UTAH COUNTY ACADEMY OF SCIENCES
ED FORM D – DATA GOVERNANCE PLAN

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data from acquisition, to use, to disposal. The Utah County Academy of Sciences (UCAS) takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301 requires that UCAS adopt a Data Governance Plan.

This Data Governance Plan is applicable to all employees, temporary employees, and contractors of the Agency and will be reviewed and adjusted on an annual basis. The Data Governance Plan is designed to ensure only authorized disclosure of confidential information. Furthermore, the Data Governance Plan works in conjunction with Policy EG: IT Systems Security, which provides policies and processes for:

- Systems administration,
- Network security,
- Application security,
- Endpoint, server, and device Security
- Identity, authentication, and access management,
- Data protection and cryptography
- Monitoring, vulnerability, and patch management
- High availability, disaster recovery, and physical protection
- Incident Responses
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training.

Roles and Responsibilities
The LEA acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

- Data Manager roles and responsibilities
    - authorize and manage the sharing, outside of the student data manager's education entity, of personally identifiable student data for the education entity as described in this section
    - provide for necessary technical assistance, training, and support
    - act as the primary local point of contact for the state student data officer
    - ensure that the following notices are available to parents:
        - annual FERPA notice (see 34 CFR 99.7),
        - directory information policy (see 34 CFR 99.37),
        - survey policy and notice (see 20 USC 1232h and 53E-9-203),
        - data collection notice (see 53E-9-305)
- Information Security Officer
    - Oversee adoption of the CIS controls
    - Provide for necessary technical assistance, training, and support as it relates to IT security

Employee Non—Disclosure Assurances
Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information. All UCAS board members, employees, contractors and volunteers must sign and obey the Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information. Non-compliance with the agreements shall result in consequences up to and

including removal of access to the UCAS network; if this access is required for employment, employees and contractors may be subject to dismissal.

Non-Disclosure Assurances
All student data utilized by UCAS is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. A signed agreement form is required from all UCAS staff to verify agreement to adhere to/abide by these practices and will be maintained in the UCAS Human Resources. All UCAS employees (including contract or temporary) will:

1. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Chief Privacy Officer.
2. Consult with the Records Manager when creating or disseminating reports containing data.
3. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
4. NOT share individual passwords for personal computers or data systems with anyone.
5. Log out of any data system/portal and close the browser after each use.
6. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
7. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided when disposing of such records.
8. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
9. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
12. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.
13. Use secure methods when sharing or transmitting sensitive data.
14. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
15. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Data security and privacy training
UCAS will provide a range of training opportunities for all faculty and staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

Data Disclosure (See UCAS Policy ED)
Providing data to persons and entities outside of UCAS increases transparency, promotes education in Utah, and increases knowledge about Utah public education. UCAS Policy ED establishes the protocols and procedures for sharing data maintained by UCAS. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301.

Student or Student's Parent/Guardian Access
In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), UCAS will provide parents with access to their child's education records. UCAS will provide an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access). Access will be granted within 45 days of receiving an official request. UCAS is not required to provide data that it does not maintain, nor is UCAS required to create education records in response to an eligible student's request.

Third Party Vendor
Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.
All third-party vendors contracting with UCAS must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-309. Vendors determined not to be compliant may not be allowed to enter into future contracts with UCAS without third-party verification that they are compliant with federal and state law, and board rule.

Data Expungement
The LEA recognizes the risk associated with data following a student year after year that could be used to mistreat the student. The LEA shall review all requests for records expungement from parents and make a determination based on the following procedure.
The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
2. The LEA shall decide whether to expunge the data within a reasonable time after the request.
3. If the LEA decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. The LEA shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. The LEA shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. The LEA shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
8. The LEA shall make its decision in writing within a reasonable time following the hearing.
9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
10. If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

Data Breach
UCAS shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, UCAS faculty and staff shall follow industry best practices outlined in the IT Systems Security Policy EG for responding to the breach. Further, UCAS shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.
Concerns about security breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of the UCAS administrative team to determine whether a security breach has occurred. If the UCAS administrative team determines that one or more employees or

contracted partners have substantially failed to comply with the IT Systems Security Policy EG and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action.

The LEA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, the LEA staff shall follow industry best practices for responding to the breach. Best practices will include the following procedures:

1. The Principal will work with the information security officer. Together they will be designated as the cyber incident response team (CIRT). Others may be asked to join the team, if needed.
2. At the beginning of an investigation, the information security officer will begin tracking the incident and log all information and evidence related to the investigation.
3. The information security officer will call the CIRT into action once there is reasonable evidence that an incident or breach has occurred.
4. The information security officer will coordinate with other IT staff to determine the root cause of the breach and close the breach.
5. The CIRT will coordinate with legal counsel to determine if the incident meets the legal definition of a significant breach as defined in R277-487 and determine which entities and individuals need to be notified, including the student, the student's parent (if the student is not at adult), USBE, or others as deemed necessary.
6. If law enforcement is notified and begins an investigation, the CIRT will consult with them before notifying parents or the public so as to not interfere with the law enforcement investigation.

Quality Assurances and Transparency Requirements
The UCAS data governance plan is structured to encourage the effective and appropriate use of educational data. Data driven decision-making is the goal of all data collection, storage, reporting and analysis. Data driven decision-making guides what data is collected, reported and analyzed.

Data Transparency
Annually, UCAS will publically post:
1. UCAS data collections
2. Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-301

Appendix

Appendix A. UCAS Employee Non-Disclosure Agreement
As an employee of the UCAS, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed the Data Governance Plan. These assurances address general procedures, data use/sharing, and data security.
_____ I will abide by the terms of the UCAS's policies and its subordinate process and procedures;
_____ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations.

Trainings
_____ I have completed UCAS's Data Security and Privacy Fundamentals Training.

Using UCAS Data and Reporting Systems
_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.
_____ I will not share or exchange individual passwords, for either personal computer(s) or UCAS system user accounts, with other UCAS faculty or staff.
_____ I will log out of and close the browser after each use of any data and reporting systems.
_____ I will only access data in which I have received explicit written permissions.
_____ I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or publicly release confidential data;

Handling Sensitive Data
_____ I will keep sensitive data on password-protected state-authorized computers.
_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.
_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.
_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured UCAS server.

Reporting & Data Sharing
_____ I will not disclose or share any confidential data analysis except to other authorized personnel without UCAS's expressed written consent.
_____ I will not publically publish any data without the approval of the administrative team.
_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.
_____ I will not transmit child/staff-level data externally unless explicitly authorized in writing.
_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or Secure File Transfer Protocol (SFTP). In addition, sharing within secured server folders is appropriate UCAS internal file transfer.
_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the UCAS Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

_____ I understand that access to the UCAS network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____ I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

_____ I agree that upon the cessation of my employment from UCAS I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of UCAS without the prior written permission of the administrative team.

Print Name: _____
Signed: _____
Date: _____