Department of Education

Internal Audit

Student Information Privacy Review

Issue Date: October 2013

Report Number: FY2014-01

Department of Education
Student Information Privacy Review

Executive Summary

AUDIT OF:	**DATE:**	**AUDIT RATING:**
Student Privacy	Fieldwork performed July 2013 – September 2013	Acceptable **[X]** Marginal **[ ]** Unacceptable **[ ]**

INTRODUCTION:

In connection with the Department of Education's (DOE) Re-Assessment of Risk Assessment and Internal Audit Plan approved on June 4, 2013, Internal Audit (IA) performed a *"Student Information Privacy Review."* This project was formerly known as Information Technology Privacy Review – Student Data. However, after preliminary analysis of DOE policies and procedures, IA decided to widen the scope and change the title to Student Information Privacy Review. The purpose of this review was to evaluate the adequacy of DOE's ability to meet its privacy commitments and stated practices in accordance with generally accepted privacy principles (GAPP) and to determine the DOE's adherence to the Family Educational Rights and Privacy Act (FERPA) and DOE policies and procedures.

BACKGROUND:

As stated in the Generally Accepted Privacy Principles, privacy is defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information." Any data that can be used to identify a person either directly or indirectly is considered personal information. Examples of personal information include, but are not limited to the following: name, gender, date of birth, home address, personal telephone number, government identifier, and behavioral information. Proper privacy protection can mitigate numerous risks to the DOE, some of which include:

- Possible damage to the organization's public image and branding.
- Potential financial losses.
- Legal liability and industry or regulatory sanctions.
- Charges of deceptive practices.
- Customer, citizen, or employee distrust.
- Damaged business relationships.

To protect the privacy of families whose children are in school, the federal government established legal statues to keep student information private. In addition to personal information, education agencies such as the DOE must also be cognizant of education records. According to the National Center for Education Statistics, "education records contain the administrative reports of students' educational progress, along with any information about past or current use of school-related services, such as special education, social work services, or other supplementary educational support. An education record is a compilation of records, files, documents, and other materials that contain information directly related to a student and maintained by education agencies or institutions, or individuals acting on behalf of the agencies."
The main office involved with student information privacy is the Data Governance Office (DGO). DGO, under Superintendent's office, provides support to the Hawaii State Department of Education as it relates to the development, implementation, facilitation, and efficient administration of grants, research, the K-12 Longitudinal Data System (LDS), and data use. In addition, DGO provides guidelines, training opportunities, support materials, and technical assistance on the acquisition, storage, use, and release of data and information, including but not limited to: security, privacy, and FERPA; ethical use; quality control; records retention; and process definitions and maps. Also, DGO conducts onsite visits as part of their annual monitoring, 10 schools were visited in SY 2011-2012.

Executive Summary

SCOPE and OBJECTIVES:

The scope of our review included an examination of the student information privacy process. We reviewed the design and operating effectiveness of the existing control procedures in place over the management, notice, choice and consent, collection, access, disclosure, quality, and monitoring of student privacy. The scope of our review specifically focused on the processes related to the following acts:

- Family Educational Rights and Privacy Act (FERPA);
- Health Insurance Portability and Accountability Act (HIPAA)

The scope of the detailed testing covered beginning of school year (SY) 2013-14 up to fieldwork date. For on-site school visit monitoring, one (1) school from each complex for a total of 16 schools were selected. Some schools selected for testing included those that had undergone SY 2012-2013 monitoring and site visits performed by DGO with findings, as well as those with FERPA issues reported in the DOE. In addition, other schools were randomly selected for complexes which had no prior issues reported during SY2012-2013. For detailed compliance testing, we randomly selected 7 schools from each complex for a total of 105 schools. We also randomly selected 8 state offices for detailed compliance testing.

This review excluded detailed testing for public charter schools.

The objectives of our review included the following:

1. To determine inherent and residual privacy-related risks in the DOE.
2. To provide assurance on controls over privacy risks.
3. To verify adherence with a set of privacy standards or regulations.
4. To ensure compliance with the DOE's own privacy statement on the use, collection, retention, and protection of student information.

