BURKE COUNTY Public Schools

Igniting Learning For A Brighter Future

Data Governance Manual

Introduction

The District is dedicated to safeguarding the privacy of students and staff through robust privacy and security measures. The BCPS Data Governance Manual provides information on the data governance team, policies, procedures, and forms, outlining how operational and instructional activities ensure accurate, accessible, consistent, and protected data. Responsibilities, procedures, and definitions are specified in the manual, which is designed to be a living document with details in appendices and supplemental resources. Any updates will be available on the District's website.

Data Governance Team

The BCPS Data Governance team consists of the following positions: Superintendent, Chief Information Officer, Chief Financial Officer, Director of Human Resources, Director of Testing and Accountability, and wide area network engineer. Members of the Data Governance Team will act as data stewards for all data under their direction. The Chief Information Officer (CIO) will act as the Information Security Officer (ISO), with assistance from the Digital Teaching and Learning Department. The wide area network engineer is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

Burke County Public Schools' technology aims to enhance student education and achievement. Access to technology has been shown to improve student outcomes, support staff professional development, and engage families and district patrons, positively influencing student success. To fulfill the district's mission and comply with the law, it is crucial to collect, create, and safeguard confidential information. Maintaining and protecting this data ensures efficient district operations, legal compliance, and the trust of stakeholders.
All individuals with access to district data must adhere to state and federal laws, district policies, and protective measures. The district's policy follows the State's Records Retention and Disposition Schedule in safeguarding of data in all forms—written, electronic, or printed—throughout its life cycle. This includes implementing security measures for equipment, software, and practices involved in processing, storing, and transmitting information. All employees and authorized contractors must strictly adhere to the district's established protections for confidential information.

Scope

The data security policy, 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 policy applies to all forms of Burke County Public Schools' data and information, as all data are considered assets requiring protection from misuse, unauthorized manipulation, and destruction, including but not limited to:

- Speech and communication methods include face-to-face interactions, phone conversations, and current/future technologies.
- Hard copy data encompasses printed or written information.
- Digital communication channels, such as post, fax, electronic mail, text, chat, and social media, as well as data storage and processing on electronic devices or cloud services, are covered.

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). Burke County Public Schools complies with all 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)
- Protection of Pupil Rights Amendment (PPRA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- NC Senate Bill 49 "Chapter 114A. "Parents' Bill of Rights"

Data User Compliance

The Data Governance Manual applies to all users of Burke County Public Schools' information including: employees, staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with the Board of Education Policies and resources as outlined within this Data Governance Manual.

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 CIO 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.

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Students may be suspended or expelled. 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. The Superintendent, School Board chair, or Board lawyer has the authority to sign any criminal complaint on behalf of the district.
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 PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized Digital Teaching and Learning (DTL) staff for the purpose of support)
- 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 crucial at every stage of the data lifecycle, commencing with the assessment of the necessity for data collection and concluding upon the data's destruction. Ensuring the presence of suitable safeguards, policies, procedures, and practices is essential for each phase of the data lifecycle.
Burke County Public Schools follows the North Carolina Records Retention and Disposition Schedule.
https://archives.ncdcr.gov/local-public-school-units-schedule/open

New Systems and Review of Existing Systems

District staff should use online services or apps for student engagement and the district's educational mission. Before using or purchasing any service/app that collects confidential information, CIO approval is necessary to ensure compliance with the law and Board policy, and the protection of such information. This applies even when services are obtained for free.

The Burke County School District has an established process for vetting new resources. Staff are required to complete a request form that can be found on the digital teaching and learning webpage as outlined in the Staff Technology Handbook.
Memorandums of understanding (MOU) or contracts for any system that create, collect or use personally identifiable information (PII), student records or confidential data must be reviewed by the superintendent or designee prior to initiation.
All new resources will be properly vetted by the CIO and the DTL department ensuring that they are aligned with the network and educational curriculum standards. All resources will also have to be in complaint with the North Carolina Vendor Readiness Agreement. Existing systems are vetted as necessary by the CIO or designee.

The District will ensure that data collection is aligned with Board Policy. 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 staff 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.

Acquisition and Creation

Upon approval, new systems or services will be processed for student and staff use and limit shared data to only directory information following the NC Vendor Readiness Agreement. Exceptions can be made if there are specific data requirements to utilize the vendor. Efforts will be made to safeguard student and staff PII.
The DTL department will use the following guidelines regarding digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the CIO prior to initiation.
- Ensure that all electronic resources are age appropriate, FERPA compliant, and are in compliance with software agreements before requesting use.
- Properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is instructionally sound, and is appropriate for the intended use.
- Utilize Classlink to ensure system account creation procedures and data access guidelines appropriately match employee job function with the data on instructional and operational systems.
- Proper procedures and practices are in place to ensure accuracy and security of data.

Management and Storage

Systems Security

The district will grant confidential information access to authorized employees and approved contractors or agents essential for district services. Access will be provided based on administrative determination and is subject to legal and district authorization.Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this manual. (maybe)

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 accuracy and security of data in the Student Information System. Data managers will:

- ensure that system account creation procedures and data access guidelines appropriately match employee job function with the data on instructional and operational systems.
- assist the CIO and administrators in following district policies and procedures regarding data management.
- Assist parents and guardians with access to their student(s) data.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices or on additional resources, such as cloud storage. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process.
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. These guidelines can be found in the Usage and Dissemination section below (see Appendix F: Securing Data at Rest and Transit).

