dataspark
THE UNIVERSITY OF RHODE ISLAND

Rhode Island DataHUB
Security & Access Policies

These policy statements pertain to the Rhode Island DataHUB maintained by the University of Rhode Island (URI) program unit known as DataSpark. The DataHUB is Rhode Island's statewide longitudinal data system that contains administrative data from state agencies, local governments, and non-profit organizations for the purpose of supporting program evaluation, conducting longitudinal analysis, and informing policy decisions. DataSpark is the authorized representative and research partner of the state education and employment agencies.

The DataHUB is managed by DataSpark in accordance with state and federal laws and regulations particularly regarding education, health, and workforce records. Among the federal laws related to the confidentiality and release of records are:

- Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g(b)(1)(F) and 34 C.F.R. § 99.31(a)(6)) (FERPA),
- Individuals with Disabilities Education Act (IDEA, 34 CFR §§ 300.127 and 300.560-300.576),
- Protection of Pupil Rights Amendment (PPRA),
- Richard B. Russell National School Lunch Act (P.L. 108-265),
- Health Insurance Portability and Accountability Act (HIPAA),
- Health Information Technology for Economic and Clinical Health Act (HITECH),
- Code of Federal Regulations. Public Welfare (45 CFR, parts 160 to 164),
- United States Code. Public Welfare (42 U.S.C. 1320d et seq),
- Code of Federal Regulations. Federal-State Unemployment Compensation (UC) Program; Confidentiality And Disclosure Of State UC Information (20 CFR § 603.5(e) and (f)), and
- Federal Driver's Privacy Protection Act of 1994 (DPPA) (18 U.S.C. § 2721 et seq.)

Rhode Island statutes that are most pertinent to the DataHUB include but are not limited to:

- RIGL § 5-37.3-1 et seq. Confidentiality of Health Care Communications and Information Act,
- RIGL § 11-49.3-1 et seq. Rhode Island Identity Theft Protection Act of 2015,
- RIGL § 16-38-5.1. Assignment of identification numbers to students,
- RIGL § 16-71-3. Educational records access and review rights – Confidentiality of records,
- RIGL § 27-49-3.1. Disclosure of personal information obtained in connection with motor vehicle records,

- RIGL § 28-42-38 and 38.1. Labor and Labor Relations. Records and reports – Confidentiality of information,
- RIGL § 28 Chapters 42-44. Sanctions and penalties for unauthorized disclosure,
- RIGL § 36-14-5. Public Officers and Employees Code of Ethics. Prohibited activities including disclosure and confidentiality,
- RIGL § 40-5.2-1 et. seq. The Rhode Island Works Program,
- RIGL § 40-6-12. Public Assistance Act,
- RIGL § 40.1-5-26 Mental Health Law. Disclosure of confidential information and records,
- RIGL § 42-72-8. Department of Children, Youth and Families. Confidentiality of records,
- DCYF Policy 100.0005 (Confidentiality: Access to Information Contained in Departmental Service Records).

Changes and additions to federal and state laws and regulations are periodically reviewed to determine whether this policy complies.

As an organization entrusted with sensitive data, DataSpark prioritizes data privacy and security. DataHUB data shall only be accessed for the legitimate business of DataSpark and as required in the performance of job functions. Under no circumstances are data released or disclosed without prior approval from the appropriate Contributing Agency.

Purpose

This policy statement outlines security policies that DataSpark follows in addition to policies maintained by the Rhode Island Department of Information Technology (DOIT), University of Rhode Island (URI) Information Technology Services (ITS), partners, and technology providers such as Amazon Web Services. It establishes and defines the roles and responsibilities of users who are granted access to DataHUB data and the acceptable use thereof.

Scope

This document focuses on the layers of technology directly controlled by DataSpark It applies to all employees, contractors and any individual or group transferring data to, storing data within, and requesting access of DataHUB data.

DataSpark employs controls to ensure the integrity, privacy, and security of DataHUB data and to prevent the unauthorized use, release, or disclosure thereof. Standards detailing the policies and procedures for the secure transfer, storage, and use are based the Security and Privacy Controls for Information Systems and Organization issued by the U.S. Department of Commerce, National Institute of Standard and Technology (NIST Special Publication 800-53 Revision 4 or superseding versions). All changes or amendments to these policies require approval of the DataHUB Contributing Agencies.

Contents and Ownership

DataHUB Contributing Agencies ("Contributing Agencies") retain ownership of their data. DataSpark functions as the custodian of these data. DataHUB data cannot be released except as expressly authorized under applicable federal and state law and with the Contributing Agency's consent.