OBSERVATIONS:

Based upon our review, we found the DOE's controls related to student information privacy are functioning at an "acceptable" level. An acceptable rating indicates that no significant deficiencies exist, while improvement continues to be appropriate; controls are considered adequate and findings are not significant to the overall unit/department.

Please refer to the Risk Ratings section of this report for a complete definition of the ratings used by IA and the Observations and Recommendations section for a detailed description of our findings.

We discussed our preliminary findings and recommendations with management and they were receptive to our findings and agreed to consider our recommendations for implementation.

Each observation presented in this report is followed by specific recommendations that will help to ensure that control gaps are addressed and, if enforced and monitored, will mitigate the control weaknesses. In summary, our observations are as follows:

1. Lack of understanding of privacy practices with third-party vendors by school staff.
2. Procedures are not always followed at the DOE school/office level and required forms and supporting documentation are not completed and/or retained.
3. Process inefficiencies resulting from unclear interpretation of 'opt out' forms.

PLANNED FOLLOW UP BY MANAGEMENT AND INTERNAL AUDIT:

IA will follow up with management on their progress of completion for their action plans, and report accordingly through the audit committee quarterly updates.

Rating Scale Definitions

OVERALL RATING SCALE	
Acceptable	No significant deficiencies exist, while improvement continues to be appropriate; controls are considered adequate and findings are not significant to the overall unit/department.
Marginal	Potential for loss to the auditable unit/department and ultimately to the DOE. Indicates a number of observations, more serious in nature related to the control environment. Some improvement is needed to bring the unit to an acceptable status, but if weaknesses continue without attention, it could lead to further deterioration of the rating to an unacceptable status.
Unacceptable	Significant deficiencies exist which could lead to material financial loss to the auditable unit/department and potentially to the DOE. Corrective action should be a high priority of management and may require significant amounts of time and resources to implement.

OBSERVATION RATING SCALE	
High (1)	1 - The impact of the finding is ***material***[1] and the likelihood of loss is probable in one of the following ways: • A material misstatement of the DOE's financial statements could occur; • The DOE's business objectives, processes, financial results or image could be materially impaired; • The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are material to the DOE's financial performance, operations or image. *Immediate action is recommended to mitigate the DOE's exposure*
Moderate (2)	2 - The impact of the finding is ***significant***[1] and the likelihood of loss is possible in one of the following ways: ➢ A significant misstatement of the DOE's financial statements could occur; ➢ The DOE's business objectives, processes, financial performance or image could be notably impaired; ➢ The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are significant to the DOE's financial performance, operations or image. *Corrective action by management should be prioritized and completed in a timely manner to mitigate any risk exposure.*
Low (3)	3 – The impact of the finding is moderate and the probability of an event resulting in loss is possible. *Action is recommended to limit further deterioration of controls.*

[1] The application of these terms are consistent with the guidelines provided by the Institute of Internal Auditors

Observations

The detailed observations noted herein were based on work performed by IA through the last date of fieldwork and are generally focused on internal controls and enhancing the effectiveness of processes for future organizational benefit.

Observations

Observation Number: 1	
Observation: Lack of understanding of privacy practices with third-party vendors by school staff.	**Rating: Moderate**

Based on the review performed and discussions with DGO, we found that schools do not consult regularly with Data Governance or Enterprise Systems Branch (ESB) for approval when contracting with third-party vendors. ESB, under the Office of Information Technology Services, is responsible for designing, developing, implementing, and supporting the core student information, operational applications, and enterprise resource planning of the public school system. Therefore, these contracts may not contain sufficient data security and privacy requirements.

DOE Memo on *Small Purchase Contracts Involving the Release of Hawaii Department of Education Data* states that all small purchase contracts involving the release of personally-identifiable student information to a vendor must specify that the vendor's use of the data will comply with all regulatory guidance of FERPA. The memo states, "the contract must specifically state which data are to be released; the purposes for which the data is to be used and that the use will not exceed those limitations; who will have access; how the security of the data will be maintained; and when all files in all forms containing the personally-identifiable information will be destroyed by the vendor."