Security/Protection

Risk Management

A thorough risk analysis of all BCPS data networks, systems, policies, and procedures shall be conducted in partnership with Microelectronics Center of North Carolina, MCNC on an annual basis or as requested by the Superintendent, CIO or designee. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist. 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 risk to an acceptable level by reducing the extent of vulnerabilities (see Appendix D: Data Security Checklist).

Security Logs

The District will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

Cloud reports from Ruckus, Crowdstrike, Google Admin, Cloud reports from LINQ, Windows Security Updates, as well as Apple product updates.

Logon Banners

The district will ensure that staff, students and parents using district systems are aware of the district data security policies. When possible, district systems users will acknowledge the full technology usage agreement prior to accessing all district technical systems.

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Chief Information Officer. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix G: Physical Security Controls). No technological systems shall be disposed of or moved without adhering to the appropriate procedures following School Board Board Policy 9400. (see Appendix H: Asset Management).

Inventory Management

The district shall maintain a process for inventory control in accordance with federal and state requirements and Board policy. All district assets will be maintained in inventory (LINQ) and verified through the regular inventory verification process following School Board Policy 8350. (see Appendix H: 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 to install other systems following School Board Policy 3225/4312/7320. (see Appendix I: 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 (UID) 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 UID. User accounts and passwords shall not be shared.
- Authorization: Access controls are maintained through a partnership between the DTL department, human resources (HR) and finance.

No user will be granted local administrator permissions unless required for the use of a specific software/application.
Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Employee Users

All new employee accounts are authorized through an HR hiring process (see Appendix J: Account Management). Role-based permissions are used to establish access to all systems (see Appendix K: Data Access Roles and Permissions). If an employee requires additional access, it must be completed and approved by the district data manager and Chief Information Officer.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using Board of Education policy 6442. All contractor/vendor access must be approved by HR and CIO. All contractors doing business on fdistrict premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. 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. Secure password requirements have been established. When possible, the district will utilize Single Sign On (SSO) or Active Directory Integration to maintain optimal account security controls.

Concurrent Sessions

When possible, the district will limit the number of concurrent sessions for a user account in a system.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the CIO. Remote access is granted through our firewall; no other method of remote access shall be granted without explicit authorization from the CIO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the District's network.
In the event that remote access is needed by a contractor/vendor, access must be approved by the CIO. The Network System Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports. All remote access accounts will be reviewed at least annually.

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 staff, 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 regulatory acts including CIPA, COPPA, FERPA, PPAA, HIPAA, PCI DSS and NC Senate Bill 49 "Chapter 114A. Users must also adhere to guidelines outlined with School Board Policies, specifically Technology Responsible Use(3225/4312/7320), Data Governance and Security(2125/7315), Staff Conduct(7305), and Student Records(4700, 4720, 4705/7825-R)

District employees, contractors and agents will notify the CIO 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.

Securing Data at Rest and Transit

All staff and students that log into a district issued computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on their 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. Staff and students may also have mapped personal and shared folders. These folders map to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts.

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 staff and students are provided with a Google Workspace for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided Google Apps for Education Drive (see Appendix F: Securing Data at Rest and Transit).

File Transmission Practices

Staff are responsible for securing sensitive data for transmission with their Google Workspace for Education account. All efforts should be made to limit access to files to appropriate school system staff. Staff should never transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval. Prior to transmission, administrators will de-identify or redact any PII or confidential information. Regular transmission of student data to services such as a learning management system is managed by the DTL department using a secure data transfer protocol (see Appendix F: Securing Data at Rest and Transit).

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such data (see Appendix F: 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 in accordance with Board policy 4700. All other mass downloads of information shall be approved by the Superintendent or designee and include only the minimum amount of information necessary to fulfill the request.

Printing

PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

Staff shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of phones in public areas. Staff 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 maintain a data security training program. This program will consist of the following:

- Initial training for all new staff is provided on technology policies and procedures, digital communication, confidentiality and data privacy, federal regulations, the use of digital resources and student electronic records.
- Annual and ongoing training for all staff is provided on technology policies and procedures, confidentiality and data privacy, federal regulations, the use of digital resources and student electronic records.

Archival and Destruction

Archival and destruction of student records is completed in accordance with the North Carolina Records Retention And Disposition Schedule

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. Student Google Workspace for Education accounts are disabled upon withdrawal date, and graduating students retain their accounts for 6 months following graduation, when their accounts are disabled. Data destruction processes will align with School Board Policies 4700 and 4705, as well as North Carolina Records Retention And Disposition Schedule and exceptions will be made for data in an active litigation and will be maintained until the conclusion of litigation.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance with School Board policy 6510. 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 H: Asset Management).

Critical Incident Response

Each school, department, or individual is required to report any instances immediately to the Superintendent, CIO, or designee for response to a system emergency. This ensures that the district can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time.

Business Continuity

The district utilizes a variety of cloud-based systems to house and maintain sensitive data, these vendors are required to backup data to ensure full recovery. We do not store sensitive data locally.

Incidence Response

The Incidence Response Plan was developed in partnership with NCDPI, MCNC, and The Friday Institute. It is reviewed, updated, and tested at least annually to ensure the incident response process remains up to date with organizational changes and the evolving threat landscape. Only through rigorous testing can an organization identify vulnerabilities, refine procedures, and ensure a swift, effective response to cyber threats, ultimately safeguarding sensitive data and maintaining business continuity.

Appendix A: Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons.
Confidential Data/Information: Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (PII) regarding students and employees.
Critical Data/Information: Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.
Data: Facts or information. Data can be in any form; oral, written, or electronic.
Data Breach, Breach of Security or Breach: A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information.
Data Integrity: Data is current, accurate and has not been altered or destroyed in an unauthorized manner.
Data Management: The development and execution of policies, practices, and procedures in order to manage the accuracy and security of district instructional and operational data in an effective manner.

