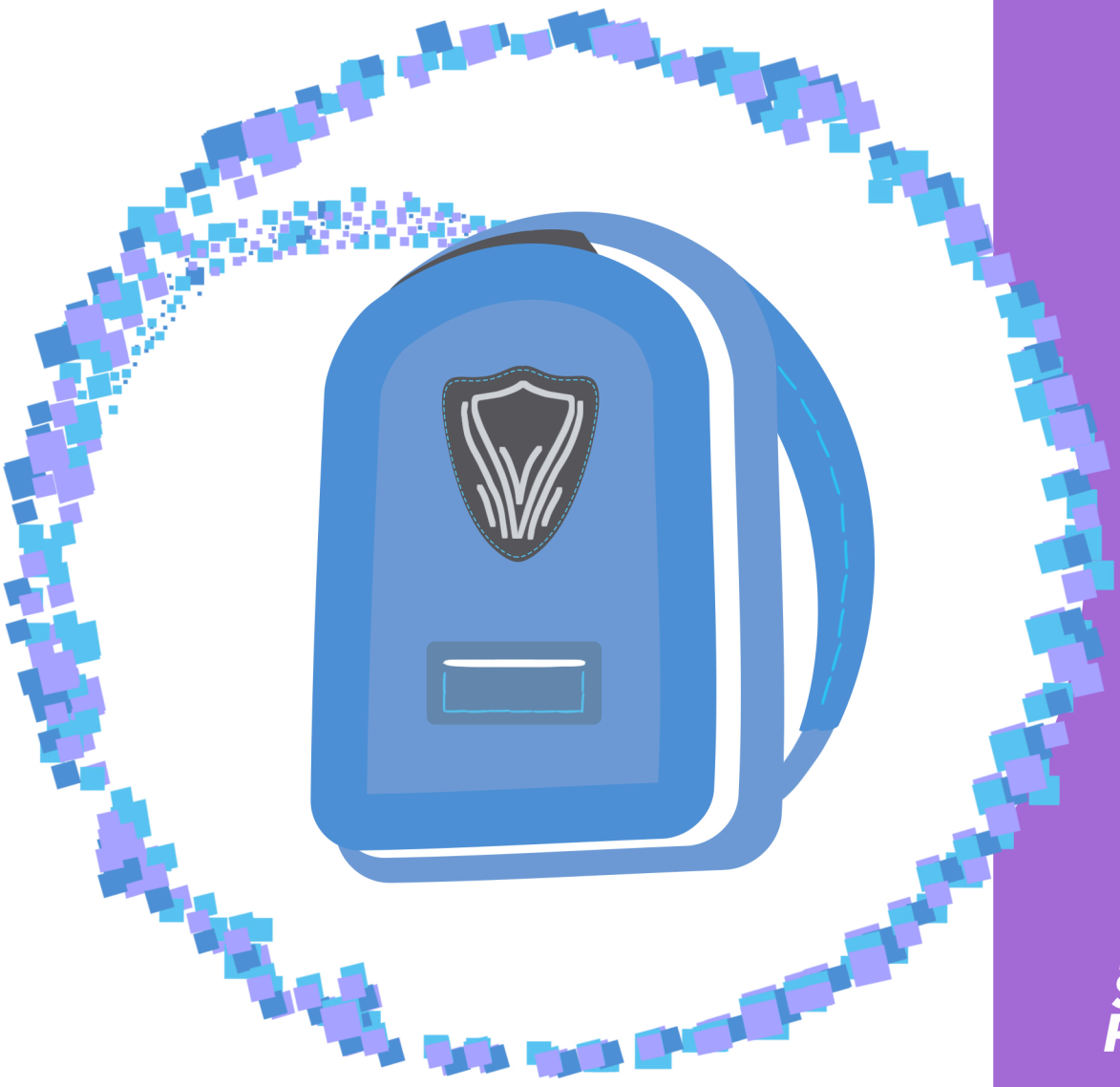
CHIEF PRIVACY OFFICERS:
WHO ARE THEY AND WHY EDUCATION LEADERS NEED THEM



A SERIES OF PAPERS ON STUDENT PRIVACY

CENTER FOR DEMOCRACY & TECHNOLOGY

JANUARY 2019

ABOUT CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology is a 501(c)(3) working to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges. Our team of experts includes lawyers, technologists, academics, and analysts, bringing diverse perspectives to all of our efforts.

