

DATA GOVERNANCE AND USE - AR

TABLE OF CONTENTS

INTRODUCTION

2020-21 Committee Members

Committee Meetings

PROCEDURES

- Purpose
- Scope
- Regulatory Compliance
- Risk Management
- Data Classification
- Systems and Information Control
- Compliance and Sanctions

APPENDICES

- A. Definitions and Responsibilities
- B. Data Classification Levels

FORMS

1. Memorandum of Agreement (CMOA)
2. Agreements for Contract Employees Including Long Term Substitutes
3. Student Data Confidentiality Agreement
4. New Employee Information Form

Introduction

Protecting our students' and staffs' privacy is an important priority and Talbot County Public Schools (TCPS) are committed to maintaining strong and meaningful privacy and security protections. The privacy and security of this information is a significant responsibility and we value the trust of our students, parents, and staff.

The Talbot County Public Schools Data Governance document includes information regarding the Data Governance Committee, the actual Talbot County Public Schools Data and Information Governance and Use Policy, applicable Appendices, and Supplemental Resources.

The policy formally outlines how operational and instructional activities shall be carried out to ensure Talbot County Public Schools' data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The Talbot County Public Schools Data Governance Policy shall be an on-going document. To make the document flexible, details are outlined in the Appendices. With the Superintendent's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications shall be posted on the Talbot County Public Schools website and shared with board members.

2020-21 Data Governance Committee

The Talbot County Public Schools 2020-21 Data Governance committee consists of:

Ms. Darlene Spurrier, Director of Student Services;

Paula Yianakis, Coordinator of Personal Services;

Ms. Anna Howie, Local Accountability Coordinator,

Mr. Stephen Wilson, Director of Technology

Ms. Jennifer Miller, SIS Data Manager

Ms. Susan Ortt, FIS Data Manager

All members of the Talbot County Public Schools Senior Staff shall serve in an advisory capacity to the committee and shall be called upon to attend meetings when the topic of the meeting requires his or her expertise.

Committee Meetings

The Data Governance committee shall meet at a minimum two times per year. Additional meetings shall be called as needed.

Talbot County Public Schools Data Governance Procedures

I. PURPOSE

- A. It is the policy of Talbot County Public Schools 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.
- B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.
- C. Talbot County Public Schools conducts annual training on their data governance policy and procedures.

**See also Appendix A (Definitions and Responsibilities)*

II. SCOPE

The superintendent is authorized to establish, implement, and maintain data and information security measures. The 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 Talbot County Public Schools' data and information, including but not limited to:

- A. Speech, spoken face to face, or communicated by phone or any current and future technologies,
- B. Hard copy data printed or written,
- C. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,
- D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and
- E. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. Talbot County Public Schools complies with all applicable regulatory acts including but not limited to the following:

- A. Children's Internet Protection Act (CIPA)
- B. Children's Online Privacy Protection Act (COPPA)
- C. Family Educational Rights and Privacy Act (FERPA)
- D. Health Insurance Portability and Accountability Act (HIPAA)
- E. Protection of Pupil Rights Amendment (PPRA)

IV. RISK MANAGEMENT

A thorough risk analysis of all Talbot County Public Schools' data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, ISO, or Technology Director. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.

V. DATA CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification the integrity/quality 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 are 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 also Appendix B (Data Classification Levels)*

VI. SYSTEMS AND INFORMATION CONTROL

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. All involved systems and information are assets of Talbot County Public Schools shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. Ownership of Software: All computer software developed by Talbot County Public Schools employees or contract personnel on behalf of Talbot County Public Schools, licensed or purchased for Talbot County Public Schools use is the property of Talbot County Public Schools and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. Software Installation and Use: All software packages that reside on technological systems within or used by Talbot County Public Schools shall comply with applicable licensing agreements and restrictions.

C. Virus, Malware, Spyware, Phishing and SPAM Protection: Virus checking systems approved by the TCPS Technology Department are deployed that ensure all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable Talbot County Public Schools' protection systems or install other systems.

