i3 Academy

Data Governance

Policies and Procedures

TABLE OF CONTENTS

Introduction

Protecting our students' and staffs' privacy is an important priority, and i3 Academy is 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 stakeholders.

The i3 Academy Data Governance document includes information regarding the Data Governance Committee, the actual i3 Academy Data and Information Governance and Use Policy, applicable Appendices, and Resources.

The policy formally outlines how operational and instructional activities shall be carried out to ensure i3 Academy 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.

i3 Academy Data Governance Policy shall be an on-going document. To make the document flexible, details are outlined in the Appendices. With the Board's permission, the Data Governance Committee may quickly modify information in the Appendices in response to changing needs. All modifications shall be posted on i3 Academy website and shared with board members.

Data Governance Committee
All members of the i3 Academy Administrative Team 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.

- Dr. Martin Nalls - Head of School
- Dr. Dylan Ferniany – Chief Academic Officer
- Dr. JohnMark Edwards – Technology Integration Specialist
- Krystal Wright – Technology Integration Specialist
- Morgan Montiel – Data & Technology Consultant
- Dr. Tara Bensinger – Instructional Support/ Media Specialist
- TJ Nguyen – Makerspace Instructor
- Tanesha Sims–Summers – Board Member & Parent

Committee Meetings
The Data Governance committee shall meet two times per year in the fall and spring. Additional meetings shall be called as needed. A quorum shall consist of a minimum of three committee

members. Notifications for meetings will be given a minimum of 48 hours in advance. All minutes from meetings will be sent to committee members within 72 hours of the meeting.

i3 Academy Data Governance Procedures

I. PURPOSE

A. It is the policy of i3 Academy 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. i3 Academy conducts annual training during the beginning of the year summit on the data governance policy and procedures.

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

II. SCOPE

The i3 Academy School Board and/or Data Governance Committee 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 i3 Academy 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. i3 Academy 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 i3 Academy data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the superintendent, Information Security Officer (ISO) or technology specialist. 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 assets of i3 Academy 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 i3 Academy employees or contract personnel on behalf of i3 Academy, licensed or purchased for i3 Academy use is the property of i3 Academy 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 i3 Academy shall comply with applicable licensing agreements and restrictions.

C. Virus, Malware, Spyware, Phishing and SPAM Protection: Virus checking systems approved by the District Technology Department are deployed that ensures all electronic

files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable i3 Academy 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 i3 Academy. 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 in 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:** i3 Academy 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 i3 Academy's network from outside is allowed using the ASC VPN. All other network access options are strictly prohibited without explicit authorization from the Technology Director, ISO, 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 i3 Academy' 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.

- Data centers' temperature and humidity levels shall be monitored and maintained. 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.

- Network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.

- The delivery and removal of all asset-tagged and/or data-storing technological equipment or systems will be monitored and controlled. i3 Academy will 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.

- Technological equipment or systems being removed for transfer to another organization or being designated as surplus property will be 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 security manager.
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 six (6) to eight (8) characters.
4. Passwords shall not be recorded anywhere that someone may find and use them.
5. 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, birthdays, etc…). A combination of alpha and numeric characters is 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. 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 and numeric characters is 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 research 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), 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 (i3 Academy 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 shall be de-identified before use.

G. Oral Communications: i3 Academy 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. i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy School technological systems.
7. The intentional unauthorized altering, destruction, or disposal of i3 Academy information, data and/or systems. This includes the unauthorized removal from i3 Academy 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 i3 Academy – 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 i3 Academy 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 i3 Academy is responsible for working with 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 i3 Academy 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 ALSDE 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 i3 Academy 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 Custodian:** The data custodian is assigned by an administrator, data owner, or the ISO based on 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 i3 Academy 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 i3 Academy 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 i3 Academy 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

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. 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 i3 Academy, and in some cases within affiliated organizations such as i3 Academy business or community partners. This type of information is already widely-distributed within i3 Academy, or it could be so distributed within the organization without advance permission from the information owner.
   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

Public Information has been specifically approved for public release by a designated authority within each entity of i3 Academy. Examples of Public Information may include marketing brochures and material posted to i3 Academy web pages.