Learn more about our experts or the issues we cover: https://cdt.org/

ABOUT STUDENT PRIVACY

CDT's vision for the *Student Privacy Project* is to create an educated citizenry that is essential to a thriving democracy by protecting student data while supporting its responsible use to improve educational outcomes. To achieve this vision, CDT advocates for and provides solutions-oriented resources for education practitioners and the technology providers who work with them, that center the student and balance the promises and pitfalls of education data and technology with protecting the privacy rights of students and their families.

Authored by Elizabeth Laird, CDT Student Privacy Senior Fellow

CENTER FOR DEMOCRACY & TECHNOLOGY

CHIEF PRIVACY OFFICERS:

Who Are They and Why Education Leaders Need Them

Executive Summary

To respond to new demands to protect student data, the education system would benefit from deploying a strategy that has been successful in other sectors and industries: hiring a chief privacy officer (CPO) who is responsible for the organization's privacy policies and practices.

The current model distributes privacy duties across an education organization and has resulted in excessive data collection and access, untrained staff with little support in protecting student data, retaining data past its usefulness, and lax controls on third party management and use of student data. Everyone plays a role in protecting student privacy, but a CPO can improve privacy protections by centralizing the strategy, policies, roles, and responsibilities for protecting data that ultimately result in preventing data incidents, establishing trust, and ultimately ensuring that information is not used to harm students.

This issue brief focuses on a variety of practices that can support such a role, and is divided into two sections: first, the role that education organizations can play in making CPOs successful, and second, the role that CPOs should play in protecting student privacy across the organization. Specifically, organizational leadership should establish the CPO as a senior position, ensure multi-disciplinary support for the CPO, and provide financial resources. Once hired, the CPO should serve as a resource to staff, collaborate with the chief information security officer, cultivate privacy advocates, and respond to current events.

Introduction

Privacy is not a new concept in education. The main federal privacy law that protects student data, the Family Educational Rights and Privacy Act (FERPA), was passed in 1974. Schools, districts, and states have been required to meet certain privacy standards for over 40 years. It is also not new that schools, districts, and states are siloed, with core functions of managing student privacy spread across multiple divisions including the office of general counsel, information technology, data analytics and reporting, human resources, and the office of the executive.

What has changed is that schools, districts, and states collect, share, and analyze more data than ever before, and as a result, the promise of using data and technology to improve student outcomes has never been greater. At the same time, concerns from parents and the public about the education sector's ability to protect the sensitive information that it is entrusted with have never been greater. This mistrust is in part due to a lack of transparency around what policies govern the collection, use, and sharing of student data and is exacerbated by an unprecedented number of data loss incidents. These losses are almost always preventable and the result of human error.

The education sector has responded by prioritizing and executing data governance strategies. Legislative entities have joined in as well: since 2013, 43 states have passed 116 new laws that address student privacy.[1] However, these efforts have not fully addressed the concerns of parents and the public. This issue brief will introduce a strategy, which is being implemented in other sectors such as business and government, to strengthen privacy protections while supporting an organization's core mission: the creation and expansion of the role of chief privacy officer (CPO). It specifically outlines how, in the education sector, the CPO can protect student data while supporting its use to improve outcomes for all students.

What is a Chief Privacy Officer?

A chief privacy officer is a senior leader who is responsible for managing an organization's privacy responsibilities and compliance with legal requirements. Although this role is new to education, other sectors have long employed chief privacy officers to ensure sensitive, personal information is protected while supporting the core work of the organization. State agencies are also hiring

[1] Data Quality Campaign (2018, October) *Education Data Legislation Review: 2018 State Activity.* Retrieved from: https://dataqualitycampaign.org/resource/2018-education-data-legislation/

chief privacy officers. At least eight states (i.e., Arkansas, Indiana, Kentucky, Ohio, South Carolina, Utah, Washington, and West Virginia) have chief privacy officers that cover all state agencies but are not specific to education.[2] A statewide CPO can support an education-specific CPO but is likely insufficient to address all of education's unique needs.

Typical functions that are led by a CPO tend to include creating and enforcing organizational privacy policies, providing privacy training and support, and supporting security efforts that reflect privacy policies and practices.

