JORDAN SCHOOL DISTRICT

Data Governance Plan
2019-20 School Year

Introduction

The role of shared information is critical in the Jordan School District. As more information is used and shared, a concerted effort must be made to protect that information. Confidentiality, integrity, and availability of information are essential to maintaining the Jordan School District's reputation, legal position, and ability to conduct its operations.

This plan works in conjunction with a variety of Jordan School District policies and procedures and is structured to encourage the effective and appropriate use of education data and data-driven decision making that guides what data is collected, reported, and analyzed.

Jordan School District is committed to:

- achieving high standards of information security governance;
- understanding information security is a critical issue and creating a security-conscious environment;
- requiring third-party vendors to deal with information security in accordance with state and federal requirements;
- demonstrating to stakeholders that Jordan School District deals with information security in accordance with state and federal requirements; and
- applying best practices in information security such as implementing controls that are proportionate to risk and achieving individual accountability.

Definitions

"Employee" means faculty, staff, administrators, temporary employees, and any individual who completes work for the Jordan School District and is compensated through Jordan School District but does not do so through a third-party contract.

"Volunteer" means anyone who completes work for the Jordan School District without compensation through the Jordan School District and without a third-party contract.

"Third-party vendor" means anyone who provides a service or product to Jordan School District and is not directly employed by the District.

"Data" means any information pertaining to a student or employee.

"Authorized Information Users" means individuals or entities who have been granted access to data in the performance of their assigned duties.

"Computing devices" refers to any electronic device used to collect, store, maintain, share, or access information. This includes desktop and laptop computers, smartphones, tablets, and other such devices.

"Information security" means the protection and maintenance of the confidentiality, integrity, and availability of data.

"Password" means any string of characters used to authenticate user level accounts, system level accounts, web accounts, email accounts, screen saver protection, voicemail, and network logins.

Sharing Student Data

Providing data to persons and entities outside the Jordan School District increases transparency, promotes a better education in Utah, and increases knowledge about public education practices in Utah. This plan 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. §53A-1-1401.

In accordance with FERPA regulations 20 U.S.C. §1232g (a)(1) (A) (B) (C) and (D), the Jordan School District will provide parents with access to their child's education records, or 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), within 45 days of receiving an official request. Jordan School District is not required to provide data that it does not maintain, nor is Jordan School District required to create education records in response to an eligible student's request.

The Jordan School District will only share education records and/or personally identifiable information (PII) in accordance with federal and state student privacy laws. De-identified data or aggregate data is not considered personally identifiable and may be released without consent or authorization.

Third Party Vendors

Third party vendors may have access to students' personally identifiable information if the vendor is designated as "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 Jordan School District has outsourced institutional services or functions.

External Research

The Director of Evaluation, Research & Accountability will ensure proper data are shared with external researchers or evaluators to comply with federal and state law and state board rule. In accordance with Jordan School District policy AA428 – Research Projects and Proposals, researchers shall submit a research project application and written proposal to the Director of Evaluation, Research & Accountability for review by the Jordan School District Research Review Committee. Once the Research Review Committee has approved a research project proposal, pertinent data reported in aggregate may be shared with the researcher. Personally identifiable information needed to conduct the study will require signed parental consent. Researchers may not publish personally identifiable information.

Compliance

In compliance with state and federal law, Jordan School District employees must:

- participate in security awareness training, and education sessions as appropriate to their job functions and as directed by their supervisors and/or management;
- agree, in writing, on an annual basis that they have been trained and understand their responsibilities with regards to the management of student personally identifiable information and will abide by federal, state, and district student data privacy requirements;
- comply with software licenses and with other legal and regulatory obligations that apply to them including, but not limited to, the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability (HIPAA) as well as United States copyright law;
- notify their immediate supervisor who will then notify the Jordan School District Data Security Officer or the Information Systems Director of any known or suspected information security incident or issue; and

- when entering into agreement with third-party vendors, ensure that contracts and agreements stipulate that the vendor manages data in accordance with state law as outlined in Utah State Code §53A-1-1410.