Chief Information Officer: The Chief Information Officer (CIO) is responsible for working with the superintendent, Data Governance Team, data managers, and users to develop and implement prudent security policies, procedures, and controls. The CIO will oversee annual security audits and will act as an advisor to:

- systems development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.

Systems: 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, whether hosted by the district or provider.
Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, SIS ID, date and place of birth, mother‘s maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes but is not limited to (a) student’s name; (b) name of the student’s parent or other family members; (c) address of the student or student’s family; (d) a personal identifier, such as the student’s social security number, student number, or biometric record; and (e) other indirect personal identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) “medical information” as may be defined in state law; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; (h) nonpublic personal information as that term is

defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; (i) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; (j) other financial account numbers, access codes, driver's license numbers; (k) and state- or federal-identification numbers such as passport, visa or state identity card numbers; (l) personal identifiable information as defined by COPPA, including but not limited to online contact information like an email address or other identifier that permits someone to contact a person directly (for example, an IM identifier, VoIP identifier, or video chat identifier), screen name or user name where it functions as online contact information, telephone number, persistent identifier that can be used to recognize a user over time and across different sites (including a cookie number, an IP address, a processor or device serial number, or a unique device identifier), a photo, video, or audio file containing a child's image or voice, geolocation information sufficient to identify a street name and city or town; or other information about the child or parent that is collected from the child and is combined with one of these identifiers.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

User: The user is any person who has been authorized to read, enter, print or update information. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).
- report promptly to the CIO the loss or misuse of data.
- follow corrective actions when problems are identified

Appendix B: Laws, Statutory, and Regulatory Security Requirements

CIPA: The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. http://www.fcc.gov/guides/childrens-internet-protection-act

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information. www.coppa.org

FERPA: The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1)), as amended from time to time, applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well. http://www.hhs.gov/ocr/privacy/hipaa/understanding

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. www.pcisecuritystandards.org

NC Senate Bill 49 "Chapter 114A. "Parents' Bill of Rights: The NC Senate Bill 49 "Chapter 114A" outlines parental rights regarding their children's education and healthcare in North Carolina.

It does this by:

- Granting parents access to review school materials and their child's library records.
- Mandating parental consent for most healthcare decisions regarding minors.
- The right to opt in to certain data collection for their child
- The right to opt in to protected information surveys

Appendix C: Digital Resource Acquisition and Use

The purpose of the Digital Resource Acquisition and Use process is to:

- ensure proper management, legality and security of information systems.
- interoperability with existing network infrastructure and hardware
- increase data integration capability and efficiency.

New Resource Acquisition

Staff are required to complete the Website/Software/App Request Form, pending approval by the DTL/CIO

- Contracts for any system dealing with personally identifiable information (PII), student records, or confidential data must undergo review by the Chief Information Officer (CIO) and comply with the requirements outlined in the NC Vendor Readiness Agreement before initiation.

- Prior to requesting the use of electronic resources, it is mandatory that they are age-appropriate, FERPA compliant, and align with software agreements.

- Staff members requesting digital content are responsible for collaborating with the CIO/DTL department to thoroughly vet the resource. This process ensures alignment with district objectives, adherence to curriculum or behavioral standards, instructional soundness, and appropriateness for the intended use.

- Digital resources accompanying adopted instructional materials undergo scrutiny by the Superintendent and the Chief Information Officer, or their designee, before any purchase is made, ensuring a comprehensive and compliant approach to digital content acquisition.

Approved Digital Resources

- To ensure compliance with security guidelines and prevent the use of software containing malware, viruses, or other security risks, evaluated digital resources are categorized as Approved or Denied. Prior to approval or denial, these resources must receive approval from the Chief Information Officer or a designated representative.
- A comprehensive list of evaluated software will be maintained on the District Technology site for reference. It is the responsibility of staff to submit a request for a resource review if a particular resource is not listed as approved, denied, or under review.
- Resources labeled as denied or those that have not yet undergone review are not permitted on district-owned devices or for use in district business or instructional practices, ensuring a secure and controlled digital environment.

Digital Licensing/Resource Use

- All computer software used by district employees or contract personnel on behalf of the District, whether licensed or purchased, is the property of the District. It should not be copied for use at home or any other location, unless explicitly allowed by the license agreement.
- Staff members are required to adhere to the following guidelines related to digital resource licensing and use:

1. Only approved district resources should be utilized.
2. District software licenses must be kept on file in the technology office.
3. Licenses must be accurate, up-to-date, and adequate.
4. Compliance with all copyright laws and regulations is mandatory.
5. Adherence to district, state, and federal guidelines for data security is required.
6. Software installed on BCPS systems and other electronic devices should have a current license on file.
7. Digital resources accessed from or storing data in a cloud environment must have completed and adhere to the NC Vendor Readiness Agreement.
8. Staff members cannot act as parental agents when creating student accounts for online resources; such resources requiring parental permission must be approved at the district level.

Appendix D: Data Security Checklist

An in-depth risk analysis of all BCPS data networks, systems, policies, and procedures is conducted annually or as requested by the Superintendent, CIO, or a designated representative. The Data Security Checklists are utilized to assess various threats that may impact the management and protection of information resources. This analysis identifies vulnerabilities within each entity, which could potentially expose information resources to threats. Additionally, the evaluation encompasses information assets and the technology associated with their collection, storage, dissemination, and protection.
By considering threats, vulnerabilities, and asset values, an estimation of the risks to the confidentiality, integrity, and availability of information is determined. This culmination is referred to as the risk assessment. The risk assessment is instrumental in devising a plan to mitigate identified threats and risks to an acceptable level by reducing vulnerabilities. This proactive approach ensures the ongoing security and resilience of BCPS data networks and systems.

