Davis Technical College
Privacy Program Policy: DTC-PPP-01

Effective Date: 25 September 2025

1. Purpose

This policy establishes Davis Technical College's privacy program, outlining the College's policies, practices, and procedures for processing personal data in accordance with Utah Code § 63A-19-401(2)(a). It also aligns with applicable records management and data governance requirements as outlined in the Government Records Access and Management Act (GRAMA), the Utah Division of Archives and Records Service (Archives), and the Family Educational Rights and Privacy Act (FERPA). Where applicable, this policy will reference more specific policies, procedures, or guidance documents that govern privacy or data management practices implemented by the College.

2. References

2.1. Division of Archives and Records Services (Archives) Utah Code § 63A-12

2.2. Government Data Privacy Act (GDPA) Utah Code § 63A-19

2.3. Government Records Access and Management Act (GRAMA) Utah Code § 63G-2

2.4. Management of Records and Access to Records Utah Administrative Code R13-2

2.5. Family Educational Rights and Privacy Act (FERPA) 34 CFR Part 99

2.6. Utah System of Higher Education (USHE) Student Data Protection Act Utah Code § 53B-28-502

2.7. Davis Technical College's Incident Response Plan (IRP)

3. Guiding Principles

This policy consolidates privacy practices, outlines governance roles and responsibilities, and ensures compliance with generally applicable records management, data protection, and data privacy obligations. It is designed to safeguard individual privacy rights, promote transparency, maintain the integrity and security of personal data, and ensure accountability across the College. This policy is meant to guide further alignment of the College with the State Data Privacy Policy as detailed in Utah Code § 63A-19-102.

4. Scope

This policy applies to all College employees involved in the management, creation, and maintenance of records or who have access to personal data as part of their job duties. This policy also applies to all contractors of the College that process or have access to personal data as part of the contractor's duties under an agreement with the College pursuant to Utah Code § 63A-19-401.

5. Definitions

The definitions below are excerpted from Utah Code § 63G-2-103 and are intended to support the College's privacy program. This list is not comprehensive; only those terms deemed relevant to the College's operations have been included, while other definitions from the statute that do not apply to the College have been omitted.

5.1. Audit – a systematic examination of program procedures and operations for the purpose of determining their effectiveness, economy, efficiency, and compliance with statutes and regulations.

5.2. Classification – determining whether a record series, record, or information within a record is public, private, controlled, protected, or exempt from disclosure under Utah Code § 63G-2-201.

5.3. Contractor – any person who contracts with a governmental entity to provide goods or services directly to a governmental entity; or any private, nonprofit organization that receives funds from a governmental entity.

5.4. Cookie – technology that records a user's information and activity when the user accesses websites. Cookies are used by website owners, third parties, and sometimes threat actors to gather user data.

5.5. Data Breach - the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised.

5.6. Designation – the primary classification assigned to a record series based on a governmental entity's familiarity with the records or a review of a reasonable sample. The designation reflects the classification that would be given to the majority of the records in the series and typically applies to similar records within the series if they were individually classified.

5.7. Device Fingerprinting – collecting attributes of a user's device configurations to create a trackable profile for the device.

5.8. Individual – a human being.

5.9. Person – an individual, nonprofit or profit corporation, partnership, sole proprietorship, other type of business organization, or any combination acting in concert with one another.

5.10. Key Logger – a program designed to record which keys are pressed on a computer keyboard

5.11. Personal Data – information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

5.12. Processing Activity – any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.

5.13. Record – any documentary material, regardless of format, that is prepared, owned, received, or retained by the College and is reproducible. This includes both paper and electronic formats. Not all materials are considered records; personal notes, drafts, proprietary software, and other exceptions are excluded under the law, as defined in Utah Code § 63G-2-103(25)(b).

5.14. Records Series – a group of records that may be treated as a unit for purposes of designation, description, management, or disposition.

5.15. Records Officer – the individual appointed by the Chief Administrative Officer of each governmental entity, or the political subdivision to work with state archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records.

5.16. Schedule – the process of specifying the length of time each record series should be retained by a governmental entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to the state archives or destroyed.

6. Governance

6.1. Chief Administrative Officers (CAOs) –

6.1.1. The President of the College shall designate one or more individuals to serve as a Chief Administrative Officer (CAO) of the College in fulfilling the duties outlined in Utah Code § 63A-12-103.

6.1.2. The President of the College may assign responsibility for the duties outlined in Utah Code § 63A-12-103 to one, or among several, CAOs as the President sees fit.