Enforcement

Failure to comply will be considered serious misconduct. This may result in:

- restriction or suspension of computer access privileges;
- disciplinary action by Jordan School District up to and including termination;
- referral to law enforcement authorities for criminal prosecution; and
- other legal action, including action to recover civil damages and penalties.

Record Retention and Expungement

The Jordan School District and its schools shall retain and dispose of student records in accordance with Section 63G-2-604 and in compliance with Jordan School District policy AS61 – Student Records II.I. and with the guidelines set by the Utah Division of Archive and Record Services.

The Jordan School District shall expunge a student's student data that is stored by the education entity in accordance with §53E-9-305 and state board rule. The Jordan School District may expunge medical records and behavioral test assessments, but it may not expunge grades, transcripts, enrollment records, and assessment information. Student-level discipline data will be expunged in accordance with federal law (20 U.S.C. 7917), state law (UCA §53E-9-305), and state board rule.

DISTRICT STUDENT DATA GOVERNANCE COMMITTEE

Introduction

The protection of information requires that specific individuals be assigned duties which allow them to oversee, audit, monitor and manage the flow of information so that checks and balances are in place at every level of information management.

Student Data Managers

In accordance with state law, Jordan School District has assigned the task of overseeing student data privacy to a student data manager. For the 2017-2018 school year, the duties of the student data manager will be assigned to two co-chairs who will delegate some responsibilities to a student data governance committee who will divide duties in accordance with their department specialties.

The purpose of the co-chairs is to:

1. Direct the committee in reaching the goals and objectives outlined in state and federal law.
2. Report on deliverables such as plans, protocols, trainings, and policies relating to student data privacy.
3. Assist Jordan School District in monitoring and auditing the management of student data.
4. Serve as a liaison between the state's Chief Privacy Officer and the Jordan School District.

Student Data Governance Committee

In addition, Jordan School District has established a District Student Data Governance Committee and a Student Data Training Subcommittee to help manage the task of monitoring and maintaining the privacy of all student personally identifiable information and to help develop and monitor employee student data privacy training.

The purpose of the committee is to:

1. Establish a Jordan School District data governance plan and then maintain yearly revisions to this plan to ensure that it complies with state and federal law.
2. Facilitate the establishment and/or refinement of requisite policies to be presented to the Jordan School District Administration and Jordan School District Board of Education.
3. Determine the training needs for each Jordan School District-level department that collects, manages, or stores student data.
4. Establish and update a list of all third-party vendors who have been contracted to collect, store, or manage student data.
5. Establish and update a list of all personnel who collect, store, or manage student personally identifiable information and the purposes for which that information is used.
6. Aid in the development and distribution of Jordan School District student data privacy training materials including videos, PowerPoints, and handouts.

Committee Members

Steven Harwood (Co-Chair)	**Information Systems, State Data Governance Committee Member**
Holly Allen (Co-Chair)	**Evaluation, Research, and Accountability SDGC Member**
Travis Hamblin	Planning and Student Services (Records Officer)
Tonya Hodges	Purchasing
Ben Jameson	Evaluation, Research, and Accountability
Anthony Muto	Information Systems (Systems Security)
Ross Menlove	Instructional Technology
Brenda Veldevere	Purchasing

STUDENT DATA SECURITY

Introduction

In accordance with federal and state law, Jordan School District follows best industry practices in maintaining the security and confidentiality of all student data. The following information outlines details of these practices.

Passwords

Passwords must be maintained in a manner that reduces the threat of unauthorized access to data. Passwords are to be treated as sensitive and confidential and must not be shared with anyone, including administrative assistants, secretaries, managers, coworkers, and family members. Passwords must not be inserted into email messages, or any other forms of electronic communication. Any user suspecting that his/her password may have been compromised must report the incident to their supervisor who will then notify the Jordan School District Data Security Officer or Information Systems Director and change all passwords.