Data Security Checklist for Cloud Based & Provider Hosted Systems

- Bi-annual MCNC network assessments provided by NCDPI
- Provider has adequate data security measures including data management and incident response
- Completion of all NCDPI Data Confidentiality and Security Agreement for Online Service Providers and Public School Units
    - Authentication methods (SIS, Active Directory, Single Sign On, District managed account, user managed account)
    - Inventory and classification of data on system
    - Ability to maintain critical system event logs
    - Ability to receive notification for critical system events

Appendix E: Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications.

Confidential Information

Confidential Information is of utmost importance, representing highly sensitive material that does not fall under the classification of Personally Identifiable Information (PII). This type of information is private or otherwise sensitive and is to be restricted to individuals with a legitimate business need for access. Examples of confidential information encompass a range of sensitive data, including but not limited to student records, personnel information, key financial details, proprietary information, as well as system access passwords and encryption keys. The stringent control and restriction of access to confidential information ensure its privacy and protection from unauthorized disclosure or use. Employees must follow School Board Policy 4700 and School Board Policy 4705/7825-R relating to student and staff confidential information.
Unauthorized disclosure of this information to individuals without a business need for access may violate laws and regulations, or may cause significant consequences for the district, its staff, parents, students or other stakeholders. Decisions about the provision of access to this information shall always be cleared through the data manager and/or CIO.

Internal Information

Internal Information is designated for unrestricted use within the district and, in certain cases, among affiliated stakeholders. This information is either widely distributed within the district or can be shared within the organization without the need for advance permission from the information owner. Examples of Internal Information encompass internal policies, procedures, and handbooks.

However, unauthorized disclosure of this information to external parties may be deemed inappropriate, considering copyright, legal, or contractual provisions.

Directory Information, on the other hand, refers to information contained in a student's education record that is generally considered non-harmful or a privacy invasion if disclosed without the consent of a parent or eligible student. This classification helps strike a balance between the need for information sharing and the privacy rights of students.
Directory information should only be shared following School Board Policy 3225/4312/7320.

Public Information

Information approved for public release by the Chief Information Officer or the relevant district administrator is considered public information. Examples of such information include patron mailings and materials posted on the district's website. This information is permissible for disclosure outside the district.

Appendix F: Securing Data at Rest and Transit

Upon logging into a district-provided computer, both staff and students will be granted access to cloud data storage and transmission. They have the option to store data on their local devices. It's crucial to highlight that this data is not included in the district's continuity plan and will not be backed up by the district's backup solution.

Cloud Storage

Regarding Cloud Storage and File Sharing, the term "Cloud Storage" encompasses all types of remote server storage accessed via the internet. All staff and students receive a Google Apps for Education account, and they are responsible for managing all digital content on their district-provided Google Workspace for Education Drive. When utilizing cloud storage, staff must adhere to the following guidelines:

- Staff and students are restricted from accessing cloud storage through third-party applications outside of approved internet browsers and Google Drive. This policy ensures that native operating systems do not compromise cloud sharing security and examples of unapproved applications.
- Users must be mindful of default sharing settings when uploading files and are obligated to limit file sharing to a necessary basis. It is imperative that staff and students only use cloud storage providers approved by the district, meeting established student data and data security standards.
- When exiting the district, staff members must ensure that they only copy personal content they have created. Copying content containing confidential information, student records, or district-created curricular or operational documentation, files, or data is strictly prohibited.
- Data containing personally identifiable information of staff or students may be posted to users' district-provided Google Drive with appropriate security settings. However, posting such data to other cloud sharing platforms without the consent of district administration is not allowed. Additionally, staff should refrain from posting documents labeled classified, confidential, or restricted to any cloud storage, including district-provided Google Drive accounts, without district approval.
- Users are required to immediately report any cloud storage security problems related to the district's technology resources to a teacher or administrator. Unauthorized attempts to gain access or actual unauthorized access to cloud storage or the files of others are strictly prohibited.

- Similar to other forms of district technology, district employees, students, and other Google Apps for Education drive users should be aware that they have no expectation of privacy regarding data stored on this platform.

The term "File Sharing" refers to all activities involving the sharing of access to digital information. When engaging in file sharing, staff is required to follow the guidelines outlined in School Board Policy 3225/4312/7320:

- Users must comply with all policies and procedures related to professional conduct and communication while sharing, reviewing, updating, commenting, and re-sharing.
- When sharing content, users must verify that other individuals accessing the information in the files have appropriate access based on their job function.

--

- All users are obligated to promptly report any instances of inappropriate sharing of the district's technology resources to an administrator.

External Storage Devices

The term "External Storage Devices" encompasses all portable storage devices, such as USB drives, memory cards, and external hard drives, utilized by staff on a MacBook and students on a Chromebook. It's important to note that the use of external storage devices is not allowed on Windows devices due to security concerns. All users must adhere to School Board Policy 3228/7323 which prohibits the storing of school business related information on personal external storage devices unless specifically authorized by the Superintendent or designee in writing. Although the district acknowledges the benefits of users maintaining information on these devices, it strongly encourages staff and students to depend on their district-provided Google Apps for Education Drive account for all storage requirements. When opting to use external storage devices, staff must comply with the following guidelines:

- Users bear responsibility for all content stored on external storage devices connected to district technology resources. It is imperative that users refrain from introducing harmful software, such as computer viruses, malware, non-district approved software, or hacking tools, to district technology resources.
- To uphold security standards, users must ensure the data's confidentiality through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device. It is advised to retain information on the external device only for the project's duration and promptly remove it afterward.
- Staff members are strictly prohibited from transferring any documents labeled classified, confidential, or restricted to external storage devices. Furthermore, they should refrain from transferring or creating confidential data or student records on personal storage devices.
- Upon leaving the district, staff members must take the necessary steps to delete any district-created or provided curricular or operational documentation, files, or data from their personal external storage devices.