Based on our on-site school visit monitoring testing, nine (9) out of 16 schools did not have the appropriate language in their contract stating proper privacy requirements. Based on responses to the questionnaire sent to the field, five (5) out of 63 schools stated that they do not make third party vendors sign confidentiality agreements when contracting with vendors that may have access to student information. All five (5) schools did not consult with DGO when contracting with those vendors.

In addition, based on discussions with schools, registrars, clerks, and School Administrative Services Assistants (SASA) have indicated confusion over what constitutes a "third-party" vendor and therefore, were not aware that a completed consent form for the release of personal information with these third-party vendors is required.

Impact

The lack of clarity and communication of privacy practices may lead to:

- Services provided by third party vendors to schools may not follow privacy guidelines.
- Schools are exposed to privacy risks from third party vendors.
- Possible damage to the organization's public image.
- Penalties for policy violations.
- Unauthorized release of student information may result in litigation and loss of funds to DOE.

Recommendation

Recommendations to address the lack of clarity and communication of privacy practices with third-party vendors include:

- Management should provide guidance that is 'clear to all' on what constitutes a third-party vendor and provide examples of when consent forms are required.
- Management should pursue feasibility of incorporating warnings or reminders within FMS for users processing purchase orders or small purchase contracts for specified Object Codes linked to related services.

Observations

- Management should create standardized templates for schools to complete/follow when contracting with third-party vendors that require access to student information and provide training.
- Training should also provide guidance to registrars, clerks, and SASAs on third party privacy practice requirements.
- Create a Memorandum of Agreement (MOA) or a Memorandum of Understanding (MOU) with frequently used third-party vendors to protect the entire DOE versus having each school include FERPA requirements in each school's respective contracts.

Management Plan

HIDOE welcomes the opportunity to clarify the conditions associated with releasing student data to vendors. Within the prior two years, HIDOE has instituted a required and annual Information Security and Privacy training for all principals and vice principals which includes a module on contracts involving data sharing. Concurrently, the Data Governance Office has conducted random monitoring of the implementation of HIDOE guidelines. Based on the results of the monitoring, the Data Governance Office has provided direct assistance to HIDOE schools and offices to promote the use of best practices.

The Data Governance Office will work with the Office of Fiscal Services to expand the annual required procurement training to include guidance regarding the release of student information to vendors. The revisions to include information pertaining to releasing student information to vendors will be completed by June 30, 2014.

The Data Governance Office will conduct a feasibility assessment to determine if warnings or reminders can be incorporated within FMS for users processing purchase orders or small purchase contracts for specified Object Codes linked to related services. The feasibility assessment will be completed by June 30, 2014.

The Data Governance Office will expand monitoring activities to include reviews of purchase orders and small purchase contracts with vendors whose services require access to student information. A plan to monitor randomly selected organizational units during School Year 2014-15 will be available by July 15, 2014.

The Data Governance Office will confirm standard language added to the special conditions to clarify the requirement of data sharing agreements for contracts that involve the release of student information to vendors. The confirmation will occur by December 31, 2013.

The Data Governance Office will continue to develop and provide resources, such as data sharing agreement templates. Direct assistance will be provided to DOE personnel to develop MOUs that involve data sharing with vendors.

Contact Person: Christina Tydeman, Director, Data Governance Office

Anticipated Completion Date: September 2014

Responsible Manager

Christina Tydeman

Observations

Observation Number: 2

Observation: Procedures are not always followed at the DOE school/office level and required forms and supporting documentation are not completed and/or retained. **Rating: Moderate**

DOE schools are required to follow student information privacy policies and procedures. The following are non-compliance with federal requirements summarizing the frequency in which forms related to student privacy are completed and/or retained. Further details are provided in the Reference column.