Workstation Security

Appropriate measures must be taken when using laptops and workstations to ensure the confidentiality, integrity and availability of data, and to minimize the possibility of unauthorized access.

Jordan School District will implement physical and technical safeguards for all laptops and workstations that access protected information to prevent unauthorized user access. The Jordan School District Information Systems Department will encrypt all new laptops that are purchased by the Jordan School District through the Information Systems Department. In addition, the Jordan School District Information Systems Department will encrypt all laptops used by those individuals such as nurses, psychologists and building administrators whose jobs demand that personally identifiable information be kept on their Jordan School District-assigned laptop.

Remote Access

It is the responsibility of all information users with remote access privileges to Jordan School District's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Jordan School District.

When accessing the Jordan School District network from a personal computer, authorized users are responsible for preventing unauthorized access to any Jordan School District computer resources or data. Please refer to the Jordan School District Information Systems Handbook for specific requirements regarding remote access.

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.
- Authorized Users shall protect their login and password, even from family members.
- While using a Jordan School District owned computer to remotely connect to Jordan School District's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct Jordan School District business must be approved in advance by Jordan School District and the appropriate Jordan School District Department manager.
- All hosts that are connected to Jordan School District internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
- Third party connections must comply with requirements as stated above.
- Personal equipment used to connect to Jordan School District's networks must meet the requirements of Jordan School District owned equipment for remote access as stated.

Wireless Access Standards

Jordan School District protects student and staff data by restricting access to the network so that only authorized people can use it. Industry standard security technologies for providing authentication, controlling user traffic, and dynamically varying encryption keys for both wired and wireless Ethernet networks are used. Vendor default passwords are changed on all equipment. Jordan School District also uses industry standard technologies to provide encryption protection for sensitive data being transmitted on the network.

By using the above mentioned security technologies, Jordan School District is able to prevent unauthorized users from being able to see confidential data appearing on the network.

Data Breach

The Jordan School District follows industry best practices to protect information and data in the event of a data breach or inadvertent disclosure of personally identifiable information. Concerns about data breaches must be reported to the Director of Information Systems or the Student Data Privacy Manager who will collaborate with Jordan School District leadership to determine if a breach has occurred. In the event of a data breach, the Jordan School District will respond promptly to ensure that the breach is contained quickly, investigated and that appropriate measures are taken to prevent such breaches in the future.

If there is a release of personally identifiable student data due to a security breach, the Jordan School district shall notify the student, if the student is an adult student, or the student's parent.

JORDAN SCHOOL DISTRICT
STUDENT RECORDS MANAGEMENT POLICIES

DP367 – District Records Management

Effective: 6/23/1992
Revision: 2/14/2012
Reviewed: 8/25/2015

I. **Board Directive**
The Board of Education is committed to see that Jordan School District records are managed in an efficient, responsible manner. Therefore, the Board delegates to the Administration responsibility for establishing criteria for maintaining, classifying, preserving, accessing, and destroying district records in compliance with the Government Records Access and Management Act (GRAMA), Utah Code §63-2-701, annotated 1991.

II. **Administrative Policy**
Records shall be defined as written or electronic records that are owned and maintained by the District. The District Records Policy shall be implemented according to the following administrative policy provisions:

A. Records Management
1. Jordan District records shall be managed under the direction of the principal and/or the appointed records officer of each school and department.
2. The Business Administrator shall be the records officer for all general district records including Board of Education minutes and all documents related to fiscal matters such as property, budgets, payroll, accounts, contracts, etc.
3. The Administrator of Human Resources shall be the records officer for all records related to personnel.
4. The administrator of Planning and Student Services shall be the records officer for all records related to students.
5. The administrator of Planning and Student Services shall serve as the District's liaison to the State Archives.

B. Records Classification
1. All Jordan District records created after July 1, 1992, shall be classified as either public, private, controlled, protected, or exempt.
2. The administrator of Planning and Student Services shall inform the State Archives no later than July 1 each year of the classification of any new record series created during the previous 12 months.