D. Access Controls: Physical and electronic access to information systems that contain Personally Identifiable Information (PII), confidential information, internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as recommended by the Data Governance Committee and approved by Talbot County Public Schools. In particular, the Data Governance Committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, confidential information, internal information and computing resources include, but are not limited to, the following methods:

1. Authorization: Access shall be granted on a "need to know" basis. On a case-by-case basis, permissions may be added to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Data Governance Committee.
2. 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 shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.
3. Data Integrity/Quality: Talbot County Public Schools provides safeguards so that PII, confidential, and internal information is not altered or destroyed in an unauthorized manner.
4. Transmission Security: Technical security mechanisms and personnel training are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks.
5. Remote Access: Access into Talbot County Public Schools' network from outside is allowed using the VPN. All other network access options are strictly prohibited without explicit authorization from the Technology Director, Systems Administrator, or Data Governance Committee. Further, 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 Talbot County Public Schools' network.
6. Physical and Electronic Access and Security: Access to areas in which information processing is carried out shall be restricted to only appropriately

authorized individuals. At a minimum, staff passwords shall be changed annually.

Electronic Access Security:

- No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
- It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

Physical Access Security:

- Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
- Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommend an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
- File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
- Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Monitor and control the delivery and removal of all asset-tagged and/or data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus

property is appropriately sanitized in accordance with applicable policies and procedures.

E. Password Standards

Users are responsible for complying with the following password standards for network access or access to secure information:

1. Passwords shall never be shared with another person, unless the person is a designated System Administrator or Technology Director.
2. Every password shall, where possible, be changed yearly if not more frequently for staff and on an age appropriate schedule for students.
3. Passwords shall, where possible, have a minimum length of eight (8) characters.
4. Passwords shall not be recorded anywhere that someone may find and use them.
5. Passwords for secure information or sites will be complex, not easily guessed or due to their association with the user (i.e. children's names, pets' names, birthdays, etc...). A combination of alpha, numeric and symbol characters are more difficult to guess.

Where possible, system software should enforce the following password standards:

1. Passwords shall be entered in a non-display field.
2. System software shall enforce the changing of passwords and the minimum length.
3. System software shall disable the user password when more than five consecutive invalid passwords are given. Software permitting, lockout time shall be set at a minimum of 30 minutes.
4. System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user. A combination of alpha, numeric and symbol characters are more difficult to guess.

F. Data Transfer/Exchange/Printing:

1. Electronic 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 reports, research, application uploads or any other purposes that include PII shall be in accordance with this policy and be approved by the Data Governance Committee. A Memorandum of Agreement (MOA), contract addendum, or equivalent, shall be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the data governance committee.

**See also (Talbot County Public Schools Memorandum of Agreement.)*

2. Other Electronic Data Transfers and Printing: PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible and shall be de-identified before use.
- G. Oral Communications: Talbot County Public Schools' staff 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. Talbot County Public Schools' 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 on public transportation.

VII. COMPLIANCE AND SANCTIONS

- A. The Data Governance Policy and Procedures applies to all users of Talbot County Public Schools' information including: employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Talbot County Public Schools' procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with Talbot County Public Schools' policies. Further, penalties associated with state and federal laws may apply.
- B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:
 1. Unauthorized disclosure of PII or Confidential Information.
 2. Unauthorized disclosure of a log-in code (User ID and password).
 3. An attempt to obtain a log-in code or password that belongs to another person.
 4. An attempt to use another person's log-in code or password.
 5. 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.
 6. Installation or use of unlicensed software on Talbot County Public School technological systems.
 7. The intentional unauthorized altering, destruction, or disposal of Talbot County Public Schools' information, data and/or systems. This includes the unauthorized removal from TCPS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
 8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

Definitions and Responsibilities Appendix A

Definitions

- A. Availability: Data or information is accessible and usable upon demand by an authorized person.
- B. Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.
- C. Data: Facts or information
- D. Entity: Organization such as school system, school, department or in some cases business
- E. Information: Knowledge that you get about something or someone; facts or details.
- F. Data Integrity/Quality: Data or information has not been altered or destroyed in an unauthorized manner.
- G. Involved Persons: Every user of Involved Systems (see below) at Talbot County Public Schools- no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.
- H. Systems: All data-involved computer equipment/devices and network systems that are operated within or by the Talbot County Public Schools physically or virtually. This includes all platforms (operating systems), all computer/device sizes (personal digital assistants, desktops, mainframes, telephones, laptops, tablets, game consoles, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.
- I. Personally Identifiable Information (PII): PII is 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, 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.
- J. Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