File Transmission Practices

- Policies and guidelines regarding file storage extend to files in transit, placing the responsibility on individuals to secure sensitive data during transmission using encryption or a password. Classified, confidential, or restricted information should not be transferred through email, Google Drive, external storage devices, or third-party file transfer services.
- Staff members are accountable for ensuring the security of sensitive data during transmission through email or other channels, utilizing encryption or a password. It is crucial that staff never include a password in any communication with the actual file attached that is being protected by the password.
- Moreover, staff should refrain from transmitting files labeled classified, confidential, or restricted through email or third-party file transfer services without obtaining prior district approval.
- Routine transmission of student data to services such as a learning management system is overseen by the DTL department using a secure data transfer protocol. All such services are approved by a district/building administrator and the Chief Information Officer, ensuring a controlled and secure data transmission process.

Credit Card and Electronic Payment

Users of systems involved in processing electronic payments, including the handling of credit card information, must strictly adhere to guidelines for safeguarding payment information and cardholder data. Compliance with the following requirements and an appropriate level of PCI compliance is mandatory:

- No Storage of Cardholder Data: Cardholder data should never be stored on district systems or in written form. All such data may only be entered into secured payment systems that have been approved by the district. Any cardholder data collected in written form must be immediately shredded after entry into the approved system.

- Third-Party Processing: The district will not maintain a data system for payment information. All payment information will be stored and processed by a third party accessible through a secure portal.

- No Transmission via Email or Electronic Communication:** Users must never request cardholder information to be transmitted via email or any other electronic communication system.

- Direct Entry into Approved Payment System: Payment information should be entered directly into the approved payment system by individuals making the payment. If the individual is unable to directly input the payment, designated staff may obtain verbal approval for the payment process, either in person or via phone (after verifying identification). If verbal payment information is received, it must be entered directly into the payment system and should not be written down during the process.

Appendix G: Physical Security Controls

The following measures for physical security controls must be followed:

- Network systems must be installed in an access-controlled area that provides protection against fire, water damage, and other environmental hazards such as power outages and extreme temperatures. It is crucial to monitor and maintain the temperature and humidity levels in data centers.
- Physical storage containing PII, Confidential, and/or Internal Information should be in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Computers and other systems must be secured to prevent use by unauthorized individuals. Users are responsible for ensuring that devices are not left logged in, unattended, and open to unauthorized use.
- The delivery and removal of all asset-tagged and/or data-storing technological equipment or systems must be monitored and controlled. A record of all such items entering or exiting their assigned location should be maintained using the district-approved technology inventory program. No technology equipment, regardless of how purchased or funded, shall be moved without explicit approval from the DTL department.

Appendix H: Asset Management

Data security must be upheld throughout the lifespan of an asset, which includes the proper destruction of data and the disposal of assets. The term "system," "asset," or "device" encompasses 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.
All systems and information involved are considered assets of the district and should be safeguarded against misuse, unauthorized manipulation, and destruction. It is imperative to prioritize the protection of these assets to ensure the overall security and integrity of the district's data.

Inventory

The technology department is responsible for maintaining an inventory of all devices or systems deemed assets, which encompasses a range of items such as network appliances, servers, computers, laptops, mobile devices, and external hard drives. Ongoing verification of staff and student devices will be conducted by the technology department.
It is a collaborative responsibility between the technology department and building staff to ensure the inventory system is updated to accurately reflect any in-school transfers, in-district transfers, or other location changes for student and staff devices. This shared effort aims to keep the inventory system current and aligned with the actual distribution and location of devices within the school or district. .

Disposal Guidelines

Assets are evaluated for disposal in adherence to state/federal regulations and School Board policy 6560.
The following criteria are taken into consideration when assessing an asset for disposal:

- End of useful life
- Lack of continued need
- Obsolescence
- Wear, damage, or deterioration
- Excessive cost of maintenance or repair

The Chief Information Officer is required to approve the disposal of any district technology asset.
Documentation of the asset disposal must include details such as the asset tag number, description, serial number, and the method of disposal. This systematic approach ensures compliance with regulations and policies while maintaining transparency in the disposal process.

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be managed according to one of the following methods. The technology department is tasked with the responsibility of updating the inventory system to accurately reflect the disposal of the asset.
Salvage
All technology assets must undergo salvage in accordance with relevant environmental regulations. Furthermore, systems may house Personally Identifiable Information (PII), Confidential, or Internal

Information, and as such, they must be thoroughly wiped clean of this information during the disposal process.

For the disposal of all technological systems/equipment, the district shall engage a district-approved vendor. This vendor is required to furnish written documentation confirming the disposal method used and provide a certificate asserting that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash. This ensures compliance with environmental regulations and the secure disposal of sensitive information.

Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

BCPS desktops, laptops, and file servers are protected using enterprise virus/malware/spyware software. Definitions are updated weekly and an on-access scan is performed on all “read” files continuously. A full scheduled scan runs monthly. A full scheduled scan is performed on all servers monthly during non-peak hours. All files and systems are scanned.

