Data Governance

Data governance describes an organization's

*collection, management and use of data
*identifies specific roles for carrying out this work; and
*outlines the process by which data may be shared with external entities

At Benway, we know that any data-based decision-making to improve educational practice or policy must rely on reliable, robust data. This is why it is important to have transparent and explicit data governance policies in place.

Benway's vision is to ensure stakeholders have access to timely, consistent, and accurate data to inform and support empirically-driven decisions affecting education. To facilitate the use of data for wise decision-making, stakeholders need a clear understanding of the Benway's data governance program, including existing policies for: data collection and use, data privacy, suppression, data reports, and public requests for data.

Data Security Measures

I. Purpose

(A) implement standards & procedures to effectively manage & provide necessary access to system data, while at the same time ensuring the confidentiality, integrity & availability of information. Insofar as this policy deals with access to Benway School computing & network resources, all relevant provisions in the Acceptable Use Policies are applicable.
(B) Provide a structured & consistent process for employees to obtain necessary data access for conducting Benway School operations.
(C) Define data classification & related safeguards. Applicable federal & state statutes & regulations that guarantee either protection or accessibility of system records will be used in the classification process.
(D) Provide a list of relevant considerations for system personnel responsible for purchasing or subscribing to software that will utilize and / or expose system data.
(E) Establish the relevant mechanisms for delegating, authority to accommodate this process at the school level while adhering to separation of duties and other best practices.

II. Scope

(A) These security measures apply to information found in or converted to a digital format. (The same information may exist in paper format for which the same local policies, state laws, statutes, and federal laws would apply, but no electronic control measures are needed.)
(B) Security measures apply to all employees, contract workers, volunteers and visitors of the Benway School and all data to conduct operations of the system.
(C) Security measures do not address public access to data as specified in the New Jersey Open Records Act.

(D) Security measures apply to system data accessed from any location; internal, external or remote.
(E) Security measures apply to the transfer of any system data outside the system for any purpose.

III. Guiding Principles
(A) Inquiry-type access to official system data will be as open as possible to individuals who require access in the performance of system operations without violating legal, federal, or state restrictions.
(B) The director and/or his/her designees shall determine appropriate access permissions based on local policies, applicable laws, best practices, and the New Jersey Open Records Act.
(C) Data users granted "create" and/ or "update" privileges are responsible for their actions while using these privileges. That is, Benway School is responsible for the system data they create, update, and / or delete.
(D) Any individual granted access to system data is responsible for the ethical usage of that data. Access will be used only in accordance with the authority delegated to the individual to conduct Benway School operations.
(E) It is the express responsibility of authorized users to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.
(F) These security measures apply to system data regardless of location. Users who transfer or transport system data "off-campus" for any reason must ensure that they are able to comply with all data security measures prior to transporting or transferring the data.

IV. Access Coordination
(A) Administrators, supervisors, and area specialists (authorized requestors) will assist in classifying data sensitivity levels for their areas of expertise and in identifying which employees require access to which information in order to complete their duties.
(B) The system technology coordinator will designate individuals within the technology department to implement, monitor and safeguard access to system data based on the restrictions and permissions determined by the authorized requesters using the technical tools available.
(C) Administration, supervisors, and area specialist will be responsible for educating all employees under their responsibilities associated with data security.

V. Data classification
(A) Benway School system data shall be classified into three major classifications as defined in this section. Requests for changes to the established data sensitivity classification or individual permissions shall come from the above identified authorized requestors to the technology department.
1) Class I - Public Use
this information is targeted for general public use. Examples include internet website content for general viewing and press releases.
2) Class II - Internal Use

Non-sensitive (see class III) information not targeted for general public use.
3) Class III - Sensitive
This information is considered private and must be guarded from unauthorized disclosure; unauthorized exposure of this information could contribute to identity theft, financial fraud, breach of contract and / or legal specification, and / or violate state and / or federal laws.
(B) FERPA Directory Information
Information disclosed as 'directory information' may fall into either Class I or Class II, depending on the purpose of the disclosure. The following is the school's list of which student information is to be considered 'directory information'.