Responsibilities

- A. Data Governance Committee: The Data Governance Committee for Talbot County Public Schools is responsible for working with the Director of technology who also serves as the Information Security Officer (ISO) to ensure security policies, procedures, and standards are in place and adhered to by the entity.
- B. Information Security Officer: The Information Security Officer (ISO) for Talbot County Public Schools is responsible for working with the superintendent, Data Governance Committee, user management, owners, data custodians, and users to develop and implement prudent security policies, procedures, and controls.
- C. Information Owner: The owner of a collection of information is usually the administrator or supervisor responsible for the creation of that information. In some

cases, the owner may be the primary user of that information. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on Maryland Department of Information Technology (DoIT) guidelines, industry standards, Data Governance Committee guidelines, or advice from the school system attorney.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created.
4. Authorizing access and assigning data custodianship if applicable.
5. Specifying controls and communicating the control requirements to the data custodian and users of the information.
6. Reporting promptly to the ISO the loss or misuse of Talbot County Public Schools' data.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
9. Following existing approval processes within the respective organizational unit and district for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

D. Data Manager/Custodian: The data custodian is assigned by an administrator, data owner, or the ISO based his/her role and is generally responsible for the processing and storage of the information. The data custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Providing and/or recommending procedural safeguards.
3. Administering access to information.
4. Releasing information as authorized by the Information Owner and/or the ISO and/or Data Governance Committee for use and disclosure using procedures that protect the privacy of the information.
5. Maintaining information security policies, procedures and standards as appropriate and in consultation with the ISO and/or Data Governance Committee.
6. Promoting employee education and awareness by utilizing programs approved by the ISO, where appropriate.
7. Reporting promptly to the ISO and/or Data Governance Committee the loss or misuse of Talbot County Schools data.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

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

1. Access information only in support of their authorized job responsibilities.
2. Comply with all data security procedures and guidelines in the Talbot County Public Schools Data Governance Policy and all controls established by the data owner and/or data custodian.
3. Keep personal authentication devices (e.g. passwords, secure cards, PINs, access codes, etc.) confidential.
4. Report promptly to the ISO and/or Data Governance Committee the loss or misuse of Talbot County Schools' information.
5. Follow corrective actions when problems are identified.

Data Classification Levels Appendix B

A) Personally Identifiable Information (PII)

- 1) PII is information about an individual maintained by an agency, including:
 - a) 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.
 - b) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

B) Confidential Information

- 1) Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access.
 - a) Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

C) Internal Information

- 1) Internal Information is intended for unrestricted use within Talbot County Public Schools, and in some cases within affiliated organizations such as Talbot County Public Schools' business or community partners. This type of information is already widely-distributed within Talbot County Public Schools, or it could be so distributed within the organization without advance permission from the information owner.
 - a) Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.
- 2) Any information not explicitly classified as PII, Confidential or Public shall, by default, be classified as Internal Information.

D) Public Information

- 1) Public Information has been specifically approved for public release by a designated authority within each entity of Talbot County Public Schools.

- a) Examples of Public Information may include marketing brochures and material posted to Talbot County Public Schools' web pages.
- E) **Directory Information**
- 1) Talbot County Public Schools defines Directory information as follows:
 - a) Student first and last name
 - b) Student gender
 - c) Student home address
 - d) Student home telephone number
 - e) Student school-assigned monitored and filtered email address
 - f) Student photograph
 - g) Student place and date of birth
 - h) Student dates of attendance (years)
 - i) Student grade level
 - j) Student homeroom
 - k) Student diplomas, honors, awards received
 - l) Student participation in school activities or school sports
 - m) Student weight and height for members of school athletic teams
 - n) Student most recent institution/school attended
 - o) Student TCPS ID number / Student State ID number

Talbot County Public Schools Technological Services and
Systems
Memorandum of Agreement
(MOA)

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the__ day of ---Month--- 202_, by and between _____, a corporation organized and existing under the laws of (the "Company"), and TALBOT COUNTY PUBLIC SCHOOLS (TCPS), a public school system organized and existing under the laws of the State of Maryland, recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled "hereafter referred to as (the "Agreement"). In connection with the execution and

delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

Confidentiality Obligations Applicable to Certain TCPS Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all TCPS student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information shall not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