Reference(s)	Summary of Observations Noted
Non-Disclosure of Information (Opt Out) Form (Form RS 12-1055)	
➢ *Notice of Rights under FERPA for Elementary and Secondary Schools* states that parents have "the right to provide written consent before the school discloses personally identifiable information contained in the student's education records." In addition, the *Notice of Directory Information* gives an explanation on how to "opt out" or request non-disclosure of student information.	➢ 10 out of 49 student records did not contain the "Non-Disclosure of Information (Opt Out)" form when "Release of Information Codes" was indicated in the Student Information System (eSIS).
Access Logs/Request Form	
➢ Based on the FERPA training video, schools should adopt a policy for record inspection including verifying parent identity and developing a request form for parents to complete and sign. At minimum, the form should include names of the parent and the student, a description, an itemized list of records that were reviewed, and the date the review was conducted and completed.	➢ Five (5) out of 16 schools selected for on-site school visit monitoring testing did not keep an access log/request form for record inspection. ➢ Based on responses to the questionnaire sent to the field, two (2) out of 63 schools stated that they do not ask for identification when parent/legal guardian/etc. request to access student information. ➢ Based on responses to the questionnaire sent to the field, 26 out of 63 schools stated that they do not keep an access log/request form for record inspection.

Observations

In addition, DOE schools are required to follow internal DOE policies and procedures. The following table summarizes the frequency in which forms related to student privacy are completed and/or retained. Further details are provided in the Reference column.

Reference(s)	Summary of Observations Noted
FERPA Video Viewing Confirmation Form/FERPA Brochure Receipts & Review Confirmation Form (Form RS 12-1055)	
➢ DOE Memo on *Family educational Rights and Privacy Act (FERPA) Training* states that all individuals working in a school, complex area, or state office are required to receive FERPA training and sign a confirmation form on an annual basis.	➢ 16 out of 64 employees selected for testing did not have a signed "FERPA Video Viewing Confirmation Form"/"FERPA Brochure Receipt & Review Confirmation Form" on file at the respective schools. ➢ Two (2) out of eight (8) branches/offices selected for detailed testing did not have signed "FERPA Video Viewing Confirmation Form"/"FERPA Brochure Receipt & Review Confirmation Form" on file at the respective branches/offices. ➢ Two (2) out of 16 schools selected for on-site school visit monitoring testing had a group signing of all the employees indicating that they've received the "Opening of the School Year Packet". However, no individual FERPA training forms were signed.
Acknowledgement of General Confidentiality Expectations Form (Form RS 12-1055)	
➢ DOE Memo on *General Confidentiality Notice – REVISED 4/29/13* states that all employees, and all new employees upon hire, are expected to read and sign the Acknowledgement of General Confidentiality Expectations.	➢ 14 out of 64 employees selected for testing did not have a signed "Acknowledgement of General Confidentiality Expectations" form on file. ➢ Two (2) out of 16 schools selected for on-site school visit monitoring testing had a group signing of all the employees indicating that they've received the "Opening of the School Year Packet". However, no individual confidentiality notices were signed.

Observations

Reference(s)	Summary of Observations Noted
Annual Notification of Privacy Rights (Poster)	
➢ DOE Memo on *Distribution and Use of Posters and Bookmarks Notifying Parents, Guardians, and Eligible Students of their Privacy Rights and Distribution of FERPA Brochures for School Staff and Volunteers Training* states that annual notification of privacy rights must be posted in clearly visible locations in their administrative offices and other public places within and around their schools.	➢ Two (2) out of 16 schools selected for on-site school visit monitoring testing did not have the Privacy Rights Poster displayed in a clear, visible location in the school's administrative office.
Annual Notification of Privacy Rights (Newsletter)	
➢ DOE Memo on *Distribution and Use of Posters and Bookmarks Notifying Parents, Guardians, and Eligible Students of their Privacy Rights and Distribution of FERPA Brochures for School Staff and Volunteers Training* states that annual notification of privacy rights must be in their newsletters.	➢ Three (3) out of 16 schools selected for on-site school visit monitoring testing did not have the privacy statement on the newsletter nor was the privacy statement sent to parents via different venues. ➢ Two (2) out of 16 schools selected for detailed testing did not have the privacy statement on the newsletter nor was the privacy statement sent to parents via different venues. ➢ One (1) out of 16 schools selected for detailed testing did not have the standard privacy statement on the newsletter. Instead, the school created its own statement for the newsletter.
Annual Notification of Privacy Rights (Website)	
➢ DOE Memo on *Annual Notification of Privacy Rights* states that all schools must copy and post the annual notification of privacy rights prominently on the front page of their school websites.	➢ 22 out of 105 schools selected for detailed testing did not have the annual notification of privacy rights on the respective school's website. ➢ Four (4) out of 105 schools selected for detailed testing did not have the annual notification of privacy rights stated on the front page of the respective school’s website.