Benway School FERPA Directory Information Disclosure

The Family Educational Rights and Privacy Act (FERPA), a federal law, requires that the Benway School, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Benway School may disclose appropriately designated 'directory information' without written consent, unless you have advised the district to the contrary in accordance with the school procedures. The primary purpose of directory information is to allow the Benway School to include this type of information from your child's education records in certain school publications. Publications may be in print or digital format.
Examples include, but are not limited to, the following:
*A playbill, showing your student's role in a drama production;
*School yearbook;
*Honor roll or other recognition lists;
* Graduation programs; and
* Sports activity sheets, such as for basketball, showing statistics of a team member.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks, take school pictures, or process data.
In addition, two federal laws require local educational agencies (LEAS) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, and institutions of higher learning, upon request, with three directory information categories - name, addresses and telephone listings - unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.
If you do not Benway School disclose 'directory information' from your child's education records without your prior written consent, you must notify the school principal in writing within five (5) school days of the student's first day of attendance.
The school may disclose the following information as directory information:
*Student's name
*Address

*Telephone listing
* Electronic mail address
* Photography
* Date and place of birth
* Dates of attendance
* Grade level
* Participation in officially recognized activities and sports
* Degrees, honors, and awards received
* The most recent educational agency or institution attended
* A student number assigned by the school (in some cases*)

* In order to make certain software applications available to students and parents, the school may need to upload specific 'directory information' to the software provider in order to create school accounts for students and / or parents. Examples of these include, but are not limited to Tynker.com, Rosetta Stone.com, tinkercad.com, and various education software applications. In these cases, the school will provide only the minimum amount of 'directory information' necessary for the student or parent to successfully use the software service.

VI. Compliance

(A) Data users are expected to respect the respect the confidentiality and privacy of individuals whose records they access; to observe any restrictions that apply to class III (sensitive) data; and to abide by applicable laws, policies, procedures and guidelines with respect to access, use, or disclosure of information. The unauthorized use, storage, disclosure or distribution of system data in any medium is expressly forbidden; as is the access or use of any system data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.
(B) Each employee at the system will be responsible for being familiar with the system data security policy and these security measures as they relate to his or her position and job duties. It is the express responsibility of authorized users and their respective supervisors to safeguard the data they are entrusted with, ensuring compliance with all aspects of this policy and related procedures.
(C) Employees, whether or not they are authorized users, are
Expressly prohibited from installing any program or granting any access within any program to class III without notifying the technology department.
(D)Violations of these data security measures may result in loss of data access privileges, administrative actions, and / or personal civil and / or criminal liability.

VII Implementation of Network / Workstation Controls and Protections and Physical Security

A. Shared Responsibilities

1. Technology department implement, maintain, and monitor technical access controls and protections data stored on the system's network.
2. System employees, including authorized requesters, shall not select or purchase software programs that will utilize were exposed class III data without first consulting the technology department to determine whether or not adequate

controls are available within the application to protect that data. (the exception to this would be any software program purchased or utilized by the New Jersey Department of Education. In this case the New Jersey Department of Education shall take all security responsibilities for data it accesses or receives from Benway School.)

3. the technology department staff and / or the authorized requester will provide professional development and instructions for authorized users on how to properly access data to which they have rights, when necessary. However, ensuring that all employees have these instructions will be the shared responsibility of the supervisor(s) of the authorized user(s) and the technology department.
4. technical controls and monitoring cannot ensure with 100% certainty that no unauthorized access occurs. For instance, a properly authorized user leaves their workstation while logged in, and an unauthorized person views of the data in their absence therefore it is the shared responsibility of all employees to cooperatively support the effectiveness of the established technical controls through their actions.

(B) Authorized Requesters

1. Authorized requestors (section IV.A) are responsible for being knowledgeable in all policies, laws, rules, and best practices relative to the data for which they are granting access including but not limited to FERPA, HIPAA, etc.
2. Authorized requesters shall be responsible for informing appropriate technology department personnel about data classification in order that the technology department and determine the best physical and / or logical controls available to protect the data. This shall include:

a. Which data should be classified as class III
b. Where that data resides (which software program(s) and servers)
c. Who should have access to that data (authorized users)
d. What level of control the authorized user should have to that data (i.e. read only, read/write, print, etc.)

C. Location of Data and Physical Security

1. Class III data shall be stored on servers / computers which are subject to network / workstation controls and permissions. It shall not be stored on portable media that cannot be subjected to password, encryption, or other protections
2. Serving devices (servers) storing sensitive information shall be operated by Professional Network system administrators, in compliance with all technology department security and administration standards and policies, and shall remain under the oversight of the technology department supervisor.
3. Persons who must take data out of the protected Network environment (transport data on a laptop, etc.) must have the permission of their supervisor prior to doing so. Permission to do so will be granted only when absolutely necessary, and the person transporting the data will be responsible for the security of that data including theft or accidental loss.

