Wilton-Lyndeborough Cooperative School District
School Administrative Unit #63

192 Forest Road Lyndeborough, NH 03082
603-732-9227

Data Governance Plan

Introduction

The Wilton Lyndeborough Cooperative School District is committed to protecting the privacy of our students, parents/guardians, and employees by maintaining strong privacy and security protections. The protection of this information is our top priority.

This manual outlines how operational and instructional activity shall be carried out to ensure that the district's data is accurate, accessible, consistent, and secured. This manual establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Wilton Lyndeborough Cooperative School District's Data Governance Manual shall be a living document. To make the document flexible, details are outlined in the appendices and referenced supplemental resources.

The Wilton Lyndeborough Cooperative School District's Data Governance Manual includes information regarding the data team, data and information governance, applicable School Board policies and district procedures, as well as applicable appendices and referenced supplemental resources.

Data Team

The Wilton Lyndeborough Cooperative School District's Data team consists of the following positions: Superintendent, Director of Curriculum, and the Director of Information Technology. Members of the Data Team will act as data stewards for all data under their direction. The Director of Information Technology will act as the Information Security Officer (ISO), with assistance of the information technology department. The IT technician for Florence Rideout Elementary School is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is unavailable. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. The Wilton Lyndeborough Cooperative School District provides its faculty, employees, and administrative employees access to technology devices, software systems, network, and internet services to support research and education. All components of technology must promote the educational objectives of Wilton Lyndeborough Cooperative School District and be used in ways that are legal, that are respectful of the rights of others, and protective of juveniles.

To that end, the district must collect, create and store confidential information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of all district stakeholders. All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect this information.

It is the policy of the Wilton Lyndeborough Cooperative School District that data or information in all its forms, written, electronic, or printed is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. All employees and authorized district contractors or agents using confidential information will strictly observe protections put into place by the district.

Scope

This data security manual's standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This plan applies to all forms of Wilton Lyndeborough Cooperative School District data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies.
- Hard copy, data printed or written.
- Communications sent by post/courier, fax, electronic mail, text, chat, and/or any form of social media.
- Data stored and/or processed by any electronic device, including servers, computers, tablets, and mobile devices.
- Data stored on any type of internal, external, or removable media or cloud based services.
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources.
- The terms data and information are used separately, together, and interchangeably throughout the plan, but the intent is the same.
- All involved systems and information are considered assets of the Wilton Lyndeborough Cooperative School District and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix A: Laws, Statutory, and Regulatory Security Requirements). The Wilton Lyndeborough Cooperative School District complies with the NH Minimum Standards for Privacy and Security of Student and Employee Data. The Wilton Lyndeborough Cooperative School District complies with all other applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)

- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Individuals with Disabilities in Education Act (IDEA)
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy
    - NH RSA 189:65 Definitions
    - NH RSA 189:66 Data Inventory and Policies Publication
    - NH RSA 189:67 Limits on Disclosure of Information
    - NH 189:68 Student Privacy
    - NH RSA 189:68-a - Student Online Personal Information
- New Hampshire Minimum Standards for Privacy and Security of Student
- New Hampshire State RSA - Right to Privacy:
    - NH RSA 359-C:19 - Notice of Security Breach - Definitions
    - NH RSA 359-C:20 - Notice of Security Breach Required
    - NH RSA 359-C:21 - Notice of Security Breach Violation

Data User Compliance

The Data Governance Manual applies to all users of Wilton Lyndeborough Cooperative School District's information including: employees, students, volunteers, and authorized district contractors or agents. All users of data are to maintain compliance with School Board Policies and District administrative procedures, EHAB (Data Governance and Security), GBEF (School District Internet Access for Employee), JICL (School District Internet Access for Students) and all policies, procedures, and resources as outlined within this Data Governance Manual and School Board Policy.

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term, or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district's technology resources.

Unless permission has been granted by the ISO or designee, no employee, vendor or other person may remove confidential or critical data from the district's premises or the district's network, remove a device containing confidential or critical data from the district's premises, or modify or copy confidential or critical data for use outside the district. If permission is given, the data may be accessed only on a district-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied, or otherwise used in a manner that would compromise the security and confidentiality of the information.

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined in accordance with CBA or terminated. Volunteers may be excluded from providing services to the district. The district will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the district reserves the right to seek all

other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The district may suspend all access to data or use of district technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. The district will cooperate with law enforcement in investigating any unlawful actions.

Any attempted violation of district policies, procedures, or other rules will result in the same consequences, regardless of the success of the attempt. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of personally identifying information (PII) or confidential information.
- Sharing your user IDs or passwords with others.
- Applying for a user ID under false pretenses or using another person's ID or password.
- Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
- The unauthorized copying of system files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district technological systems.
- The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to: laptops, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information.
- The introduction of computer viruses, hacking tools, or other disruptive or destructive programs.