A chief privacy officer is typically responsible for creating and enforcing organizational privacy policies that govern an organization's data collection, sharing, and use. This could include user access policies that limit access to only those with a legitimate need, practical data retention and deletion schedules that are based on the uses of the data, data minimization guidelines that ensure that the organization collects the minimum amount of data necessary to fulfill stated needs, and statistical methods that ensure that individuals cannot be identified from any publicly reported data.

Additionally, a CPO is often responsible for providing training and support in important organizational areas on privacy best practices and legal compliance. Issues that require training and support might include foundational privacy knowledge and best practices, data incident response planning, and guidance to the executive team and staff on how to achieve their goals while protecting privacy.

Lastly, a CPO supports security efforts to ensure that they reflect privacy policies and practices; these efforts may focus on internal or external systems, data, tools, and processes. For example, a CPO may inform and support an internal process regarding the review and approval of data that has been requested, as well as data systems that will include sensitive information prior to release to ensure they comply with the organization's policies. They will also be involved in coordinating privacy and security audits. An example of supporting security efforts in external systems is in the area of procurement. A CPO may provide guidance during the evaluation process to ensure that products meet the standards of the organization's privacy policies, train third parties on the organization's privacy policies and standards, and ensure contracts and data sharing agreements include appropriate privacy protections.

[2] The Pew Charitable Trusts (2018, August 21) *More States Appoint 'Chief Privacy Officers' to Protect People's Data.* Retrieved from: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/08/21/more-states-appoint-chief-privacy-officers-to-protect-peoples-data

Increasingly, large school districts and state education agencies are hiring chief privacy officers in response to data incidents or student privacy legislation. For example, New York, West Virginia, Utah, and Georgia have state laws that created chief privacy officer positions. However, rather than wait for a legal mandate or breach of trust, education leaders would benefit from taking a proactive approach to student privacy and empowering a senior leader to meet the growing and evolving demands surrounding the collection and and protection student data.

Why Should Education Leaders Consider a CPO?

Data incidents and misuse of information that result from lax privacy controls are unfortunately becoming more common as more data is collected, analyzed, and used to make decisions. For example, a principal at a school in Brooklyn, New York, included the names of all students who were suspended in a weekly newsletter that was sent to all staff, regardless of whether they were teaching those students, and was allegedly viewable by parents.[3] Not only is this a potential FERPA violation, but more importantly, it is a bad privacy practice in which information is overshared with individuals who did not have a legitimate interest in it.

Another example is in the District of Columbia public school system, where three similar data breaches have occurred. Three times in the last three years, the Office of the State Superintendent of Education (OSSE)[4] as well as the District of Columbia Public Schools (DCPS)[5] have experienced data breaches when files with thousands of unredacted student records were inadvertently shared with external stakeholders. These data breaches were the result of human error and inferior privacy processes that allowed files to be accidentally shared when they included students' personally identifiable information.

Lastly, it is not just education systems that have directly violated student privacy. Companies that education leaders have contracted with have also exhibited poor privacy practices. In 2014, ConnectEdu declared bankruptcy and sought to sell 20 million student records that it had collected on behalf of schools as part of its acquisition

[3] International Association of Privacy Professionals (2017, February 27) *Principal Publishes Names of Suspended Students in Newsletter.* Retrieved from: https://iapp.org/news/a/principal-publishes-names-of-suspended-students-in-newsletter/

[4] Washington Post (2016, February 11) *D.C. Accidentally Uploads Private Data of 12,000 Students.* Retrieved from: https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-ea152f0b9561_story.html

[5] AP News (2018, September 5) *Officials Expose DC Students' Personal Information Online.* Retrieved from: https://apnews.com/d06546813bef438f946db8daddbe2d0e

by another company.[6] ConnectEdu's privacy policy indicated that users would be able to delete information prior to any sale; however, this process was not followed, and student records were left in limbo. Fortunately, the Federal Trade Commission (FTC) intervened and ensured that the company that acquired ConnectEdu provided an opportunity to parents and users to delete their information. This underscores the importance of the education system having strong privacy agreements and audits to ensure that any third party with which it has shared sensitive student information is protecting the students' privacy.