E. Directory Information

i3 Academy defines Directory information as follows:

1. Student first and last name
2. Student gender
3. Student home address
4. Student home telephone number
5. Student school-assigned monitored and filtered email address
6. Student photograph
7. Student place and date of birth

8. Student dates of attendance (years)
9. Student grade level
10. Student homeroom
11. Student diplomas, honors, awards received
12. Student participation in school activities or school sports
13. Student weight and height for members of school athletic teams
14. Student most recent institution/school attended
15. Student ID number

Resource: ALSDE State Monitoring Checklist

Appendix C

ON-SITE	YES	NO	INDICATORS	NOTES
1. Has a data governance committee been established and roles and responsibilities at various levels specified?	✔		• Dated minutes of meetings and agendas • Current list of roles and responsibilities	
2. Has the local school board adopted a data governance and use policy?			• Copy of the adopted data governance and use policy • Dated minutes of meetings and agenda	
3. Does the data governance policy address physical security?			• Documented physical security measures	
4. Does the data governance policy address access controls and possible sanctions?			• Current list of controls • Employee policy with possible sanctions	
5. Does the data governance policy address data quality?			• Procedures to ensure that data are accurate, complete, timely, and relevant	
6. Does the data governance policy address data exchange and reporting?			• Policies and procedures to guide decisions about data exchange and reporting • Contracts or MOAs involving data exchange	
7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?			• Documented methods of distribution to include who was contacted and how • Professional development for all who have access to PII	

i3 Academy Technological Services and Systems
Memorandum of Agreement (MOA)

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the ___ day of _____, 20__, by and between _____, a corporation organized and existing under the laws of _____ (the "Company"), and **i3 Academy** , a public school system organized and existing under the laws of the state of Alabama (the "School Board"), 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 i3 Academy Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all i3 Academy 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 i3 Academy Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all i3 Academy Student Information. The Company shall take all reasonable steps to insure that no i3 Academy Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for i3 Academy under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of i3 Academy, or (c) are entitled to such i3 Academy student information from the Company pursuant to federal and/or Alabama law. The Company shall use i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy of planned system changes that may impact the security of i3 Academy data; (g) return or destroy i3 Academy data that exceed specified retention schedules; (h) notify i3 Academy of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of i3 Academy information to the previous business day. The Company should guarantee that i3 Academy 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 i3 Academy 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 i3 Academy student information compromised by the breach; (c) return compromised i3 Academy data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with i3 Academy efforts to communicate to affected parties by providing i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy 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 i3 Academy data of any kind, failure to follow security requirements and/or failure to safeguard i3 Academy data. The Company’s compliance with the standards of this provision is subject to verification by i3 Academy 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 i3 Academy 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 i3 Academy student data and/or staff data. The Company hereby

acknowledges and agrees that, solely for purposes of receiving access to i3 Academy 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 i3 Academy 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 i3 Academy 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 Alabama, 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 Alabama.

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

_____**C**
OMPANY NAME

By:_____
[Name] **[Title]**

i3 Academy

By:_____
Head of Schools, i3 Academy

Agreements for Contract Employees (Including Long Term Substitutes)

Procedure:

1. All contract employees should complete the following prior to gaining access to the i3 Academy Network, PowerSchool SIS, and Special Programs (if applicable):

    A. Complete the **Request for Email Account and Other Resources for Contract Employees Form**, read and sign to acknowledge the **Technology Use Agreement, and complete the Data Governance online training (online modules available starting 2022-2023 school year).**

        - Make appointment with your designated Technology Integration Specialist to review Data Usage and Classroom Tools

2. Read and sign i3 Academy **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, iNow, SETS 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 i3 Academy 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 i3 Academy Student Data Confidentiality Agreement.

_____ _____

Signature of Employee Date

_____ _____

Job Title School

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:_____

Would you like for i3 Academy to request a transfer of your STI PD professional development records? __If yes, in which school system were you employed?

_____

I have received and am knowledgeable of the content in the revised Technology Acceptable Use Agreement adopted by the i3 Academy Board of Education in July 17, 2014 and completed the online training for the Data and Information Governance and Use Policy.