6.1.3. The designation of the CAO(s) shall be reported to the Utah Division of Archives and Records Services (Archives) within 30 days of the designation.

6.1.4. If responsibility for the duties outlined in Utah Code § 63A-12-103 are divided between more than one CAO, such specification should be reported to Archives along with the designation.

6.1.5. The designation and responsibilities of the CAO shall be reviewed and confirmed by the College on an annual basis.

6.2. Appointed Records Officers (AROs) –

6.2.1. The designated CAO(s) shall appoint one or more individuals to serve as records officers in fulfilling the duties of working with Archives and the Office of Data Privacy in the care, maintenance, scheduling, disposal, classification, designation, access, privacy, and preservation of records.

6.2.2. A designated CAO may assign responsibility for the duties of appointed records officers to one or more officers, as the CAO deems appropriate.

6.2.3. The appointment of records officers shall be reported to Archives within 30 days of the appointment.

6.2.4. If responsibility for the duties of appointed records officers are divided between more than one officer, such specification should be reported to Archives along with the appointment.

6.2.5. The appointment and responsibilities of a records officer shall be reviewed and confirmed by the College on an annual basis.

7. Record Series

7.1. Records and Records Series –

7.1.1. The College shall create and maintain records and records series in accordance with the requirements provided in GRAMA and FERPA in addition to correlated guidance issued by Archives.

7.1.2. The College shall appropriately designate and classify records and records series in accordance with the requirements provided in GRAMA and FERPA in addition to correlated guidance issued by Archives.

7.1.3. The Data Privacy Specialist shall be responsible for submitting a proposed retention schedule for each type of material defined as a record under GRAMA to the state archivist for review and final approval by the Records Management Committee (RMC).

7.1.4. Upon approval by the RMC, the College shall maintain and dispose of records in strict accordance with the approved retention schedule. In instances where the College has not received an approved retention schedule for a specific type of record, the general retention schedule maintained by the state archivist shall govern the retention and disposition of those records.

7.2. Record Series Privacy Annotation

7.2.1. The College shall perform a privacy annotation for each record series that contains personal data pursuant to Utah Code § 63A-19-401.1.

7.2.2. Privacy annotations shall include:

7.2.2.1. The legal authority under which personal data is processed;

7.2.2.2. The purposes and uses for the personal data; and

7.2.2.3. The types of personal data that may be processed within the record series.

7.2.3. Privacy annotations shall be conducted and reported in accordance with additional requirements provided by Archives via administrative rule.

8. Awareness & Training

8.1. Departmental Data Privacy Training –

8.1.1. The Data Privacy Specialist of the College shall ensure that all employees that have access to personal data as part of the employee's work duties complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year.

8.1.2. The Data Privacy Specialist, in conjunction with the Professional Development Specialist, is responsible for monitoring the completion of data privacy training by the College's employees.

8.2. AROs Training and Certification –

8.2.1. The CAO and Data Privacy Specialist shall ensure that all appointed records officers complete annual online training on GRAMA and maintain certification through the State Archives, in accordance with Utah Code § 63A-12-110.

8.2.2. The CAO and Data Privacy Specialist shall annually review and confirm the certification status of all appointed records officers.

8.2.3. AROs with GRAMA transparency responsibilities must complete the corresponding training and obtain certification through the State Archives.

8.2.4. AROs specializing in records management and privacy are required to complete both records management and GRAMA transparency training, as well as obtain the corresponding certifications.

9. Identify

9.1. Inventorying –

9.1.1. The Data Privacy Specialist of the College shall maintain a comprehensive inventory of:

9.1.1.1. All Information Technology (IT) systems that may process state or federal data which the state owns or is responsible for.

9.1.1.2. All records and record series that contain personal data and the types of personal data included in the records and record series.

9.1.1.3. All processing activities, the inventory of which shall include:

9.1.1.3.1. Non-compliant processing activities, pursuant to the GDPA, that were implemented prior to May 1, 2024, and a prepared strategy for bringing the non-compliant processing activity into compliance by no later than January 1, 2027; and

9.1.1.3.2. All processing activities implemented after May 1, 2024, with documentation confirming compliance status.

9.2. Information Technology Privacy Impact Assessment –

9.2.1. The Data Privacy Specialist of the College shall ensure that the College completes a Privacy Impact Assessment (PIA) for all IT systems that may process personal data prior to the initiation of data processing in the IT system.

9.2.2. The Data Privacy Specialist shall use the PIA template that is created and maintained by the Chief Privacy Officer, and which is approved by the Chief Information Officer.