Internet Filtering

The utilization of online content and collaborative learning among students is on the rise. BCPS sees Internet filtering as a means to strike a balance between safety and learning, allowing positive content, resources, and connections while preventing access to harmful ones. In order to maintain an equilibrium between educational internet resources, application usage, student safety, and network security, all internet traffic from devices within the district network is directed through the district firewall and content filter. Authentication is mandatory for personal devices before gaining access to the district network, determining the appropriate filtering level based on the role of the guest user. The district ensures that sites associated with malicious software, phishing, spyware, etc., are blocked for a secure learning environment.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using Google services.

Security Patches

Security patches are applied on an as needed basis. Workstations are checked on a regular basis for security patches. These patches are applied on an as needed basis.

Appendix J: Account Management

Securing data integrity and security necessitates effective access controls. Burke County Public Schools adheres to a rigorous procedure for initiating and concluding district accounts. Each new employee account undergoes authorization through the HR hiring process before being created. Role-based permissions play a crucial role in determining access to all systems. Access security undergoes an annual audit, or whenever there are changes in access permission requirements for a specific application/software, or when an application/software is deemed unnecessary. This ensures a proactive approach to maintaining a secure and controlled access environment.

Employee Accounts

When an employee is hired by BCPS, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of new employees is sent from Human Resources to the DTL Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the DTL Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (data manager) and the Chief Information Officer.

When a staff member's employment is ended, either by termination, retirement, or resignation, account permissions are revoked in one of three ways.

- In the event of termination, HR will send immediate notification via email or phone call to the CIO requiring accounts to be disabled at once, preventing any further access to district resources.
- In the event of resignation, HR sends a Suspension of Service to Technology, indicating the termination date. The account is disabled or deleted at the end of business on the termination date, preventing further access to district resources.
- In the event of retirement, HR sends a Suspension of Service to Technology, indicating the retirement date. The account is modified for security purposes to only allow access to Google email and Drive.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.
- In all instances, the system account and associated network storage of the user that has separated from the District are immediately secured upon termination.

Local/Domain Administrator Access

All accounts needing this elevated permission must be approved by the CIO. Additionally, only DTL staff will have domain administrative access.

Remote Access

Access into the District’s network from outside is strictly prohibited without explicit authorization from the CIO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the District's network.
Contractors/Vendors
Approval for contractor/vendor access is a joint responsibility of HR, Auxiliary services and the CIO. Contractors conducting business on district premises are required to undergo a background check, unless alternative security measures are stipulated in the vendor contract. Those contractors accessing student data will be treated as on-premise users. Following the approval process, the DTL department is responsible for creating the account, ensuring a controlled and secure access environment for approved contractors/vendors

Appendix K: Data Access Roles and Permissions

Student Information System (SIS)

Only staff requiring access are provided accounts for the system.

Once basic information and a user ID are established, site(s) are associated with the account, and permissions are granted. Employee permissions are exclusively allocated to the site(s) assigned to the account. These permissions, unless additional ones are required, align with the job title and are categorized as Site and District permissions. The permissions are tailored for Past, Current, and Future years on an individual basis.
While system preset configurations determine permissions, there is flexibility to extend permissions on a case-by-case basis to accommodate special needs or when a single account covers multiple positions. Any such changes must receive approval from the site administrator and/or HR, ensuring a controlled and authorized access framework.

Student Information Access

- Attendance including type of attendance
- Grades/Assessments
- Programs and Services
- Discipline
- Parent Communication (Email, Phone numbers, addresses)
- Family Demographics
- Fees

Medical Information

- Medical data includes Immunizations, conditions
- Designated staff are the only accounts that can view medical information

Financial System

All staff members are entered into the financial system for the purpose of employee payroll and HR tracking. Employee access to their individual payroll information is granted through the BCPS Time Keeper website. Only staff requiring access are provided accounts for the financial/personnel application.

Special Education System(ECATS)

The special education system serves as the repository for student IEP information. At the start of the school year, new accounts are imported, and adjustments are made manually by administrators in the Special Education department as needed throughout the year.
Special Education Administrators and district coordinators have access to all students within the district. They are responsible for assigning building-level access to building coordinators. Building coordinators, in turn, allocate student access to teachers and staff, including pathologists, based on the specific needs and requirements of each student. This hierarchical access structure ensures that the right individuals have appropriate access levels for effective management of student IEP information.

Appendix L: Password Security

The District requires the use of strictly controlled passwords for network access and for access to secure sites and information. All passwords to district systems shall meet or exceed the below requirements.

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall not be recorded anywhere that someone may find and use them.
- When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, or birthdays).
- Users and employees who have reason to believe a password is lost or compromised must notify the CIO or designee as soon as possible. The DTL department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through Active Directory/SSO/Google:

- Active directory passwords must be "strong" and reset every 180 days.
- Active directory passwords cannot contain any part of your name, must be a minimum of 10 characters, including three of the four of the following: uppercase letter, lowercase letter, number, and/or special character.
- Google Account passwords must be a minimum of 8 characters, and two-factor authentication must be enabled.

Appendix M: Burke County Public Schools Incident Response Plan

Objectives

Burke County Public Schools Incident Response Plan is designed with the primary goal of facilitating an effective and efficient response to natural disasters or critical failures affecting the district's data center and core systems. The key objectives during such events include:

- Minimize Loss or Downtime: The plan aims to reduce the loss or downtime of core systems and ensure access to critical data.
- Recover and Restore: Efforts are focused on the recovery and restoration of the district's critical systems and data.
- Maintain Essential Resources: The plan strives to sustain essential technology resources crucial for the day-to-day operations of the district.
- Minimize Impact: It aims to minimize the impact on staff and students, both during and after a critical failure, ensuring a smooth and resilient response to adverse situations.