C. Public Records
1. Public records shall include:
a. Official minutes, actions and decisions of the Board of Education and District Administration unless the record involves information which is classified as private, controlled, or protected.
b. Official District and school policies, contracts, minutes, and accounts.

c. Names, gender, job titles, job descriptions, business addresses, business telephone numbers, gross salaries, working hours, and dates of employment of all current and former employees.

d. Documents showing formal criminal charges against an employee unless, in the judgment of the Superintendent, the charges are groundless or the charges are not sustained.

2. Public records shall be open for public inspection during regular office hours.

D. Private Records

1. Private records shall include:

a. Personnel files including applications, nominations, recommendations, evaluations, and proposals for advancements or appointments.

b. Documents related to eligibility for unemployment benefits, social services, welfare benefits, personal finances, individual medical condition, and military status.

c. Individual student records. (See policy AS61—Student Records.)

2. Private records shall be open only to the subject of the record and other authorized individuals or agencies. Access to student records shall be provided in accordance with the Family Educational Rights and Protection Act (FERPA). (See policy AS61—Student Records.)

E. Controlled Records

1. Controlled records shall include records containing medical, psychiatric, or physiological data on an individual which, if disclosed, could be detrimental to the individual's mental health or safety.

2. Controlled records shall be open only to authorized persons or agencies but are not open to the subject of the record.

F. Protected Records

1. Protected records shall include:

a. Any information that, if disclosed, would jeopardize the life or safety of an individual or security of district property or programs.

b. Documents that, if disclosed, would place the District at a disadvantage in contract negotiations, property transactions, or bargaining position or could enable circumvention of an audit.

c. Records related to potential litigation or personnel hearings.

d. Records generated in meetings which are closed in accordance with the Utah Open and Public Meetings law.

e. Test questions.

2. Protected records shall be open only to authorized individuals and agencies or in response to court order.

G. Exempt Records

1. Exempt records shall include student records which are protected by the Family Educational Rights and Protection Act (FERPA).

H. Access to District Records

1. Requests to view District records should be addressed to the appropriate records officer during regular business hours.

2. Individuals requesting to view records classified as private, controlled, or protected shall be required to submit their request in writing. Requesters must prove their right to access the record through personal identification, written release from the subject of the record, power of attorney, court order, or other appropriate means.
3. The records officer shall determine whether access to the requested record(s) is to be granted or denied.
    a. If the request is approved, the records shall be provided as soon as possible and not more than 10 working days from the date the request was received.
    b. If the request is denied, the records officer must specify the reason, and the requester shall be informed of the right to appeal.

I. Appeals Process

1. Appeals to the District Administration
    a. An appeal cannot be filed to access records that would require the District to compile, format, manipulate, package, summarize or tailor information.
    b. An appeal cannot be filed to access records that are not prepared, owned, received or retained by the District.
    c. The requester shall file a written request for a hearing with the administrator of Planning and Student Services at least 10 working days prior to the desired hearing date.
    d. Upon receiving the request, the administrator of Planning and Student Services shall schedule a mutually convenient date, time, and location for the hearing and notify all parties.
    e. The requester has the right to be represented by legal counsel at the hearing.
    (1) If the requester is to be represented by legal counsel, the administration must be notified at least 10 working days in advance of the hearing.
    (2) If the requester has legal counsel present at the hearing, the administration may also be represented by legal counsel.
    f. Within 10 working days of the hearing, the administrator of Planning and Student Services shall notify the requester in writing of the action recommended.
    g. If the requester is not satisfied with the action recommended, an appeal may be filed with the Board of Education.
2. Appeals to the Board of Education shall follow the same procedures and time lines outlined in items E.1. above.
3. If the Board upholds the action recommended in the hearing with the District Administration, the requester has the right to appeal the Board's decision in Third District Court.