9.2.3. The Data Privacy Specialist must maintain a copy of each completed assessment for a period of four years to provide audit documentation and ensure accountability in privacy practices.

10. Transparency

10.1. Website Privacy Policy –

10.1.1. The Data Privacy Specialist of the College shall create and maintain privacy policies on their websites as outlined in Utah Code § 63A-19-402.5 and Utah Admin Code R895-8.

10.1.2. The Data Privacy Specialist of the College shall ensure that personal data related to a user of the College's website is not collected unless the College website complies with Utah Code § 63A-19-402.5.

10.1.3. The Data Privacy Specialist of the College shall ensure that all websites of the College contain a privacy policy statement that discloses:

10.1.3.1. The identity of the governmental website operator;

10.1.3.2. How the College website operator may be contacted;

10.1.3.3. The personal data or user activity data collected on behalf of the College through tracking technologies such as web analytics tools;

10.1.3.4. The practices related to disclosure of personal data collected by the College website operator; and

10.1.3.5. The procedures, if any, by which a user of the College may request:

10.1.3.5.1. Access to the user's personal data; and

10.1.3.5.2. Access to correct the user's personal data.

10.1.3.6. A general description of the security measures in place to protect a user's personal data from unintended disclosure.

10.2. Privacy Collection Notice –

10.2.1. Employees shall only collect personal data from individuals if, on the day the personal data is collected, the College has provided a privacy notice to an individual asked to furnish personal data that complies with Utah Code § 63A-19-402.

10.2.2. Personal data request privacy notice shall generally include:

10.2.2.1. The record series that the personal data will be included in;

10.2.2.2. The reasons the person is asked to furnish the information;

10.2.2.3. The intended purposes and uses of the information;

10.2.2.4. The consequences for refusing to provide the information; and

10.2.2.5. The classes of persons and entities that currently:

10.2.2.5.1. Share the information with the College; or

10.2.2.5.2. Receive the information from the College on a regular or contractual basis.

11. Individual Requests

11.1. The Data Privacy Specialist of the College shall ensure that the College has established appropriate processes and procedures that facilitate compliance with applicable governing law for handling the following privacy requests of individuals:

11.1.1. Individual's requests to access their personal data;

11.1.2. Individual's requests to amend or correct their personal data; and

11.1.3. Individual's requests for an explanation of the purposes and uses of their personal data.

11.2. The CAO of the College shall ensure that the College has established processes for public access requests to inspect or copy the College's records, which are not requests from an individual to access their personal data.

11.3. The CAO of the College shall ensure that employees of the College follow established business practices with respect to GRAMA and FERPA.

12. Processing

12.1. Minimum Data Necessary –

12.1.1. The Data Privacy Specialist of the College shall ensure that all programs within the College obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose.

12.1.2. The Data Privacy Specialist of the College shall ensure that all programs within the College regularly review their data collection practices to ensure compliance with the data minimization requirement.

12.2. Record and Data Sharing Policy –

12.2.1. The College will only share or disclose personal data when there is appropriate legal authority. The sale of personal data is prohibited unless required by law.

12.2.2. Data sharing must comply with GRAMA or other governing laws, such as FERPA, and may include sharing with governmental entities, contractors, private providers, or researchers. Compliance with GRAMA or other governing law, such as FERPA, is contingent upon the purpose of the sharing, the parties involved, and the nature of the records

12.2.3. The Data Privacy Specialist is required to report annually to the Chief Privacy Officer on personal data sharing and selling activities, including types of data shared, the legal basis for sharing, and the entities receiving this data.

12.2.4. All contracts involving personal data must incorporate appropriate privacy protection terms. Written agreements for data sharing are recommended to ensure compliance with applicable laws and regulations.

12.3. Retention and Disposition of Records Containing Personal Data –

12.3.1. Employees shall maintain, archive, and dispose of records, which includes all personal data, in accordance with an approved retention schedule.

12.3.2. In instances where the College has not received an approved retention schedule for a specific type of record, the general retention schedule maintained by the state archivist shall govern the retention and disposition of those records.

12.3.3. Employees shall comply with all other applicable laws or regulations related to retention or disposition of specific personal data held by the College or by a particular operating unit or program of the College.

13. Information Security

13.1. Incident Response –

13.1.1. The College follows an internal Incident Response Plan (IRP) to manage and address all security incidents, including data breaches and privacy violations.

13.1.2. Employees shall report all suspected security incidents, including non-IT incidents such as unauthorized access to physical records, to the Director of IT and the Data Privacy Specialist.

