NAF Data Security and Protection Policy

Contents

1. About

NAF values its role as a trusted steward of the data our district partners and clients make available to us in delivery of the services we are contracted to provide. We are committed to developing and implementing safeguards that effectively protect students and other sensitive data from unauthorized access and disclosure.

The Data Security and Protection Policy document defines processes and systems of how NAF will store, share, maintain and destroy data that we acquire from our constituents, particularly Personally Identifiable Information (PII) with intent to

- Ensure the security and confidentiality of our clients' information.
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to our clients.

While this document will not eliminate all malicious data theft, it stands to guide user awareness and practice and establish reasonable physical, technical, and administrative standards to protect against accidental loss and disclosure scenarios.

NAF's Data Security and Protection plan is in alignment with other NAF policies that address client data protection. It will be reviewed and revised annually, or as new developments require. Clients will be notified of these revisions.

View NAF's Online Privacy Policy here

View NAF's Data Privacy Provisions here

View NAF's Data Classification Plan here

2. Scope

2.1. In Scope

The Data Security and Protection Policy applies to all client data, personal data and other defined data classified as sensitive by the NAF's data classification policy. It will apply to any server, database and Tech system that handles such data, including any device that is used for email, web access or other work-related tasks. Every user who interacts with classified data is also subject to this policy.

2.2. Out of Scope

Information that is classified as public, which can also be PII (such as email addresses) that may be accessed through a customer's public website or third party who has the rights to distribute that data. Other data can be excluded from the policy by company management based on specific business needs, which could be attributed to being too costly or complex to maintain.

3. Policy

3.1. Data Access Principles

NAF shall provide all employees and contracted third parties with access to the information and training they need to carry out their responsibilities as effectively and efficiently as possible. The policy includes responsibilities relating to the delivery of contracted services.

NAF will inform sub-contractors of the NAF Data Privacy and Security provisions and require assurance of their understanding, intent, and capacity to meet or exceed the established standards and practices.

The practice of vetting sub-contractors lies with the Finance Department or the Supervisor of the department that owns the sub-contractor relationship.

3.2 General User, Educator and Staff Guidelines

1. Each user shall be identified by a unique user ID and will be held accountable for their actions.
2. The use of shared identities is not permitted except for training or service accounts. Personal accounts cannot be shared.
3. Each user shall read this data security and protection policy and login and logoff guidelines, and guidelines and sign a statement that they understand the conditions of access.

3.3 Training

1. All NAF Staff will undergo Data Privacy and Protection training prior to accessing student and other Personally Identifiable Information (PII) data as advised by our Research + Tech department.
2. All newly positioned Staff and Consultants' NAF Supervisors will indicate if and why access to PII information from NAF's systems is required. NAF's data privacy and protection training will be completed prior to them receiving access to sensitive data.
3. Signed agreements and subcontractor representatives' completion of NAF's data privacy and protection training will serve as acknowledgement of the user guidelines and responsibilities required for the contracted work. Contract management leads will ensure that all staff involved in the execution of contracts are aware of the contract and security and protection specifications.

3.4 Access to Confidential or Restricted Information

1. Access to data classified as “Confidential” or “Restricted” shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security and Protection Policy or higher management.

3.5 Network Access

1. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.
2. Accessing files and resources will require user authentication methods such as signing into cloud-based services.

3.6 User Responsibilities

1. All users will follow data privacy and security guidelines and effective practices to reduce the risk of unauthorized access, such as locking their screens whenever they leave their desks; keeping their workspace clear of sensitive or confidential information when they leave the area; refraining from printing or downloading sensitive information unless absolutely necessary; and using a shredder to destroy any printed data to reduce the risk of unauthorized access.
2. Passwords must be stored in systems that are designed to store passwords that require a prior sign in (such as Okta). Passwords will be allowed to be stored in a written format around a computer.
3. All users must keep their workplace clear of any sensitive or confidential information when they leave.
4. All users must keep passwords confidential and not share them unless directly requested by the Tech department in a written request.
5. All users will not print out sensitive information unless absolutely necessary and will utilize a shredder to destroy sensitive data that was printed out.

3.7 Application and Information Access

1. All company staff and contractors shall be granted access to data and applications required for their job roles.
2. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from their staff supervisor.

3.8 Transfer of Data

1. NAF staff or contractors may not share sensitive data in messages – like email –or as attached files in messages.
2. NAF staff and contractors may share data for NAF service-related purposes that includes PII only when necessary, using a secure connection (SSL certificate) like a cloud service (e.g., OneDrive or ShareFile) that requires two-factor authentication. Users are required to enable the restricted access feature which can include an expiration date or password request when the feature is available.
3. Systems that automatically send PII will require end to end encryption. In rare cases where the information is not encrypted at the time of transit, the minimum requirement is that it goes through a secure socket connection (i.e., HTTPS, FTPS) and includes a form of authentication.
4. Clients may use NAF Services to run reports that may include sensitive data that is only available to client representatives with access rights to their reports. Access to these reports requires sign in authentication from the user. Changes to this data may be presented to NAF for revision or made within the reports by client users (this includes student or parent/guardian inquiries).
5. Data provided by or owned by the client will be securely transferred back when requested due to termination of services or the end of scheduled term for retention.

3.9 Data Destruction

1. PII associated with high school records or work of graduated students will be anonymized and permanently restricted in access within 30 months (about 2 and a half years) of the student's graduation except in aspects of the system related to 5 and 6, below.

