incident: This email was forwarded from the LEA POC to the Head of School, which subsequently led to an email back to OSSE.
7. Date and Time Discovered: 1/1/2017, 10 a.m.
8. Date and Time incident occurred: 1/1/2017, 10 a.m.
9. Contact Info of Reporter: John.Smith@dc.gov, 202-xxx-xxxx

Systems Permission

1. Nature of incident: Systemwide
2. Storage Medium: Password to (XYZ) QuickBase Application was compromised and unauthorized access was granted
3. Description of information: (XYZ) QuickBase application stores X thousand individual records of student-level data. The records include the following elements:
    a. First and Last Name
    b. USI
    c. Date of Birth
    d. Enrollment status

    e. Student Address
4. Data Source: (XYZ) QuickBase application pulls from the following sources:
    a. LEA SIS Feeds
    b. ABC data set
5. Actions taken since the incident discovery: XYZ QuickBase application has not been suspended.
6. Any additional information relevant to the incident: The media was alerted that the password was compromised by a third party (NAME).
7. Date and Time discovered: 1/10/2017, 10 a.m.
8. Date and Time incident occurred: 1/9/2017, 11:59 p.m.
9. Contact Info of Reporter: John.Smith@dc.gov, 202-xxx-xxxx