J. Copying District Records

1. The District shall charge a fee for duplicating District records that is equal to the actual duplication cost plus any employee time involved.
2. The District shall refuse to allow duplication of copyrighted materials.
3. The District shall charge 50 cents per page for duplicating records. If more than 15 minutes of research is involved, the District shall also charge for all personnel time (actual salary and benefit costs) of the employee fulfilling the GRAMA or other record request.

K. Retention of District Records

1. The District shall adhere to the general schedule for records retention approved by the State Records Committee.
2. Records which are not covered by the general schedule shall be submitted to the State Records Committee for scheduling.

L. Public Access to District Records

1. If public access is granted to view or inspect District records, files, documents, etc., the District shall charge for all personnel time (actual salary and benefit costs) of the individual fulfilling the request necessary to facilitate such access. Fees will also be charged for requests for information involving extensive searches. The fee will be based on the actual salary and benefit costs of the employee fulfilling the request.
2. The District is not required to create a document or file to answer a GRAMA or other request for records. Should the requestor request a document that does not already exist, and if the District agrees to prepare such a document in its sole discretion, all personnel time (actual salary and benefit costs and duplicating costs to prepare that document) will be charged to the requestor.
3. If possible, the District should estimate the preparation cost for such documents in advance, and receive the funds from the requestor, prior to preparing the requested material.

AS61 – Student Records

Effective: 1/27/1976
Revision: 3/25/2014

I. **Board Directive**

Complete and accurate records are essential to student education. Therefore, the Board delegates to the administration responsibility for establishing policy that assures accuracy, completeness, appropriate access, and efficiency in the preparation and management of student records. This policy is to be administered in accordance with the Family Educational Rights and Privacy Act (FERPA) and in compliance with the Government Records Access and Management Act (GRAMA).

II. **Administrative Policy**

The Student Records policy shall be administered according to the following administrative policy provisions:

A. Confidentiality of Student Information and Student Records

1. Employees, student aides, and volunteers in public schools who have access to student records shall receive appropriate training annually from the Planning and Student Services administrator regarding the confidentiality of student records including an overview of all federal, state, and local laws that pertain to the privacy of students, their parents, and their families. They shall become familiar with the laws regarding the confidentiality of student information and student records.
2. All student records that are electronically maintained shall require password protection.
3. An employee, student aide, or volunteer shall not share, disclose, or disseminate passwords for electronic maintenance or access to student records.
4. All public education employees, student aides and volunteers have a responsibility to protect confidential student information and access records only as necessary for their assignments.

5. Public education employees shall maintain confidentiality concerning a student unless revealing confidential information to authorized persons serves the best interest of the student and serves a lawful purpose (see II.C. of this policy).
6. Failure to adhere to confidentiality laws and policies may result in licensing discipline as defined in R277-515-1G.

B. Management of Student Records
1. The Planning and Student Services administrator shall serve as the District Student Records Officer and shall be responsible to see that student records are classified and maintained according to the Jordan District Student Record Classification and Retention schedule found online in the Planning and Student Services manual.
2. The principal shall serve as the Student Records Officer for the school.
    a. The principal shall be responsible to see that counselors, teachers, secretaries, and assistants are appropriately trained in record keeping and follow the Jordan District Student Record Classification and Retention schedule.
    b. The principal shall receive requests to access student records and determine whether access is to be granted or denied.
    c. The principal shall be responsible to see that records are appropriately maintained in safe, secure files which will protect the documents and assure privacy.
    d. The principal shall be responsible to see that records are retained, transferred, archived, and destroyed in a timely, efficient, appropriate manner.
3. Teachers and other school personnel as designated by the principal shall be responsible to see that attendance rolls, student progress reports, grades, health cards, and other necessary student records are prepared and maintained in accordance with this policy, and with all federal, state and local laws.

C. Health or Safety Emergency (FERPA §99.36)
1. If a student poses an articulable and significant threat to the health or safety of the student or other individuals, an educational agency or institution may disclose, without consent, personally identifiable information from a student's education record to any official whose knowledge of the information is necessary to protect the health or safety of the student or other individuals.
2. Educational agencies and institutions shall record the articulable and significant threat that formed the basis for a disclosure under the health or safety emergency, and the parties to whom the information was disclosed.