4. All servers containing system data will be located in secured areas within limited access. At the school or other local building-level, the principal or other location supervisor will ensure limited, appropriate access to these physically secured areas.
5. District staff who must print records that contain Class II or III data shall take responsibility for keeping this material in a secured location Dash Vault, locked filing cabinet, etc. In addition, all printed material containing class III documentation when no longer in use.

(D) Disposal of Hardware Containing System Data

1. prior to disposal of any computer, the user will notify the technology department. A technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.
2. Any school departments which purchase or lease copy machines or multifunction printers will be expected to include provisions for the destruction of data on the devices hard drive or the destruction of the hard drive itself prior to disposing of the copier or MFP or its return the leasing agency.

(E) Application of Network and Computer Access Permissions

1. The technology department staff shall be responsible for implementing network protection measures that prevent unauthorized intrusions, damage, and access storage and transport mediums; including, but not limited to:

a. Maintaining firewall protection access to the network and slash or workstations.
b. Protecting the network from unauthorized access through wireless devices or tapping of wired media, including establishing guest wireless networks with limited network permissions.
c. Implementing a virus and malware security measures throughout the network and on all portable computers.
d. Applying all appropriate security patches.
e. Establishing and maintaining password policies and controls on access to the network, workstations, and other data depositories.

2) Technology department staff will apply protection measures based on the data classifications (see sections IV and V), including:

a. Categorizing and / or re - classifying data elements and views.
b. Granting select access to system data.
c. Documenting any from mandatory requirements and implementing adequate compensating control(s).
d. Conducting periodic access control assessments of any sensitive information devices or services.

(F) Sensitive Data as it Pertains to Desktops / Laptops / Workstations / Mobile Devices

1. Firewalls and antivirus software must be installed on all desktops, laptops and workstations that access or store sensitive information, and a procedure must be implemented to ensure that critical operating system security patches are applied in a timely manner.
2. Storage of sensitive information on laptops, mobile devices, and devices that are not used or configured to operate as servers is prohibited, unless such information is encrypted in a technology department - approved encryption format.
3. The user responsible for the device shall take proper care to isolate and protect files containing sensitive information from inadvertent or unauthorized access.
4. Assistance with securing sensitive information may be obtained from school dad level technology coordinator with input from the technology department, as necessary.

VII Transfer of Data to External Service Provider

A. Student class I data, directory information, and, in some cases Class II data, may be transferred to an external service provider, such as an online website that teachers wish students to use for educational purposes. Provided that:

1. The teacher follows the protocols for getting approval for the site to be used.
2. The district notifies parents about their right to restrict their child's data from being shared with such sites annually via code of conduct AUP.
3. The transfer of data is handled in a manner approved by the technology department, or is performed by the technology department.

(B) No class III data, or FERPA protected educational records, will be transferred to an external service provider without prior approval of the data governance committee exception: New Jersey State Department of Education.

(C) No Department should enter into a contract for the use of any program that requires the import of school data without first consulting and receiving approval from the data governance committee.

(D) The data governance committee will determine which of the following should be required of the service provider and assist in ensuring these requirements are met prior to any data transfer:

- Contract
- Designating the service provider as an official as defined in FERPA
- Memorandum of understanding
- Memorandum of agreement
- Non-disclosure agreement

(E) Non-Disclosure Agreement (NDA) Information

The following instructions comply with the Benway school policy data security

When to Use a Non-Disclosure Agreement

1. Private information. confidential information, as defined by FERPA and other regulations and policies, is to be protected and disclosed only to the employees who have a direct legitimate reason for access to the data in order to provide Educational Services to the student.
2. You must seek guidance from the administration, and / or the technology department prior to transferring confidential information to any outside Company, online service (free website), or to any outside individual, organization, or agency without the explicit written permission of the parent of a minor student or an adult age student. This information includes:

a. Social security number
b. grades and test scores(local and standardized)
c. special education information
d. health information and 504 information
e. attendance information (not enrollment, but specific attendance dates)
f. family / homeless / or other similar stats
g. Child Nutrition program status (free or reduced meals)

This includes providing confidential information to individuals, including system employees, for use in dissertations or other studies for college courses or doctoral studies.