These three examples illustrate the potential harms that can result from poor privacy policies and practices. But the good news is that a CPO could improve an organization's privacy strategy and prevent issues like these from happening in the future.

How Can a CPO Help?

Protecting student privacy is not a new function; however, the expansion of education data and technology has placed new and unprecedented demands on the education sector. Even though everyone plays a role in protecting student data, distributing privacy responsibilities across a siloed organization does not position the organization to respond to these increased demands. A chief privacy officer can improve student privacy protections by centralizing this responsibility and establishing clear roles and responsibilities, the result of which is a single organizational strategy to protect student data that will be led and enforced by a senior leader who will be accountable for its successes and failures.

Data Governance + the CPO

This issue brief promotes the value of a chief privacy officer; however, not all education organizations will be able to hire a full-time employee for this function. For example, a state education agency or large school district that is responsible for hundreds of thousands of students and maintains myriad data systems has a different level of risk than a small school district or single-site charter school.

According to the Institute of Education Science's SLDS Grant Program, data governance is "the overall management of data, including its availability, usability, integrity, quality, and security."[7] Organizations will be in various stages of data governance maturity, so it is

[6] Education Week (2014, December 9) *Millions of Student Records Sold in Bankruptcy Case.* Retrieved from: https://www.edweek.org/ew/articles/2014/12/10/millions-of-student-records-sold-in-bankruptcy.html

[7] National Center for Education Statistics Institute of Education Sciences (2017, December) *SLDS Issue Brief Communicating the Value of Data Governance.* Retrieved from: https://nces.grads360.org/#communities/data-governance/publications/15066

important to assess the organization's needs and whether it needs to employ a full-time chief privacy officer or pursue a different solution. Education organizations of all sizes have legal and policy obligations when it comes to protecting student privacy, but their approaches to meeting these requirements will be informed by how advanced their data governance work is and/or should be.

If an organization determines that it does not serve a sufficient number of students, maintains too few systems, and collects too little data to warrant a fulltime CPO, other solutions might include:

- Appoint an existing full-time employee as the organization's privacy officer in addition to their other responsibilities,
- Establish a network of schools or school districts that can employ and share a chief privacy officer,
- Collaborate with and receive support from a state chief privacy officer, or
- Establish a privacy working group that consists of people assigned to lead various components of a comprehensive privacy strategy who meet regularly to ensure all aspects of this strategy are being implemented.

What Steps Can an Organization Take to Support a Chief Privacy Officer's Success?

- **Establish as senior position**: A chief privacy officer will be more successful if they have sufficient authority and leadership support to lead and implement an organization's privacy policies and practices. It can be helpful for this position to be codified in legislation as it mandates its existence and authority, and a CPO should be a senior position that ideally is not more than two direct reports away from the executive. In other sectors, 46% of privacy professionals report that they have a title of director or higher, and the majority are 1-2 direct reports from the chief executive officer.[8]

- **Ensure multi-disciplinary support**: Chief privacy officers can have a variety of backgrounds, including, most frequently, legal, information technology, risk management, and/or policy.[9] Education leaders will need to

[8] International Association of Privacy Professionals (2016) *IAPP-EY Annual Privacy Governance Report 2016*. Retrieved from: https://iapp.org/media/pdf/resource_center/IAPP%202016%20GOVERNANCE%20SURVEY-FINAL3.pdf

[9] Ibid.

determine which skill set is most important for their organization and where to place the CPO in their organization. However, regardless of the skillset and placement in an organization, a chief privacy officer requires the participation of other divisions to be successful. For example, human resources may need to include privacy policies and training as part of the new employee onboarding process, and procurement will need privacy expertise to negotiate privacy controls with third parties. According to a survey by the International Association of Privacy Professionals, almost 50% of privacy professionals have established a privacy working group to coordinate multi-disciplinary support for organization-wide privacy efforts.[10]

- **Provide financial resources**: As the CPO manages and identifies privacy risks for an organization, they will undoubtedly uncover vulnerabilities that might require resources, including staff time and money, to fix. For example, a system may require changes, upgrades, or even replacement if it does not comply with an organization's privacy policy. This could include an inability to limit user access based on roles, the result of which is excessive data access to those who do not have legitimate need. Other sectors are reporting that they are increasing their budget for privacy,[11] so education leaders should consider how to ensure that the CPO, in collaboration with the CISO, can secure resources when an organizational risk is identified.