Observations

Reference(s)	Summary of Observations Noted
Annual Notification of Privacy Rights (Brochure)	
➢ DOE Memo on *Distribution and Use of Posters and Bookmarks Notifying Parents, Guardians, and Eligible Students of their Privacy Rights and Distribution of FERPA Brochures for School Staff and Volunteers Training* states that Privacy Rights bookmarks and brochures should be available for general distribution.	➢ One (1) out of 16 schools selected for on-site school visit monitoring testing did not have the Privacy Rights brochures available for general distribution.
Training and Compliance	
➢ DOE Memo on *Family Educational Rights and Privacy Act (FERPA) Training* states that all individuals are required to view the FERPA training video prior to commencement of service every fifth calendar year. During the non-fifth calendar years, the employees have the option of reading the FERPA brochure and signing a statement acknowledging that the FERPA information was received and read.	➢ Based on responses to the questionnaire sent to the field, one (1) out of 63 schools stated that the SASA does not think that the school is in compliance with FERPA guidelines. ➢ Based on responses to the questionnaire sent to the field, eight (8) out of 63 schools stated that they do not feel that they are provided with adequate policies and procedures and training on FERPA requirements.

These observations indicate a lack of understanding of FERPA and its related policies and procedures. IA spoke to numerous SASAs, registrars, and administrators and they were not aware that they had to complete and/or submit certain forms and supporting documents or follow certain procedures. Based on discussions with DGO, although online training is available, schools can request "live" training.

Information on student privacy is documented on the DOE website as well as the DOE FERPA website at http://ferpa.k12.hi.us. The websites are public and accessible to all including employees, students, parents, legal guardians, etc. Forms and training documents are also available on the FERPA website and are accessible to all DOE employees. In addition, periodic DOE memos are sent to the field for changes, updates, and reminders through DOE Memos and Notices on Lotus Notes.

Impact

Student privacy procedures were designed to include internal controls to mitigate risks that may violate student privacy rights. There is an increase in risk exposure when designed procedures are not followed. Specifically:

- Release of student information without authorization by parents may result in deterioration of relationships between parents and the school.
- Unauthorized access to confidential information by employees.
- Parents are not informed of their rights regarding student privacy.
- Invalid/incorrect data collected for students.

Observations

- Possible violation of FERPA guidelines may result in termination of eligibility for the DOE to receive funding.
- Inconsistent application of policies and procedures.

Recommendation

Recommendations for the observation regarding procedures not followed at the DOE school/office level and required forms and supporting documentation not completed and/or retained include:

- Management should hold schools accountable for following proper procedures by expanding annual on-site monitoring of compliance to DOE procedures pertaining to student information privacy.
- Management should enforce the proper completion of forms.
- Periodic spot checks should be conducted by someone outside the schools to ensure that proper student privacy procedures are followed (i.e. Complex Area Business Managers, staff in DGO, Administrative Services Assistants, etc.).
- Training should be provided to registrars, account clerks, and SASAs regarding privacy guidelines.
- Management should clarify policies and procedures to cover steps to take when parents request to access student information.
- Management should create standardized templates for schools to complete (i.e. standardized access logs/request forms).
- Management should create a 'quick reference checklist' noting all the DOE requirements and due dates regarding schools' role in complying with FERPA guidelines (i.e. "Annual Notification of Privacy Rights" should be posted on school's website and in school's newsletter; Privacy Rights bookmarks and brochures should be distributed to all students; Privacy Rights poster should be posted; etc.)