Refer all such requests, including those for federal, state, or other studies to the administration and the technology department for their approval before releasing any such individualized information. Approved recipients may be required to complete an NDA so that they fully understand the responsibilities with regard to safeguarding and later destroying this private information. This restriction does not apply to publicly available aggregated data such as dropout rates, attendance rates, percentage of free and reduced lunch program students.

Exceptions. Other K-12 schools - Private information may be transferred upon request to the State Department of Education or other school system with a legitimate need for the data; however, the transfer process should comply with data security protocols (see below). In addition, personnel must research all recipients to ensure that the school is legitimately a school.

Colleges - confidential information may be transferred to institution of higher education,

when the adult student or the parent of a minor student request the transcript or other private information be released specific institutions. Such information should not be transferred to colleges based on a request from the college directly, unless approved by the individual whose records will be transferred.

3. Directory Information. Although Benway school has identified the following as directory information, school should still carefully consider the transfer or publication of this information. Seek guidance when in doubt. Much of this information, combined with data collected elsewhere can be used for identity theft purposes, stalking, and other unlawful or unethical purposes.

a. Home address
b. Home or cell phone numbers of students or their parents
c. Email addresses of students or their parents
d. Date and place of birth

Exceptions: U.S. military and institutions of Higher Learning for recruiting purposes. However, school must first determine which parents have submitted out forms relative to these request prior to transferring data.

(E) Non-Disclosure Agreement Processing

1. The school office administrative assistant will keep all NDA's on file. This will eliminate the need for Each department to solicit an NDA from companies which already have NDA's on file. Technology will also ensure that NDA is renewed annually where necessary.
2. What the school should do:

a. get the following specific information from The Entity to which you want to transfer the information: company name, web address, phone number, fax number, and email address, name of individual you are working with.
b. List the information you wish to transfer to The Entity
c. send this information to the tech department for referral to the data governance committee

3) upon approval by the data governance committee, the technology department will determine if there is a current NDA already on file with the entity. If not, one will be prepared and sent to them. Once the agreement has been signed, the technology department will notify the department and oversee the process of securing uploading the necessary data to the service provider.

4) Note that all confidential data that will be transferred by email, weather in the body

of the email or as an attached file, should be encrypted. The technology department can help you with transporting this data.

(F) Sample Non-Disclosure Agreement (see Appendix A)

IX Reporting Security Breaches

All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, lost / theft of device, or failures of technical measures.

Data Governance Training

I. School and Office Administrators

A. School and office administrators will receive refresher training on FERPA and other data security procedures annually at principal meetings

B. Principles and office administrators shall contact the technology coordinator or the executive directors department when in doubt about how to handle class II and III information.

II. Teacher and Staff Training

A. All new teachers will complete training on all School Technology policies, including how their use of technology is governed by FERPA and other data security procedures established by the school.

B. All department heads / supervisors will be expected to educate their support staff on data governance as it applies to their department work.

C. All users will receive reminders throughout the year via email regarding malware threats and phishing scams and how to report suspected threats.

Data Quality Controls

I. Job Descriptions

A. Job descriptions for employees whose responsibilities include entering, maintaining, or deleting data shall contain provisions addressing the need for accuracy, timeliness, confidentiality, and completeness. This includes, but is not limited to school clinical staff, administrative assistance, and school nurse.

II. Supervisory Responsibilities

A. It is the responsibility of all supervisors to set expectations for data quality and to evaluate their staff performance relative to these expectations annually.

B. Supervisors should immediately report incidents where data quality does not meet standards to their superior and to any other relevant department, including the State Department of Education, if applicable

Student Information Systems

I. Student Information Applications

A. Any software system by the school which is used to store, process, or analyze student educational records as defined by FERPA shall be subject to strict security measures . These systems are: Paradigm Pioneer Database

B. With supervisory responsibilities over the schools student information systems shall determine the appropriate access rights to the data and enforce compliance with these roles and permissions.