Once Hired, What Can a CPO Do to Succeed?

- **Serve as a resource to staff**: CPOs are more successful if their working style approaches privacy from a perspective of being a resource to staff rather than a punitive enforcer of policy. Enforcing compliance is a necessary part of a CPO's job but should not be a CPO's primary objective. If a CPO is viewed as an obstacle or threat, staff will not seek to collaborate and may attempt to hide known issues from the CPO. On the other hand, staff are more likely to follow privacy policies and practices if they view the CPO as a resource and someone who can help them achieve their goals and objectives.
- **Collaborate with chief information security officer**: A chief privacy officer will have different skill sets and responsibilities than a chief information security officer (CISO). As discussed in the *Importance of Chief Information Security Officer*on p. 8, a

[10] Ibid.

[11] Ibid.

chief privacy officer is primarily concerned with policy whereas a CISO leads an organization's technical efforts to secure sensitive information. Both roles are crucial components of a holistic approach to protecting privacy, so a CPO should work with the CISO and IT staff to ensure that data systems and applications effectively implement the organization's privacy policies.

- **Cultivate privacy advocates:** A chief privacy officer alone cannot solve all of an organization's privacy problems, so to be successful, everyone must play a role in protecting student data. To accomplish this, a CPO should establish advocates at all levels and in each division of the organization. They can do so by building informal relationships as well as formalizing a privacy working group, which can inform the organization's privacy efforts and should be considered as part of the organization's larger data governance strategy.
- **Respond to current events**: The demands on a CPO will continue to evolve as policies and technologies change. A CPO should stay attuned to current events, including privacy trends in other education jurisdictions and sectors, incorporate lessons learned, and prevent data incidents that have occurred elsewhere. It is also important to stay abreast of current events to continue communicate the urgency and relevance of privacy risks.

What Distinguishes a CPO from a Chief Information Security Officer

There can be confusion between the roles of a CPO and a CISO. Both are critical to protecting student data; however, each has distinct skills and responsibilities.

Privacy is the idea that people should be able to control their own information and that the entities that are *authorized* to collect and use that information do so in ways that respect an individual's autonomy. Privacy professionals not only ensure compliance with the law, but design policies to reduce the risk of information collected or used in ways that result in embarrassment, loss of trust, or unfair treatment.[12]

Security is the practice of preventing *unauthorized* access to information and the systems that hold it. It includes physical and technological controls that seek to prevent the accidental or malicious disclosure of information.

[12] National Institute of Standards and Technology (2017, January) *An Introduction to Privacy Engineering and Risk Management in Federal Systems.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

Broadly put, a CISO requires a more technical skill set whereas a CPO is oriented toward establishing the right organizational policies. For instance, a CPO may create a policy that records of students' visits to the principal's office are destroyed at the end of the school year. The CISO is then responsible for ensuring that deletion is carried out at the appropriate time and in a method that makes the information sufficiently unrecoverable.

A CISO would lead efforts related to technical strategies, including deploying and updating security software/upgrades, implementing user management policy, managing passwords and devices, and creating an acceptable use policy.

A CPO and CISO may share responsibilities related to tasks that rely heavily on policy and technology like responding to data incidents, securing analog data, auditing implementation of privacy and security policies, and monitoring and ensuring compliance of third parties.

Conclusion

Protecting student data must be a core component of any responsible effort to use data and technology to improve student outcomes because of the many examples of wasted resources, failed initiatives, and leadership turnover that result from student privacy concerns. Rather than wait for a data incident or legal mandate, education leaders can support their efforts to effectively use data by being proactive and empowering a senior leader to ensure the organization fulfills its responsibilities to protect the student data with which it is entrusted.

Although everyone plays a role in protecting student privacy, employing a chief privacy officer in the education sector can be an important strategy to advance efforts to use data and technology while ensuring student information remains protected. This role is proving to be successful in other industries and sectors, and would be an improvement over the current practice of sharing privacy responsibilities such that everyone is responsible yet no one is responsible.

Student privacy responsibilities are only growing, along with the potential for data and technology to improve student outcomes. It is a critical moment for education leaders to decide whether they are going to evolve to the meet these new demands in service of students, or maintain the status quo to their detriment.