D. Access Rights
1. All documents in the Student Cumulative/Permanent Record File, which include directory information, ethnic origin, schools and years attended, subjects completed, grades and credits earned, competency evaluations, certain health records, and other documents related to the educational program, shall be classified as private with the exception of certain directory information (refer to Item J).
2. Student records shall be open to:
    a. Authorized school personnel having responsibility for the student's educational program and to individuals conducting district, state, or federal audits of educational programs.
    b. Parents or guardians.

i. In the event that parents are divorced or separated, both parents shall be entitled to access their child's student records unless prohibited by court order.
a) The custodial parent may not prohibit the non-custodial parent's access to their child's written record unless prohibited by court order.
b) A non-custodial parent must make a written request to obtain his/her student's written educational record. A new request must be submitted each time records are requested. Standing requests will not be honored.
c) Access to a student's record granted to non-custodial parents does not include electronic access to academic or attendance records. A school or the District will not disclose the electronic access pin number to the non-custodial parent, unless court documents allow electronic access.
d) A custodial step-parent has the right to written education records only. The non-custodial step-parent has no rights, unless approved in writing by the custodial parent. (34 CFR §99.3 Family Policy Compliance office August 20, 2004).

ii. Information on access rights shall be distributed to parents as part of the school registration packet.

c. Eligible students who are 18 years of age or older or who are married or enrolled in post-secondary education programs.

3. Access to student records shall not be given to individuals other than those listed under item 2. a., b., and c. above without written permission of the parent(s)/legal guardian(s) or eligible student or in response to a court order.
4. Current or future employers, police officers, and public or private agencies have no access rights to student records.
5. Information from student records classified as private shall not be released by telephone even though the caller may be authorized to access the record.

E. Access Requests
1. Requests to access student records should be addressed to the school principal.
a. The requester may be required to submit the request in writing.
b. The requester must prove access rights by personal identification, written consent from the parent(s)/legal guardian(s), or a court order.
c. The principal shall either grant or deny the request as soon as possible. In no event shall the requester be required to wait more than 15 days for a response.
d. The principal shall maintain a record of individuals or agencies that are granted access to student records.

F. Right of Appeal
1. Parent(s)/legal guardian(s) and eligible students who feel that their privacy rights have been violated because access to student records was granted inappropriately should make a written complaint to the Family Educational Rights and Act Office, Department of Health, Education, and Welfare, 330 Independence Avenue, S.W., Washington, D.C., 20201.
2. Individuals who feel they have been inappropriately denied access to student records or who have complaints about record content or management have the right to appeal the principal's decision to the District Administration through the Planning and Student Services administrator.

G. Appeals Process

1. Appeals to the District Administration
    a. The parent(s)/legal guardian(s) or eligible student shall file a written request for a hearing with the Planning and Student Services administrator at least 10 days prior to the desired hearing date.
    b. Upon receiving the request, the Planning and Student Services administrator shall schedule a mutually convenient date, time, and location for the hearing and notify all parties.
    c. The parent(s)/legal guardian(s) or eligible student has the right to be represented by legal counsel at the hearing.
    (1) If the parent(s)/legal guardian(s) or eligible student is to be represented by legal counsel, the District Administration must be notified at least 10 days in advance of the hearing.
    (2) If the parent(s)/legal guardian(s) or eligible student has legal counsel present at the hearing, the District Administration may also be represented by legal counsel.
    d. Within 30 days of the hearing, Planning and Student Services administrator shall notify the parent(s)/legal guardian(s) or eligible student in writing of the action recommended.
    e. If the parent(s)/legal guardian(s) or eligible student is not satisfied with the action recommended, an appeal may be filed with the Board of Education.
2. Appeals to the Board of Education shall follow the same procedures and timelines outlined in G.1. of this policy.
3. If the Board upholds the action recommended in the hearing with the District Administration, the parent(s)/legal guardian(s) or eligible student has the right to appeal the Board's decision in Third District Court.