II. Paradigm Pioneer Database

Paradigm Pioneer database enables users to access the application from anywhere there may be an internet access. In response to this anywhere / anytime access, the following has been implemented:

* Strong passwords will be assigned by the school
* Staff will keep computer areas secure by locking or logging off their machine when it is unattended
* Staff will not share network or program passwords with others
* Staff will not allow personal data that has been printed into the view or hands of unattended parties
* Staff will not use software rights to grant other permission to data to which they are not entitled

Data Backup and Retention Procedures

I.Purpose of Data Backup and Retention Procedures

A. Ensure that procedures for comprehensive data backup are in place and that system data is restorable in the event of data corruption, software or Hardware failures, data damage or deletion (either accidental or deliberate), and properly executed requests from the office of the director, or forensic purposes.

B. Provide a document to policy of how long data is retained, and therefore restorable

C. Provide documentation of what systems and data are specifically included in, and excluded from, backup and retention.

D. Establish the groups or individuals responsible for data backup and retention procedures, including the on-site and off-site locations of backup media.

E. Establish the procedural guidelines used to initiate a data restore.

II. Scope

A. this policy applies to all servers and systems installed and controlled exclusively by the Benway School technology department and excludes servers and systems

controlled by specific departments within Benway School in cases where other departments are responsible for their backup system, the technology department will provide technical and professional guidance for back up routines and procedures, as requested

B. The policy applies to all user data in the following manner:

Users with network permissions are trained and urge to store data on to their server workspace, but they are permitted to store files on local machines. Individual users may delete their data from either network server or local machine at will. If data stored on a server is the end user and falls outside of the back-up, the system has no method of recovering such files.

File stored by users on individual hard drives or other individual storage devices are not backed up and maybe come unrecoverable in the case of the hard drive failure or accidental deletion. Although technicians may be able to locate or recover locally stored files, these files are not part of the data backup or recovery plan.

(C) This policy does not apply to Connected systems which are the property, and therefore the responsibility, of outside entities such as the New Jersey State Department of Education.

(D) This policy includes a special section for the email system as its backup and retention system is separate from other systems.

Danielle Bourne……..…..…...Director
Harry Carline ……..…….Administrator
Patrick McAloon……...…..Administrator
Julie Morganti …….Technology Coordinator
Joli Simpson ……..LDTC

Appendix A

Non-Disclosure Agreement

This non-disclosure agreement(this "Agreement"), by and between Benway School (the "School"), and _____ (the "Service

Provider), relates to the disclosure of valuable confidential information. The school refers to all school departments and other entities within Benway School. The service provider refer to any free or fee based company, organization, agency, or individual which is providing services to the school or is conducting school approved academic research. The disclosing party and the receiving party are sometimes referred to herein, individually as a “party” and collectively, as the “parties”.

To further the goals of this agreement, the parties may disclose to each other, information that the disclosing party considers proprietary or confidential.

The disclosure of Benways confidential information by receiving party may result in loss or damage to the school, it's students, parents, employees, or other persons or operations. Accordingly, the parties agree as follows:

Confidential information disclosed under this agreement by the school should only be transmitted in compliance with the schools approved security protocols. The receiving party must accept the data transmitted in these formats.

The service provider will request or receive confidential information from the school solely for the purpose of entering into or for filling its contractual obligation or pre-approved academic research.

The service provider will carefully Safeguard the district's confidential information and may be required to describe such safety measures to the school upon request.

The service provider will not disclose any aspect or portion of such confidential information to any third party, without the schools prior written consent.

Confidential information disclosed under this agreement shall not be installed, accessed or used on any computer, network, server or other electronic medium that is not the property of the school or the service provider, or to which third parties have access, unless otherwise provided in a separate contract or agreement between the parties here too.

The service provider shall inform the district promptly if the service provider discovers that an employee, consultant, representative were other party, or any outside party has made, or is making or threatening to make, unauthorized use of confidential information.

The service provider shall immediately cease all use of any confidential information and return all media and documents containing or incorporating any such confidential information within 5 days to the school after receiving written notice to do so, or whenever the contract for services between the school after receiving written notice to do so, or whenever the contract for services between the school and the service provider expires or is terminated. In addition, the service provider may be

required by the school to destroy any confidential information contained on primary or backup media upon written request from the school.

_____	_____
Date	Date
__Benway School_____	_____
School	Service Provider
_____	_____
Printed Name	Printed Name
_____	_____
Signature	Signature
_____	_____
Title	Title
_____	_____
Phone/Email	Phone/Email

Confidential Information includes:

* any written, electronic or tangible information provided by a disclosing party
* any information disclosed early by a disclosing party that is treated as confidential when disclosed
* all information covered by FERPA or other local, state, or federal regulations applying to educational agencies