Regarding Acknowledgement of General Confidentiality Expectations Form and FERPA Training Forms:

- Management should clarify that signing for the "Opening of the School Year Packet" does not suffice and that each employee still has to sign the "Acknowledgement of General Confidentiality Expectations" form and the "FERPA Video Viewing Confirmation Form"/"FERPA Brochure Receipts & Review Confirmation Form".
- Management should clarify FERPA training memo to state that ALL EMPLOYEES must receive FERPA training and sign a confirmation form on an annual basis.

Management Plan

The Data Governance Office will expand annual on-site monitoring of compliance to DOE procedures pertaining to student information privacy. A plan to monitor randomly selected organizational units during School Year 2014-15 will be available by July 15, 2014.

The Data Governance Office will expand annual virtual monitoring of compliance to DOE procedures pertaining to FERPA training compliance and confidentiality. A plan to monitor randomly selected organizational units during School Year 2014-15 will be available by July 15, 2014.

The Data Governance Office will conduct periodic spot checks of complex area processes to ensure that proper student privacy procedures are followed by the complex area schools. The spot checks will begin no later than February 28, 2014.

Observations

The Data Governance Office will include specific training pertaining to documentation of parental requests to access student information in the annual Information Security and Privacy training beginning in July 2014.

The Data Governance Office will revise and redistribute standardized templates for schools to complete (i.e. standardized access logs/request forms) by July 15, 2014.

The Data Governance Office will create and distribute a 'quick reference checklist' noting all the DOE notification requirements and due dates by July 15, 2014.

Beginning in July 2014, the Data Governance Office will require evidence that all employees individually signed the "Acknowledgement of General Confidentiality Expectations" and the "FERPA Video Viewing Confirmation Form"/"FERPA Brochure Receipts & Review Confirmation Form" during the annual confidentiality monitoring.

Contact Person: Christina Tydeman, Director, Data Governance Office

Anticipated Completion Date: September 2014

Responsible Manager
Christina Tydeman

Observations

Observation Number: 3	
Observation: Process inefficiencies resulting from unclear interpretation of 'opt out' forms.	**Rating: Low**

DOE Memo on *Annual Notification of Privacy Rights* states that "requests to withhold directory information must be made via a signed, legibly written request. The written request must contain the school name, student's name, date of birth, and must specify that the directory information should not be disclosed. Should a parent, guardian, or eligible student request a form to complete in order to serve as a written request, a copy of the attached form ["Non-Disclosure of Information Form"] must be available".

Based on the on-site school visit monitoring testing, IA noted seven (7) out of 16 schools distributed "Non-Disclosure of Information (Opt Out)" forms to all parents at the beginning of the school year. As a result, hundreds of completed opt out forms were returned to each school. Those schools then entered all the opt out information into eSIS and filed each form into the respective student's cumulative folder. According to those schools, this effort is very time consuming.

It appears that some schools are doing more work than necessary. Opt out forms are not required to be given out to all parents. The only requirement is that the forms are available should it be requested.

Impact

Complete distribution of opt out forms may lead to process inefficiencies and inconsistencies in following policies and procedure. Distribution of forms could create confusion which may result in erroneous selection of opt out options by parents/legal guardians/eligible students. Such inefficiencies result in wasted resources and financial loss to the DOE.

Recommendation

In order to improve controls of procedures related to the complete distribution of opt out forms, we recommend that management should clarify that complete distribution of opt out forms is not a requirement and that communication of annual notification of privacy rights is sufficient.

Management Plan

Beginning in July 2014, the Data Governance Office will monitor distribution of opt out forms during on-site visits and provide direct guidance to schools found to be distributing the forms in error.

Contact Person: Christina Tydeman

Anticipated Completion Date: September 2014

Responsible Manager

Christina Tydeman

Acknowledgements

We wish to express our appreciation for the cooperation and assistance afforded to the review team by management and staff during the course of this review.