APPENDIX

A

B

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Appendix A: Sample Chief Privacy Officer Job Description

The audiences for the following job description are school districts, charter management organizations, state education agencies, and the companies that serve them. The job description may need to be adapted to reflect additional priorities and existing data governance and privacy protection structures.

Position Title: Chief Privacy Officer

Immediate Supervisor: Senior Executive at [Organization name]

Position Overview: The Chief Privacy Officer is a senior leader who is responsible for managing [organization name]'s privacy responsibilities and compliance with legal requirements to balance the use of data and technology with protecting the privacy rights of students and their families. The Chief Privacy Officer will work closely with the Chief Information Security Officer, Human Resources Director, General Counsel, and other senior leaders as needed. Strong interpersonal skills, excellent written and oral communication skills, and the ability to develop privacy champions throughout the organization are important for success in this role.

Responsibilities:

- Create and enforce organizational privacy policies that govern [organization name]'s data collection, sharing, and use including but not limited to:
    - User access policies that limit access to only those with a legitimate need,
    - Data retention and deletion schedules that are based on the uses of the data,
    - Data minimization guidelines that ensure that the organization collects the minimum amount of data necessary to fulfill stated need(s), and
    - Statistical methods that ensure identifiable information has been removed from any publicly reported data.
- Provide training on privacy best practices and legal compliance.
- Support and inform data incident response planning.
- Support procurement of technology and data tools and systems by:
    - Providing guidance during the evaluation process to ensure that products that meet the standards of the organization's privacy policies,
    - Training third parties on the organization's privacy policies and standards, and

    - Ensuring contracts and data sharing agreements include appropriate privacy protections.
- Review and approve data that have been requested by external parties as well data systems that will include sensitive information prior to release to ensure they comply with the organization's policies.
- Coordinate privacy and security audits.
- Provide guidance to executive team and staff on how to achieve their goals while protecting privacy as well as develop privacy advocates throughout [organization name] to ensure effective implementation of privacy protections.
- Supervise staff as needed.

Qualifications:

- Strong commitment to balancing the use of data and technology with protecting the privacy rights of students and their families.
- Familiarity with relevant federal student privacy laws including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PPRA).
- Familiarity with [relevant state student privacy laws].
- Demonstrated ability to work collaboratively with staff at all levels of an organization.
- Demonstrated ability to provide guidance that furthers the business needs of an organization.
- Excellent oral and written communication skills, including the ability to translate technical and legal information into a digestible format.

Education and Experience:

- Bachelor's degree.
- Law degree or masters degree in relevant area.
- Equivalent of ten (10) years of full-time experience with privacy and confidentiality, student information management, or information security.
- Project and change management experience to effectively lead organizational change and ensure projects are implemented thoroughly and with urgency.
- Experience working for a school, district, or state education agency is preferred.
- Privacy professional certification or other credential that requires formal privacy training is preferred.


CENTER FOR
DEMOCRACY
& TECHNOLOGY

Appendix B: Sample Chief Privacy Officer Hiring Exercises

The following exercises are examples of tasks that may be given to candidates during the interview process to assess their content knowledge and working style.

Exercise #1: Create data incident response plan

[Organization name] recently experienced a breach of student data when a file was released publicly that inadvertently included student information. [Organization name] did not have a data incident response plan at the time, so one of the lessons learned is that [organization name] would benefit from creating a data incident response plan. Please describe the steps that you would take to establish a data incident response plan and how you would measure its success.

Exercise #2: Establish a privacy training program

According to a recent study, 95% of data incidents are the result of human error.[13] As a result, [organization name] would like to establish a privacy training program. Please describe how you would establish this program including: audience, goals, major areas of focus, compliance, and measures of success.

Exercise #3: Create a process to establish an annual student privacy strategic plan

The CPO is a new role, and [organization name] does not currently have an annual student privacy strategic plan. Please describe the steps you would take to establish a strategic plan, including who you would involve, how you would involve them, and how you would measure success.

[13] SC Media (2014, June 16) *"Human Error" Contributes to Nearly All Cyber Incidents, Study Finds.* Retrieved from: https://www.scmagazine.com/home/security-news/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/