The DataHUB contains administrative data from:

- The Rhode Island Department of Education (RIDE)
- The Office of the Postsecondary Commissioner (RIOPC)
- The Rhode Island Department of Labor and Training (RIDLT)
- The Rhode Island Department of Children, Youth and Families (RIDCYF)
- The Rhode Island Department of Health (RIDOH)
- The Rhode Office of the Secretary of State (RISOS), and
- Local government and non-profit organizations.

Data Transfer

Transfers between DataSpark and Contributing Agencies use Secure Shell (SSH) or Secure File Transfer Protocol (SFTP). In transfer, data are encrypted and conform to Federal Information Processing Standard (FIPS) 140-2 or superseding versions. DataSpark uses multiple secure data transfer methods depending on the requirements or preferences of the Contributing Agency.

Data Storage

DataHUB data are encrypted at rest and backed up for redundancy. The underlying infrastructure is updated quarterly, with security vulnerabilities addressed immediately. Mechanisms are in place to record and examine access to the DataHUB. Additional measures confirm that DataHUB data are not altered or destroyed improperly.

DataSpark complies with destruction requests from DataHUB Contributing Agencies.

External and public-facing applications created and controlled by DataSpark never access the DataHUB directly. DataSpark employs dual methods of control, authentication, and access. DataSpark implements role based, unique user, password protected credentials to access DataHUB data.

Data Access

Access to DataHUB data is restricted to only authorized individuals. There are at least two barriers between DataHUB data and an unauthorized individual or entity, including but not limited to physical barriers, virtual access controls, Identity and Access Management (IAM), multi factor authentication, and firewalls and Intrusion Detection/Prevention Systems (IDPS).

DataSpark Staff

DataSpark staff are granted privileges consistent with their responsibilities to access DataHUB data and only after completing the DataSpark required privacy and security trainings. All DataSpark staff are trained on URI and DataSpark security policies and procedures. DataSpark staff are required to have knowledge of and to adhere to the regulations of these policies and procedures as well as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). DataSpark staff must have an active Human Subject's Research Certificate in accordance with the DataHUB Internal Review Board documentation.

DataSpark staff exercise due care in accessing DataHUB data to protect it from unauthorized access, use, disclosure, release, alteration, or destruction.

Only authorized DataSpark staff access identifiable data. For the purposes of this policy, identifiable data means information that alone or in combination is linked or linkable to a specific individual and that would allow a reasonable person to identify the individual with reasonable certainty (such as name, address, date of birth, social security number).

- **Directors** ensure a secure office environment with regard to the DataHUB. Directors ensure that, for their areas of accountability, their DataSpark staff know and understand their responsibilities as defined in this policy and that their office environment is secure. Directors validate access requirements of their staff. Directors may access identifiable data.

- **Data Engineers** require access to identifiable data to perform their job responsibilities: to import and link data as well as to validate that process.
- **Data Scientists** require access to identifiable data to perform their job responsibilities: to prepare data for import, to clean and analyze data, and to troubleshoot potential linkage problems.
- All other DataSpark staff may access identifiable data only with authorization by the appropriate Director and under the supervision of that Director, Data Engineer, or a Data Scientist.

Contributing Agencies

DataHUB Contributing Agencies consist of any state agency, local government, or nonprofit organization providing data to the DataHUB. Contributing Agencies also refers to vendors providing data on behalf of a state agency, local government, or nonprofit organization. Contributing Agencies maintain ownership of their data, and their data cannot be released without their approval. Vendors providing data on behalf of a state agency, local government, or nonprofit organization are not assumed to retain ownership rights over the data unless specified in a data sharing agreement or memorandum of understanding.

Contributing Agencies may request their Agency Information returned or to have their data linked with another Contributing Agency's data and then to have the linked Agency Information returned. These requests are governed by the Data Release Policies.

Third Parties

A Third Party, meaning an individual or entity that is not a DataHUB Contributing Agency, may request data, whether aggregate or individual-level. These requests are governed by the Data Request & Release Policies.

Incident Management

Should a data breach or cybersecurity event occur, DataSpark immediately informs the University's security officer, as designated by URI Information Technology Security, and follows the University's incident management plan.

Violations

Appropriate procedures shall be followed in reporting any breach of security or compromise of safeguards. Any person engaging in unauthorized use, disclosure, alteration, or destruction of DataHUB data in violation of this policy shall be subject to appropriate disciplinary action.

Updated October 18, 2021