H. Transferring Student Records
1. Within 14 days after enrolling a transfer student, and simultaneous with enrolling a child of active military personnel, a school shall request, directly from the student's previous school, a certified copy of his/her record.
2. Any school requested to forward a copy of a transferring student's record to the new school shall comply within 30 school days of the request, and within 10 days of a request for a child of active military personnel records, unless the record has been flagged as a "Missing Child," in which case the copy may not be forwarded and the requested school shall notify the police department (refer to item H.3.) Note: A parent release is not required when transferring student records from one school to another.
    a. The permanent cumulative record folder, which includes all of the records created as part of the student's instructional program, shall be purged of all outdated or irrelevant materials and of documents containing confidential medical information, social history, teachers' notes, reports from outside agencies, or other sensitive information included as an insert in the file but not part of the cumulative/permanent record. Items included in the cumulative folder are:
        i. Achievement test scores
        ii. Birth certificate
        iii. Copies of report cards
        iv. Health records
        v. Pertinent information concerning the student

b. The cumulative/permanent records, including directory information, schools and years attended, grades and credits earned, health records (Utah School Immunization Record), and test scores, and transcripts shall be forwarded to the receiving school as follows:
   i. The original records of students in grades kindergarten through eight shall be transferred. Copies of the original records may be provided to the parent(s)/legal guardian(s), if a request is received prior to the time the original records are transferred.
   ii. A certified copy of the cumulative/permanent record along with the original health record (Utah School Immunization Record) of students in grades 9 through 12 shall be transferred to requesting schools outside of Jordan School District.
   iii. The cumulative/permanent records and a copy of the health record (Utah School Immunization Record) of students in grades 9 through 12 shall be archived at the high school until three years after the student would have graduated. Original records for ninth grade students whose records were requested and certified copies mailed, shall be delivered to the feeder system high school to be archived.
   iv. Teacher files on students in resource or other special programs shall be kept until five (5) years after the student graduates or five (5) years after the student turns 22.
   v. The date the record transfer request was received and the date and school where the record was sent shall be entered on each archived file.

c. It is permissible to transmit individual detailed student records between public schools and the Utah State Office of Education through the Utah eTranscript and Record Exchange (UTREx) (R277-404).

3. The principal shall not transfer the record of any student whose file is flagged as a "Missing Child" pursuant to Utah Code Annotated. The principal shall immediately notify the police department of the transfer request. The flag restricting transfer shall be removed from the student's file and the transfer facilitated only upon official police notification that the child has been located.

I. Requests to Correct or Expunge Student Records
   1. Parent(s)/legal guardian(s) and eligible students may request a conference with the principal and ask for correction or expungement if they feel information entered on their student record is inaccurate or inappropriate.
   2. If the requested record change or expungement is denied, the parent, guardian, or eligible student has a right to enter a statement of disagreement into the record.

J. Publication of Directory Information
   1. The principal may authorize the release of certain student directory information for the purpose of publishing school directories, yearbooks, team rosters, honor roll lists, graduation lists, and other school purposes which would not normally be considered an invasion of student privacy.
   2. The Planning and Student Services administrator may authorize the release of certain student directory information for use by United States Military Forces and other authorized agencies.

3. Parents who object to publication of their child's directory information may block publication by submitting a written notification to the principal.
4. Parents have 14 days from the first day of school to provide written notification to the principal to block publication of directory information. (PPRA 20 USC section 1232h)

K. Use of Student Records for Research Purposes
1. Individual student information may not be released for research purposes without written consent from parents.
2. Information which does not reveal the individual identity of a student or infringe upon privacy rights; i.e., group test results, enrollment statistics, etc., may be released by the Planning and Student Services administrator for use in approved research projects.
3. Information involving students which is not generated by the schools such as United States census data may be released to outside individuals or agencies in accordance with state and federal law.