The Company shall cause each officer, director, employee and other representative who shall have access to TCPS Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all TCPS Student Information. The Company shall take all reasonable steps to insure that no TCPS Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for TCPS under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of TCPS, or (c) are entitled to such TCPS student information from the Company pursuant to federal and/or Maryland law. The Company shall use TCPS student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the TCPS student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to TCPS student information Other Security Requirements. The Company shall maintain all technologies,

policies, procedures and practices necessary to secure and protect the confidentiality and integrity of TCPS student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify TCPS of planned system changes that may impact the security of TCPS data; (g) return or destroy TCPS data that exceed specified retention schedules; (h) notify TCPS of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of TCPS information to the previous business day. The Company should guarantee that TCPS data shall not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify TCPS within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the TCPS student information compromised by the breach; (c) return compromised TCPS data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with TCPS efforts to communicate to affected parties by providing TCPS with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with TCPS to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with TCPS by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide TCPS with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of TCPS data of any kind, failure to follow security requirements and/or failure to safeguard TCPS data. The Company's compliance with the standards of this provision is subject to verification by TCPS personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall not be shared, sold, or moved to other companies or organizations nor should other companies or organization be allowed access to said information.

Disposition of TCPS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required TCPS student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to TCPS data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be

school officials of the School Board, and shall maintain TCPS data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in TCPS data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law; Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Maryland, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Maryland

IN WITNESSWHERE OF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

COMPANY NAME

By: _____
[Name]

[Title]

TALBOT COUNTY PUBLIC SCHOOLS

By: _____
Superintendent, Talbot County Public School

Agreements for Contract
Employees

Including Long Term
Substitutes

Procedure:

1. All contract employees should complete the following prior to gaining access to the Talbot County Public School Network, Powerschool, FinancePlus, (if applicable):
 - A. Complete the Request for Email Account and Other Resources for Contract Employees Form, read and sign to acknowledge the Technology Usage Policy, and complete the Data Governance online training.
 - Forms available on Talbotschools.org under
 - Make appointment with Data Manager and technology facilitator to review Data Usage and Classroom Tools
2. Read and sign the Talbot County Public Schools Student Data Confidentiality Agreement
3. Once the above has been completed and forms reviewed, if all requirements are met, the new email account shall be enabled.

**Account shall be created as soon as Technology Department receives the Request for Email Account and Other Resources for Contract Employees Form for the contracted employee.

**STUDENT DATA CONFIDENTIALITY
AGREEMENT**

I acknowledge my responsibility to respect the confidentiality of student records and to act in a professional manner in the handling of student performance data. I will ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated in violation of state and federal laws.

Furthermore, I agree to the following guidelines regarding the appropriate use of student data collected by myself or made available to me from other school/system employees, Powerschool, Edocrina, or any other file or application I have access to:

- I will comply with school district, state and federal confidentiality laws, including the state Data and Information

Governance and Use Policy, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34

CFR Part 99; and, and the Talbot County Public Schools Student Data Confidentiality Agreement.

- Student data shall only be accessed for students for whom I have a legitimate educational interest and shall be used for the sole purpose of improving student achievement.
- I understand that student specific data is never to be transmitted via e-mail or as an e-mail attachment unless the file is encrypted and/or password protected.
- I understand that it is illegal for a student to have access to another student's data. I shall not share any student's information from any source with another student.
- I shall securely log in and out of the programs that store student specific data. I shall not share my password. Any documents I create containing student specific data shall be stored securely within the District network or within a password protected environment. I shall not store student specific data on any personal computer and/or external devices that are not password protected. (external devices include but are not limited to USB/Thumb drives and external hard drives)
- Regardless of its format, I shall treat all information with respect for student privacy. I shall not leave student data in any form accessible or unattended, including information on a computer display.

By signing below, I acknowledge, understand and agree to accept all terms and conditions of the Talbot County Public Schools

Student Data Confidentiality Agreement.

Signature of Employee

Date

Job Title

School or Building

School Year:-----

NEW EMPLOYEE TECHNOLOGY INFORMATION
PLEASE PRINT

Legal First Name: _____ Middle Initial: _____ Legal Last Name: _____

Nickname: _____

Street Address: _____

City: _____ State: _____ Zip: _____

Last Four Digits of SS#: _____

Date of Birth: ___ / ___ / ___

Home Phone: _____ Current Email _____

Address: _____

Emergency Contact Information (Name and Number):

Grade/Subject/Position: _____

School: _____

I have received and am knowledgeable of the content in the Technology Acceptable Use Agreement adopted by the Talbot County Public Board of Education and completed the online training for the Data and Information Governance and Use Policy.

Name: _____ Date: _____

-END-