By addressing these objectives, the BCPS IRP is instrumental in safeguarding BCPS against the potential disruptions caused by natural disasters or critical failures, contributing to the overall continuity and stability of the district's operations.

Key Terms

An **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

A **cyber incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Incident Response is the mitigation of violations of security policies and recommended practices. It is the process to address and manage the remediation of a security attack or breach in an organized and efficient manner. Incident response enables a quick, appropriate reaction to an attack and minimizes potential damage to business operations.

Definition of Cyber Incident
A cyber incident refers to any malicious, unauthorized, or unexpected event that compromises the security, confidentiality, integrity, or availability of information systems, networks, or data. These incidents can include cyberattacks, data breaches, malware infections, denial-of-service attacks, unauthorized access, and other activities that pose a threat to the digital environment. Cyber incidents can have various impacts, ranging from the theft of sensitive information to disruption of services, financial losses, and damage to the reputation of individuals or organizations. Effectively responding to and mitigating cyber incidents is crucial to maintaining the security of digital systems and protecting against potential harm.

Planning Assumptions

The planning assumptions for the development of BCPS IRP include:

- Some natural disasters may have a greater impact than others.
- Factors beyond the department's control or predictability may arise during a disaster.
- Complete loss of the current data center is a possibility.
- Adequate storage is available for system recovery.
- District data is stored at the district data center and backed up in the cloud.
- District data is hosted by 3rd party providers.
- A critical failure in the network infrastructure of the data center may significantly impact district networking.

Incident Response Team

BCPS has appointed the following people to the incident response team:

Role
IR Team Leader: Responsible for overall leadership and management of the IR Team including declaring an incident, invoking incident response plans, and reporting to applicable local, state, and federal partners (i.e. Notify NCDIT of Incident within 24 hours)
IR Team Administrator: Responsible for ensuring all stages of incident response are thoroughly documented and serves as the point of contact for legal counsel, insurance representatives, communications/PR, and other internal stakeholders about the incident and response.
IR Team Lead Investigator: Named by the Team Leader and responsible for coordinating comprehensive response activities, including most technical aspects of the incident.
Communications/PR: In consultation with legal counsel, responsible for ALL inbound/outbound communications with media and other external stakeholders.

Legal Counsel: Responsibilities vary depending on the incident or event scenario but will generally ensure that the organization's incident response plans, policies, and procedures are in compliance with relevant local, state, and federal laws and guidelines.
Human Resources: Advise the CIRT on how to apply existing HR policies and procedures in the context of the incident and collaborate with the CIRT to assess the potential impact of the incident on employees, such as data breaches involving personal information
Superintendent: Ensure academic continuity by collaborating with the CIRT to develop and implement plans that ensure the continuation of educational programs and services during and after the cybersecurity incident
Business or Chief Finance Officer: Collaborate with the CIRT to assess the potential financial implications of the cybersecurity incident, including direct costs (e.g., recovery expenses, legal fees) and indirect costs (e.g., reputation damage).
Operations / Facilities: Assess the potential physical risks resulting from the cybersecurity incident, such as disruptions to access control systems, surveillance systems, or building management systems
Cybersecurity Insurance Provider: Responsibilities vary depending on provider, coverage terms, and local and state policies.
MCNC: The Incident Response Team Leader may establish relationships with cybersecurity vendors that may provide additional support in the face of an incident such as cyber insurance, intelligence feeds, tooling support, security monitoring and alerting, forensic analysis, or incident response retainers.

In the event the BCPS IRP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

Role	Responsibility
IR Team Leader	● Responsible for overall leadership and management of the IR Team ● Responsible for declaring an incident, invoking incident response plans, and reporting to applicable local, state, and federal partners (i.e. Notify NCDIT of Incident within 24 hours) ● Assigns the IR Team Lead Investigator and identifies resources needed during all stages of incident response ● Coordinates with executive leadership to establish incident response policy, budget, and staffing ● Coordinates with for executive leadership teams regarding communications, financial, external engagements, human resources, academic, and potential operational and business changes/shifts
IR Team Administrator	● Responsible for ensuring all stages of incident response are thoroughly documented and serves as the point of contact for legal counsel, insurance representatives, communications/PR, and other internal stakeholders about the incident and response. ● Collecting and documenting incident details and response activities ● Leading post mortem discussions to determine root cause, necessary changes/updates, response strengths/weaknesses, and lessons learned. ● Responsible for overseeing and prioritizing response activities to ensure complete detection, analysis, and containment of the security incident