Data Lifecycle

Data Governance is necessary at each phase in the data lifecycle. This lifecycle starts at evaluating the need for data collection and ends when the data is destroyed. It is important that appropriate safeguards, policies, procedures and practices are in place for each phase of the data lifecycle.

Identifying Need & Assessing Systems for District Requirements

To accomplish the district's mission and to comply with the law, the district may need to maintain confidential information, including information regarding students, parents/guardians, employees, applicants for employment, and others. The district will collect, create, or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

District employees are encouraged to research and utilize online services or applications to engage students and further the district's educational mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or employees, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and School Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.
Memorandums of Understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects, or uses personally identifiable information (PII), student records, or confidential data must be reviewed by the ISO prior to initiation.
All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment, including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements, including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - The district continues to own the data shared, and all data must be available to the district upon request.
    - The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising, or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
    - District data will be maintained in a secure manner by applying appropriate technical, physical, and administrative safeguards to protect the data.
    - The online or application service provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - All data will be treated in accordance to federal, state, and local regulations
    - The provider assumes liability and provides appropriate notification in the event of a data breach.

Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent and/ or guardian permission is requested during the yearly registration process for district vetted and approved applications and tools.

A current list of all vetted and approved software systems, tools and applications is published here.

Review of Existing Systems

The District will ensure that data collection is aligned with School Board Policy EHAB. Data systems shall be regularly reviewed to ensure that only necessary data is being transmitted and collected.

Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for employees and students.

The district must ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by their terms of service.

The District will audit data imports annually. These audits should include:

- Review of provider's terms of service to ensure they meet the district's data security requirements.
- Verification that software imports are accurate and pulling correct information.
- Verification that, when applicable, the employees, students, and classes included in the imports are still necessary for instructional purposes (only those that need data collected are included in import).
- Determine if the fields included in the imports are still necessary for the intended purpose.

Storage and Management

Systems Security

The district will provide access to confidential information to appropriately trained district employees and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district (School Board Policy EHAB). Therefore, systems access will only be given on an as needed basis as determined by the data manager and ISO.

Data Management

The effective education of students and management of district personnel often require the district to collect information, some of which is considered confidential by law and district policy. In addition, the district maintains information that is critical to district operations and that must be accurately and securely maintained to avoid disruption to district operations.

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. All district administrators are data managers for all data collected, maintained, used, and disseminated

under their supervision, as well as data they have been assigned to manage. Data managers will:

- Ensure that system account creation procedures and data access guidelines appropriately match employee's job functions with the data on instructional and operational systems;
- Review all employees with custom data access beyond their typical group's access;
- Review district processes to ensure that data will be tracked accurately;
- Review contracts with instructional and operational software providers to ensure that they are current and meet the district data security guidelines;
- Ensure that employees are trained in the district's proper procedure and practices in order to ensure accuracy and security of data;
- Assist the ISO in enforcing district policies and procedures regarding data management.

Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format (see Appendix D: Data Classification Levels).

The ISO or designee will identify all systems containing district data, such as student information systems, financial systems, payroll systems, transportation systems, food service systems, email systems, instructional software applications and others. The ISO or designee will identify the data files and data elements maintained in those systems and identify confidential and critical information the district possesses or collects.

The district will create and maintain a data inventory for all information systems containing PII or confidential information. When possible, a data dictionary will be maintained for critical information systems. The data inventory will contain the following elements:

- Data Source
- What data is stored
- Where the data is stored
- Employee or Employee categories that have access to the data

Security/Protection

Risk Management

A thorough risk analysis of all Wilton Lyndeborough Cooperative School District's data networks, systems, policies, and procedures shall be conducted as requested by the Superintendent, ISO, or designee. An internal audit of district network security will be conducted annually by District Technology employees. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist (Appendix D). The product of the risk

analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risks to an acceptable level by reducing the extent of vulnerabilities.

Physical Security Controls

Most technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Director of Information Technology and/or the Director of Facilities. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix F: Physical Security Controls). No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix G: Asset Management).

Inventory Management

The district shall maintain a process for inventory control in accordance with federal and state requirements and School Board policy. All district technology assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix G: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

The district uses a multi-layered approach to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus/malware/ spyware software, group policy, gateways, firewalls, and content filters. Users shall not turn off or disable district protection systems or install other systems (see Appendix H: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

District employees will only access personally identifiable and/or confidential information if necessary to perform their duties. The district will only disclose this information to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law.