L. Retention of Student Records
1. Attendance class roll books and grade sheets shall be retained three years at the local school.
2. Cumulative/permanent records of students in grades kindergarten to eight, including records created as part of the instructional program and student history shall be maintained at the local school as long as the student is enrolled. When a student transfers, item H. of this policy should be followed. Records that are not requested should be kept at the school until at least three years after the student would have graduated, then destroyed.
3. The original records and a copy of the health record (Utah School Immunization Record) of students in grades 9 through 12 shall be archived at the high school until at least three years after the student would have graduated, then destroyed.
4. Transcripts, including but not limited to grades, directory information, recorded suspensions and expulsions shall be archived permanently at the local high school.
5. Teacher files on students in resource or other special programs shall be kept until five (5) years after the student graduates or five (5) years after the student turns 22.
6. The date the record transfer request was received and the date and school where the record was sent shall be entered on each archived file.

M. "Transcript" means an official document or record(s) generated by one or several schools and shall be permanently retained at the high school. The transcript shall include, at a minimum:
1. Courses in which the secondary student was enrolled
2. Grades and units of credit earned
3. State basic standard competency skills test scores and dates of testing
4. Citizenship and attendance records
5. Notation of any recorded suspensions and/or expulsions, which shall be defined as 10 or more days for which a due process hearing was conducted. (Utah Code 53A-11-907 (4) (a))
6. By State Rule 277-404, it is permissible to transmit transcripts through Utah eTranscript and Record Exchange (UTREx) to any post-secondary institution that participates in the e-transcript service.

N. Diplomas or certificates, credit or unofficial transcripts may not be withheld from students for nonpayment of school fees. (State Board Rule R277-705.)

1. Cap and gown may be withheld and a student not be allowed to participate in graduation ceremonies for nonpayment of school fees.
2. The diploma may be withheld until after the graduation ceremony for nonpayment of school fees; however, once the graduation ceremonies are completed, the diploma cannot be withheld and must be awarded to the student.

RESEARCH REVIEW POLICY

AA428 – Research Projects and Proposals

Effective: 8/27/1969
Revision: 9/8/2009
Reviewed: 12/10/2013

I. **Board Directive**
The Board encourages and supports research projects relating to the various functions of the District. The Board recognizes that current research data are required in the development of improved operational and instructional programs. The Board delegates to the Administration the responsibility for policy regarding research in the District.

II. **Administrative Policy**
District administrators shall actively support and promote appropriate research by identifying and encouraging projects concerning operational and instructional programs. In recognition of the need to coordinate such research efforts, the Administration shall appoint a Research Review Committee and delegate to the committee the responsibility for the review and approval of research project proposals. The Director of Evaluation, Research and Accountability shall accept and coordinate requests for research projects.

A. The Administrators of Schools and the Director of Evaluation, Research and Accountability shall constitute the Research Review Committee.

B. One Administrator of Schools serves as chairperson of the Research Review Committee.

C. Administrators, principals, and consultants may be used as advisers to the Research Review Committee.

D. The committee shall review all research proposals to determine their educational value and to evaluate the research design. The Committee will then approve or disapprove each research project.

E. Applicants requesting to conduct research projects shall submit to the Research Review Committee a completed Research Project application and a written proposal that outlines the purpose of the research, the methodology to be followed, the instruments to be used, and the anticipated benefits which shall accrue to the District upon completion of the research.

F. Requests for budgeting support for research projects shall be prepared and submitted to the administrator in charge of research prior to March 1st.

G. Following consideration by the Research Review Committee, formal notice of approval or disapproval shall be given to the applicant by the Committee chairperson.

H. Administrators of Schools, division administrators, and department directors shall have the responsibility to coordinate approved research projects within their areas or departments.

I. Upon completion of a research project, whether or not the District participates in the funding, a copy of the findings, thesis, dissertation or other written report shall be submitted to the administrator in charge of research. The results of significant projects shall be reported to the Administrative Cabinet, appropriate staff members and/or the Board of Education by the chairperson of the Research Review Committee.