	● Facilitates information sharing and coordination of activity across the PSU to support rapid response and recovery, as well as meet contractual and regulatory obligations ● Involves relevant external parties during the incident response as needed and remains an involved party in any external investigations or remediation activities
IR Team Lead Investigator	● Named by the Team Leader and Responsible for coordinating comprehensive response activities (network/hardware/software), including most technical aspects of the incident. NOTE: Role may be filled by external technical experts skilled in detection and response. ● Monitors information systems for potential security events ● Receives reports of security events from end users ● Conducts initial triage of event to determine if an Information Security or Privacy Incident has occurred ● Completes analysis, containment, eradication, and recovery actions as directed by the IR Team Leader ● Serve as SME during any external IR investigations or remediation activities, as needed
Communications PR	● In consultation with legal counsel, responsible for ALL inbound/outbound communications with media and other external stakeholders.
Legal Counsel	Responsibilities vary depending on the incident or event scenario. ● Ensure that the organization's incident response plans, policies, and procedures are in compliance with relevant laws and federal guidance ● Provide legal guidance on matters within the incident response process that may have legal implications, such as evidence collection, preservation, and handling ● Draft, review, and support the creation of binding agreements, such as Memoranda of Understanding (MOUs), that outline liability limitations for information sharing among relevant parties ● Determine the organization's obligations under applicable NC laws, particularly with regards to breach notification requirements ● Advise the CIRT on whether and how to involve law enforcement agencies or regulatory bodies in response to the incident ● Provide guidance on how to manage investigations that involve teachers, staff, and/or students, ensuring that legal considerations are properly addressed. ● Review and approve incident communications that are drafted by the Communications Manager to ensure that they align with legal requirements and do not compromise the organization's legal position ● Collaborate with other external legal experts or counsel as needed, especially when specialized legal expertise is required for specific aspects of the incident response
Other Internal Teams that may need to be involved as needed	
Human Resources	● Advise the CIRT on how to apply existing HR policies and procedures in the context of the incident. ● Collaborate with the CIRT to assess the potential impact of the incident on employees, such as data breaches involving personal information

	● Work closely with legal counsel to ensure that any personnel-related actions, such as notifications to employees or effected parties, adhere to legal requirements and protect the organization's interests ● Provide insights into managing remote work arrangements if necessary due to the incident, addressing issues such as connectivity, productivity, and work-life balance ● Assist in documenting the HR-related aspects of the incident, including employee inquiries, concerns, and any actions taken by HR to address personnel-related issues
Chief Academic Officer	● Collaborate with the CIRT to develop and implement plans that ensure the continuation of educational programs and services during and after the incident ● Assess the potential impact of the incident on curriculum delivery, instructional materials, and online learning platforms ● Coordinate communication efforts to keep faculty and staff informed about the incident's impact on academic activities and provide guidance on how to adjust teaching and engagement strategies ● Collaborate with student services to ensure that students receive the necessary support to navigate the challenges posed by the incident, such as disruptions to online learning platforms ● Collaborate with communication teams to provide accurate and timely information to students and their families about the incident's impact on academic programs and the organization's response ● Engage with external educational partners, such as other institutions or educational boards, to communicate the organization's response to the incident and coordinate joint efforts if necessary.
Chief Finance Officer	● Collaborate with the CIRT to assess the potential financial implications of the cybersecurity incident, including direct costs and indirect costs ● Allocate necessary funds for incident response activities, such as hiring external experts, investing in additional security measures, or addressing regulatory compliance requirements ● Ensure that budget adjustments are made to accommodate unexpected expenses related to incident response. ● Liaise with insurance providers to determine coverage for cybersecurity incidents and initiate the claims process, if applicable. ● Assess the contractual obligations and liabilities of vendors and third parties involved in the incident response, including forensic experts, legal counsel, and communication teams ● Ensure that vendor contracts account for cybersecurity incidents and the associated financial implications ● Collaborate with the CIRT to develop and execute business continuity plans that address financial and operational aspects during and after the incident
Operations / Facilities	● Assess the potential physical risks resulting from the cybersecurity incident, such as disruptions to access control systems, surveillance systems, or building management systems ● Collaborate with security teams to ensure that physical security measures, such as access control, alarms, and surveillance systems, are functioning effectively ● Assess the impact of the incident on critical resources required for the safety and well-being of teachers and students, such as power, water, heating/cooling systems, transportation, and communication networks.

	● Address any environmental concerns that might arise from the incident, such as hazardous material spills or air quality issues caused by disruptions to monitoring systems.
Westchester Insurance Note: Responsibilities vary depending on provider, coverage terms, and local and state policies	● Covers financial losses from data breaches and cyber attacks ● Incident Response: Funds experts, investigators, legal support for managing incidents ● Covers notification, credit monitoring, and PR efforts ● Compensates for lost revenue during cyber-related downtime ● Covers legal fees, fines, and regulatory compliance ● Manages claims from breaches affecting others ● Supports PR to rebuild trust post-incident
Network Analyst	● Assist in diagnosing and resolving network issues ● Aid systems engineers to redeploy network scripts

Activation

The BCPS IRP will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the District's data center. A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and flood.
- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Chief Information Officer (CIO) will act as the incident response leader (IRL). If the CIO is not able to act as the IRL, a member of the Superintendent's Leadership Team will assume the role of IRL, with assistance from the IRT.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team (SLT)
- Technology Staff
- District Employees
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication is available at the time. This could include any one or combination of the following:

- Phone
- Email
- Social Media
- Radio or Television

The BCPS IRT will work with district leadership, including the Chief Information Officer, on which information will be conveyed to each above group and what means will be used.

Implementation

The BCPS IRT has the following in place to bring the District back online in the least of amount of time possible:

- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the technology office and the Superintendent of Operations' office. An electronic version will be housed on Google Drive.
- Maintained spreadsheet of all local administrator accounts, passwords and vendor contact information. A hard copy of this document will be secured at the technology office and the Superintendent of Operations' office. An electronic version will be housed on Google Drive.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District's critical virtual servers can be run directly from the cloud with limited access.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Deactivation

The IRT team will deactivate the plan once services are fully restored.

Evaluation

BCPS will conduct an internal evaluation of its Incident Response Plan (IRP) response. This involves collecting documentation from the response and obtaining feedback from all stakeholders. The findings will be integrated into an after-action report and a corrective action plan. The outcome will lead to updates in the BCPS IRP and other emergency response plans as deemed appropriate. This iterative process ensures continuous improvement and readiness in the face of incidents or emergencies.