Name: _____ Date: _____

**Accounts are disabled on the last day of active employment or when on leave for more than 6 months.*

Request for Email Account and Other Resources for Contract Employees

For contract employees to qualify for an email account in the i3academy.org domain, they shall have a contract on file with Personnel and perform work for i3 Academy on a regular basis. If i3 Academy has a contract with an agency to send "consultants" to i3 Academy on an as needed basis, they generally do not qualify and should use the email account provided to them by the agency. However, we will review all requests.

Contract Employee legal Name: _____ _____ _____
(First Name) (Middle Name) (Last Name)

Requester: _____ Department/School:_____

Start Date: _____ End Date: _____

Work to be Performed or Position: _____

Has contract employee had background check? _____ Yes _____ No

Has contract employee been E-Verified? _____ Yes _____ No _____ NA

Other Access Requested:

INow-should have permissions equal to ____ Teacher ____ Office _____ Other

If other, please specify: _____

SETS-Network Account with permissions equal to _____ Staff ____ Office _____

Reason for Request: _____

Signature of Requester: _____

_____ Denied _____ Approved Date: _____ Initials: _____

Employee Technology Use Agreement and Practices

All technology resources will be used to achieve the educational objectives outlined by i3 Academy. I understand that i3 Academy will comply with state mandates regarding our infrastructure and maintaining a safe virtual environment. I am expected to adhere to all policies and the administration has the authority to determine if I have used any technology resource inappropriately. I understand that i3 Academy expects all employees to exercise digital responsibility by practicing ethical behaviors while using technology resources both and off campus. I will adhere to all policies in accordance with the board, as well as, with local, state, and federal laws and understand that any/all policies could change at any time. It is expected that all employees of i3 Academy who use equipment, including laptops and multimedia devices and personal devices (cell phones), agree to the following guidelines and rules:

Statements of Understanding

- I understand that the use of i3 Academy's network is to promote educational and professional purposes.
- I understand that I should never circumvent or advise others to circumvent the school's network.
- I understand that I should never send or mask inappropriate behavior.
- I understand that I should never create accounts that require student data but will consult with school administration regarding acquiring online resources.
- I understand that I must consult with a school administrator and receive approval prior to creating a club or classroom social media account.
- I understand that I am to use caution when posting content online both on and off campus.
- I understand that I am to adhere to copyright laws.
- I understand that I should confirm if students/parents have submitted a request for FERPA and/or Public Posting of Intellectual Property Opt Out before posting student work.
- I understand that FERPA should be observed by all employees and at all times.
- I understand that I should not post personal demographic information of students or staff.
- I understand that I should not purchase any hardware or software on a school-owned device but should check with an administrator and/or technology specialist first.
- I understand that all purchased technology equipment and software must be purchased through an approved contract or bid.
- I understand that I should limit the amount of network space I use to store large files.
- I understand that I should report any technology issues to the Technology Department and/or an administrator.
- I understand that I should keep all devices password protected at all times.
- I understand that I may not share password information with anyone other than the Technology Department.
- I understand that I should never share password information for myself or others via email.
- I understand that I should always use a secure network when accessing confidential information pertaining to students and staff.
- I understand that I should keep backup copies of all data.
- I understand that I should only use my school email to send confidential information.
- I understand that i3 Academy can inspect all emails sent and received.
- I understand that my email should include a professional signature.

- I understand that when I send a group email to all recipients I should enter recipients as a Blind Carbon Copy (BCC) to ensure the security of the recipients email addresses.
- I understand that I should exercise all best practices against cyber attacks.
- I understand that personal devices should not be connected to the school's network.
- I understand that I am responsible for damaged or lost equipment.

I have read and will abide by the statements of appropriate practices regarding the use of technology. I have also read the *i3 Academy Data Governance Policies and Procedures Guide*. I understand that any technology device or network owned by i3 Academy is not private and can be inspected at any time. I understand that costs not covered by warranty for any damages is the responsibility of the employee. *I further understand that if I violate any of the above policies, it is a violation and can result in disciplinary consequences including, but not limited to, termination of employment, access, and legal action when applicable.*

Employee Name: _____ Date: _____

Employee Signature: _____ Date: _____

_