13.1.3. The Data Privacy Specialist shall ensure compliance with all other applicable laws or regulations related to incident response and breach notification of specific personal data held by the College.

13.2. Breach Notification

13.2.1. USHE Requirements –

13.2.1.1. In the event of a *significant* data breach involving personally identifiable **student data**, the College shall notify each affected student as required under Utah Code § 53B-28-504.

13.2.1.2. A data breach is presumed to be *significant* unless the College determines, based on a risk assessment, that there is a low probability of substantial harm to affected students. This determination is made by evaluating the totality of circumstances, including the nature of the data involved, the likelihood of misuse, the identity of unauthorized recipients, and any mitigation efforts. In accordance with Utah Admin. Code R765-1010-4, the following are **not** considered *significant* breaches:

13.2.1.2.1. Inadvertent access or use by authorized personnel acting in good faith;

13.2.1.2.2. Disclosures where the recipient is unlikely to retain or misuse the data;

13.2.1.2.3. Breaches involving encrypted or otherwise safeguarded data;

13.2.1.2.4. Information already lawfully public;

13.2.1.2.5. Incidents affecting fewer than 25 individuals;

13.2.1.2.6. Disclosure of directory information as defined under FERPA.

13.2.1.3. USHE institutions are not required to comply with Utah Code § 63A-19-406 for data breaches involving personally identifiable student data, per USHE Board Policy R1013.

13.2.2. GDPA Requirements –

13.2.2.1. The College must notify both the Utah Cyber Center and the Office of the Attorney General of any data breach affecting 500 or more individuals, as required by Utah Code § 63A-19-405. Notification must occur without unreasonable delay and no later than five days after discovering the breach.

13.2.2.2. If the data breach affects fewer than 500 individuals, the College must create and retain an internal incident report in accordance with Utah Code § 63A-19- 405(5). A log of all data breaches affecting fewer than 500 individuals must be reported yearly to the Cyber Center

14. Surveillance

14.1. Covert Surveillance –

14.1.1. Employees may not establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law.

14.1.2. The Data Privacy Specialist of the College shall ensure that surveillance activities are documented and that a PIA for the activity has been completed if such a process is implemented.

14.2. Cookies, Fingerprinting, Key Loggers, and Tracking Technologies –

The college is committed to transparency and privacy protection for individuals that visit a website of the College with regard to the use of any tracking technologies, including but not limited to cookies, device fingerprinting, web analytics, and other similar methods for monitoring or collecting information from website users.

14.2.1. Cookies – the use of cookies on the College's websites and digital services must comply with applicable privacy and security policies. Cookies should be limited to essential operational purposes. Where third-party cookies are used for website analytics (e.g., Google Analytics), the College must disclose their use clearly in a privacy statement. Explicit consent is not required under Utah law but must be obtained where required by other applicable law or if additional tracking technologies are introduced.

14.2.2. Device Fingerprinting – device fingerprinting is prohibited unless explicitly authorized by the President of the College, and where the legal basis or appropriate justification for such processing is documented in a PIA. The purpose and extent of fingerprinting must be clearly defined, documented, and disclosed to users in a privacy notice or statement that complies with applicable legal requirements.

14.2.3. Key Loggers – key loggers are prohibited without specific authorization from the President of the College, and documented justification in the activity's PIA. Key loggers may only be used when

there is a clearly defined operational need that complies with security standards and legal requirements, including appropriate user notice where required.

14.2.4. Other Tracking Technologies – the use of other tracking technologies, such as web beacons, pixel tags, or similar tools, is prohibited unless explicitly authorized by the President of the College, and the legal basis for such tracking is documented in a PIA. Disclosure of these technologies must be included in a user-facing privacy statement, with user consent obtained when required by law.

14.2.5. User Notification and Consent – the College must ensure users are informed about the use of tracking technologies. A clear website privacy statement must explain the types of data collected, the purpose of the tracking, and how users can manage their preferences or consent. Any updates to tracking practices must be promptly reflected in the privacy statement.

14.2.6. Data Security and Retention – data collected through authorized tracking technologies must be securely stored, with access limited to authorized personnel. Retention of this data must align with approved retention schedules, and the data should only be retained as long as necessary for the defined operational purpose.

15. Related Documentation

15.1. Incident Response Plan

15.2. Security Awareness and Training Policy

15.3. Privacy Impact Assessment Guidelines

15.4. Privacy Collection Notice

15.5. Website Privacy Notice

15.6. Student Policy and Procedures

15.7. Responsible Use Policy

16. Approval and Notes

President's Council Approval: 21 July 2025
Board Approval: 25 September 2025