2. Upon request or NAF's scheduled destruction, NAF will anonymize and restrict access to all Personally Identifiable Information (PII) in the active systems based on the contract between NAF and a third party.

3. This data is not removed from NAF's backup systems as they are stored as a single image and only retrieved when necessary.

4. This data protocol will apply due to terminated services, graduated students, and parent-student requests.

5. This will not include "certifications" or "credential data" in cases where NAF is offering services to active students or alumni using elements of NAF's services that allow them to connect their work with post-secondary experiences or employment opportunities. These elements are core NAF services, and districts can opt-out of these student supports at any time. NAF's scheduled data destruction is included in the organization's records retention and destruction policy.

6. NAF will retain select PII past the 30-month period for the purposes of FERPA-compliant research on program impact. This PII will be kept according to NAF's agreed-upon data privacy and security standards but will only be used to conduct FERPA-compliant research and will be limited to the personnel conducting research.

NAF will provide notification of the destruction of the data, noting date and time.

4. Technical Guidelines

The technical guidelines section specifies requirements for technical controls used to grant user access to data. The access control method list includes:

1. Auditing of attempts to log onto any device on the company network or cloud services
2. Single Sign On (SSO) is implemented through our primary SSO vendor where available.
3. Role-based access model
4. Restricted server access rights
5. Web authentication rights
6. Database access rights and ACLs
7. Written requests to provide access by NAF staff.

5. Reporting Requirements

At the discovery of an incident, the Tech department will work with the lead for the NAF department involved in the incident (if applicable), and the Communication Team to notify partners and share our incident reports according to the established protocols. Elements of this plan include:

1. Formation of an Incident Response Team
2. Outreach to the affected partners to let them know about the incident as soon as possible and according to unique timelines established by partner agreements.
3. Identification and ownership of key contacts needed to t initiate and maintain contact throughout the discovery phase.
4. Identify and list compromised data information and/or platforms.
5. Development and maintenance of a resource folder that includes key information related to all phases of specific incidences – including next steps while in the discovery mode.
6. Isolation and de-authorization of accounts believed to be compromised if necessary.
7. Development of a final- steps document to amend the issue and communicated the plan with the necessary contacts.

6. Ownership and Responsibilities

Data owners are staff and contractors who have primary responsibility for overseeing the collection, use, and management of information, such as an executive, department manager or team leader.

The Tech Security Administrator is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.

Users include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees, and volunteers.

The Incident Response Team shall be chaired by an executive and include employees from departments such as Research and Tech, Human Resources, Finance, Network Development and Implementation, and Communications.

The Contract Management Lead serves as the primary point of contact between the client and NAF in matters related to the contracted services.

Higher Management refers to executive and senior leaders at NAF.

7. Enforcement

1. Any user found in violation of this set of policies is subject to targeted training and disciplinary action, up to and including termination of employment.
2. Any third-party partner or contractor found in violation may have their network connection or NAF contract terminated.

8. Version

1. This document will be reviewed annually by the Research and Tech department.
2. This document was last updated December 2023.

Addenda

Sample Document
NAF Data Security and Protection Plan by Commonly- Required Feature

NAF's Alignment with NIST Framework

NAF Data Security and Protection Support & Services by Required Feature

Data Security and Protection Requirements	NAF's Data Security and Protection Policy Elements
Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Sections 2-7
Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Sections 3-7
Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Section 3.3
Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Section 3.3.3
Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Section 5
Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Section 3.8
Describe your secure destruction practices and how certification will be provided to the EA.	Section 3.9
Outline how your data security and privacy program/practices align with the EA's applicable policies.	This document serves as the description.
Outline how your data security and privacy program/practices materially align with the NIST CSF vl.1	See the following pages.

NAF's Alignment with NIST Framework

The NAF Security and Protection plan addresses and is guided by the five core areas of the National Institute of Standards and Technology (NIST)'s Cybersecurity Security Framework (CSF). As NAF continues to refine the plan and address risk management programming, processes, and partner participation. This table reflects current areas of alignment with NIST Framework. Links to the documents referenced are available via links provided at the end of the document.

NIST Core Components	NAF Data Security and Protection Elements of Alignment
Identify	Data Classification Plan – **Data Custodians** **Data validation:** Periodically validate data integrity. **Data access:** Develop data access guidelines for each data classification label. Data Classification Plan –**Appendix A** **Types of information that must be classified as Restricted.**
Protect	Data Security and Protection Policy –-**Section 3** **Data Policy** 3.1. Data Access Principles 3.2 General User, Educator, and Staff Guidelines (including third parties) 3.3 Training 3.4 Access to Confidential or Restricted Information 3.5 Network Access 3.6 User Responsibilities 3.7 Application and Information Access 3.8 Transfer of Data 3.9 Data Destruction
Detect	Data Classification Plan – **Data Custodians** **Monitor activity:** Monitor and record data activity, including information on who accessed what data sets. **Data validation**: Periodically validate data integrity.
Respond	Data Security and Protection Policy **-** Sections 5, 7 **5. Reporting Requirements** At the discovery of an incident, the Tech department will work with the lead for the NAF department involved in the incident (if applicable), and the Communication Team to notify partners and share our incident reports according to the established protocols. **7. Enforcement**

	Any user found in violation of this set of policies is subject to targeted training and disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection or NAF contract terminated. Data Classification Plan - **Data Custodians** **Data Back-ups**
Recover	Data Classification Plan - **Data Custodians** **Data Back-ups**

Referenced Documents

NAF Data Security - Protection Plan

NAF Data Classification Policy - March 2021 (2).docx Section 3