Mechanisms to control access to PII, confidential information, internal information, and computing resources include, but are not limited to, the following methods:

- **Identification/Authentication**: Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, confidential information, and/or internal information. Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.
- **Authorization**: Access controls are maintained through a partnership between the technology department, human resources (HR), and data managers

Additionally, only employees of the district Technology Department or authorized contractors will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Employee Users

All new employee accounts are authorized through an HR hiring process (see Appendix I: Account Management). Role-based permissions and security groups are used to establish access to all systems (see Appendix J: Data Access Roles and Permissions). If an employee requires additional access, a request must be made directly to the ISO with a clear justification for access.

Contractors/Vendors

Access by contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by the ISO. Once the approval has been obtained, the technology department will create the account, only granting access to the server/application that the contractor/vendor supports.

Password Security

The District will enforce secure passwords for all systems within their control (see Appendix K: Password Security). When possible, the district will utilize Single Sign On (SSO) or LDAP/Active Directory Integration to maintain optimal account security controls.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices, data in transit, and data stored on additional resources. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process. Regular transmission of student data to internal and external services is managed by the technology department using a secure data transfer protocol.

Users must ensure that they are securely storing their data. Guidelines have been established for Cloud Storage and File Sharing, External Storage Devices, and File Transmission Practices (see Appendix E: Securing Data at Rest and Transit). These guidelines are outlined in the following section.

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. All district employees, volunteers, contractors, and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe protections put into place by the district including, but not limited to, maintaining

information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

All users are responsible for the security and integrity of the data they create, store, or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority. Users must follow all guidelines outlined with School Board policies, specifically Employee and Student Technology Usage (GBEF, JICL, JICJ), Data Governance and Security (EHAB), and Student Records (JRA, JRA-R).

District employees, contractors, and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

Data Storage and Transmission

All employees and students who log into a district-owned PC computer will be provided with several options for data storage and transmission. Employees and students will need to ensure that they are securely storing their data. Employees with windows machines will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Employees and students using Chromebook devices have limited local storage capabilities. Chromebook users are to store data within their Google GSuite for Education Drive account.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the Internet. All employees and students are provided with a Google GSuite for Education. Users are responsible for all digital content on their district-provided Google GSuite for Education Drive (see Appendix F: Securing Data at Rest and Transit).

File Transmission Practices

Employees are responsible for securing sensitive data for transmission through email or other channels. Employees shall not transmit files to third party file transfer services without district approval. When possible, employees should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to services such as a single sign-on provider is managed by the technology department using a secure data transfer protocol (see Appendix E: Securing Data at Rest and Transit).

Mass Data Transfers

Downloading, uploading, or transferring PII, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be reviewed and approved by the Superintendent, ISO or designee.

Printing

When possible, employees should de-identify or redact any PII or confidential information prior to printing. PII and confidential information shall not be downloaded, copied or printed indiscriminately, or left unattended and open to compromise.

Oral Communications

Employees shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of cellular telephones in public areas. Employees shall not discuss PII or confidential information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Training

The district shall create and maintain an annual data security training plan. This plan will consist of the following:

- Training for all employees on technology policies and procedures, including confidentiality and data privacy and cybersecurity.
- Training for all new employees on technology policies and procedures, including confidentiality and data privacy and cybersecurity (training must be completed within 21 days of account creation).

Archival and Destruction

Once data is no longer needed, the ISO or designee will work with the data managers to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record unretrievable.

District Data Destruction Processes

The district will regularly review all existing data stored on district-provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. District data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student Google GSuite for Education accounts will be maintained for one school year after the student’s final date of attendance, or until the 1st of July after graduation

whichever comes first. Students only have access to download their data, and must contact ISO or designee for additional access.
- Employee Google GSuite for Education accounts will be suspended after the final work day, unless the ISO approves to maintain access.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance with School Board policy (DN). The district will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed (see Appendix G: Asset Management).

Critical Incident Response

Controls shall ensure that the district can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach, and natural disaster) that damages/breaches data or systems.

Business Continuity

The district's administrative procedure EHB-R delineates the timeline for data retention for all district data. The district will maintain systems that provide off-site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test off-site backups of critical systems semi-annually.

Disaster Recovery

The district's Technology Disaster Recovery Plan outlines critical employee responsibilities and processes in the event of a disaster or critical data loss. The District shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the district to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure (see Appendix L: Disaster Recovery Plan).

Data Breach Response

New Hampshire's Data Breach Law (RSA 359-c:19, 20, 21) is triggered when a school district computer system is breached and personal information is acquired without authorization in a way that compromises the security or confidentiality of the information. The law requires a school district experiencing a breach to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information was, or will be, misused. The

Data Breach Response Plan enables the district to respond effectively and efficiently to a data breach involving personally identifiable information (PII) as defined by NH Law, confidential or protected information (ie-FERPA), district identifiable information, and other significant cybersecurity incidents. The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix M: Data Breach Response Plan).Critical Incident Response Controls shall ensure that the district can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach, and natural disaster) that damages/breaches data or systems.