

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 16 – Records Management - Table of Contents

Article I. GENERAL RECORDS AWARENESS 127

 Section 1.01 Responsibility 130

 Section 1.02 What is a “Record?” 130

 Section 1.03 Exclusions 131

 Section 1.04 Administrative Records – Open and Closed 131

 Section 1.05 Student Records..... 131

 Section 1.06 Subpoenas for Records 131

 Section 1.07 Records Control Schedule 132

 Section 1.08 Tyler ISD Records Management Program 132

Article II. RECORDS MANAGEMENT ORGANIZATION 133

 Section 2.01 Role of the Records Management/Public Information Officer 133

 Section 2.02 Selection of Records Coordinators 134

 Section 2.03 Role of Records Coordinators 134

 Section 2.04 Records Control 134

Article III. HANDLING STUDENT RECORDS REQUESTS 135

 Section 3.01 Student Information Requests..... 135

 Section 3.02 Definitions..... 135

 Section 3.03 Privacy and Student Information 136

 Section 3.04 Record of Information Requests and Release 136

 Section 3.05 Parental Access to Student Records 137

 Section 3.06 Request for Student Records to be Amended/Corrected 137

 Section 3.07 Release of Student Information without Consent..... 138

 Section 3.08 Student High School Transcript Requests 139

 Section 3.09 High School Transcript Charges 139

 Section 3.10 Student/Parent Mailing List Requests 139

Article IV. HANDLING ADMINISTRATIVE RECORDS REQUESTS 140

 Section 4.01 Public Information Requests (Open Records) 140

 Section 4.02 TPIA Request Procedures 140

 Section 4.03 Open or Protected 141

 Section 4.04 Administrative Record Charges 141

 Section 4.05 Employee Mailing Lists 142

Article V.	REQUEST FORMS AND RECORDS CHARGES	143
Section 5.01	Records Available at No Charge.....	143
Section 5.02	Record Charges	143
Section 5.03	Procedure for Copy Charges	143
Article VI.	CORRESPONDENCE RECORDS	144
Section 6.01	Definition	144
Section 6.02	Classification and Retention.....	144
Section 6.03	Management of Correspondence Records	145
Section 6.04	Email Correspondence.....	145
Article VII.	RECORDS EVALUATION AND VITAL RECORDS.....	146
Section 7.01	Record Evaluation	146
Section 7.02	Records Appraisal	146
Section 7.03	Records Classification.....	146
Section 7.04	Essential, Useful, and Non-Essential Records	147
Section 7.05	Vital Records	147
Section 7.06	Identification of Vital Records.....	147
Section 7.07	Management of Vital Records.....	148
Section 7.08	Protection of Vital Records.....	148
Section 7.09	Methods of Vital Records Protection.....	148
Section 7.10	Preservation of Records Relevant to Legal Matters	148
Section 7.11	Disaster Planning	149
Article VIII.	ELECTRONIC RECORDS, FILING, AND STORAGE	149
Section 8.01	Record Types	149
Section 8.02	Standards	149
Section 8.03	Preferences and Common Files Types.....	150
Section 8.04	Management	151
Section 8.05	Privacy of Electronic Communications.....	151
Article IX.	ELECTRONIC IMAGE MANAGEMENT AND FILEBOUND	151
Section 9.01	Definition	151
Section 9.02	Standards	153
Section 9.03	Management	153
Section 9.04	FileBound – Content Management Program	153
Article X.	MICROGRAPHICS.....	154
Section 10.01	Definitions	154
Section 10.02	Standards.....	154
Section 10.03	Management	154
Article XI.	FILING STANDARDS AND FORMS CONTROL	154
Section 11.01	Filing Systems.....	154
Section 11.02	Filing Training and Audits	155
Section 11.03	Definition of Forms Control	155

Section 11.04	Overview of Forms Control	155
Section 11.05	Forms Approval and Management	155
Article XII.	RECORDS CONTROL AND DESTRUCTION	156
Section 12.01	Definition and Purpose.....	156
Section 12.02	Standards.....	156
Section 12.03	Disposal and Destruction of Records	157
Section 12.04	Keeping Control of Records.....	157
Section 12.05	Archival of Records.....	158
Section 12.06	Management of Student Records	159
Article XIII.	CENTRAL AND OFF-SITE RECORDS STORAGE.....	159
Section 13.01	Responsibility.....	159
Section 13.02	Procedures.....	159
Article XIV.	PRIVACY AND IDENTITY PROTECTION.....	159
Section 14.01	Purpose.....	159
Section 14.02	Scope.....	160
Section 14.03	Sensitive and/or Confidential Information.....	160
Section 14.04	Protection of Hard Copy Distribution	161
Section 14.05	Protection of Electronic Distribution.....	161
Section 14.06	Breach of Sensitive and/or Confidential Information	162
Article XV.	GLOSSARY.....	163

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Article I. GENERAL RECORDS AWARENESS

Section 1.01 Responsibility

The Tyler Independent School District (herein referred to as Tyler ISD) uses public funds to provide education services to the community. This gives us great responsibility to the public to document how their money is spent and how their children are served. Several laws outline our responsibilities in creating, maintaining, and documenting records of our efforts:

- Local Government Records Act (LRGA), Chapter 201 to 205, Local Government Code, 1973
- Local Government Code, Chapter 552, Public Information
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g (Buckley Amendment), 1974

Copies of these laws are available for review in the Records Management Office. As a district employee you may create, transcribe, handle records, or even be asked for information by members of the public. It is important that you understand your responsibilities under the law and district procedures. Tyler ISD requires that its records be managed in a systematic and logical manner according to plans developed by the departments that maintain those records in conjunction with procedures established by the Records Management Department, and consistent with applicable law.

Section 1.02 What is a "Record?"

A "Record" is any form of information in the custody of a local government that belongs to the public. Local government records may not be destroyed without prior scheduled or specific permission from the state. The district maintains two main categories of records: Administrative Records related to business and support services, and Student Records related to individual students.

As defined by the Local Government Records Act, Chapter 201.002(b), the legal definition of a local government record is:

...any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium, or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under the law of the state, created, or received by a local government of any of its officers or employees pursuant to law, including an ordinance, or in the transaction of public business.

In other words, most of the information created and received in daily district operations is a record. For each record, there is only one "Official Source Record." Other copies may be described as "Convenience Copies." The Official Source Record is the one copy that must be retained for the retention period listed in the Record Control Schedules adopted by Tyler ISD.

The record copies of records are public property. District officials or employees have no property right to records, even though they may have created or received them. Local Government Records Act, Chapter 201.005

Unauthorized destruction, removal from files, or personal possession of record copies of records may be a Class A misdemeanor, punishable by a \$25 to \$4,000 fine and imprisonment in the county jail for 3 days to 6 months. Local Government Records Act, Chapter 202.008 and 202.009

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 1.03 Exclusions

These items are NOT local government records:

- Extra identical copies of documents created for convenience, reference, or research;
- Notes, journals, diaries, and similar documents created only for personal convenience;
- Blanks forms and stocks of publications;
- Library or reference materials acquired solely for display; and
- Copies of documents provided to the public under Chapter 552.

Section 1.04 Administrative Records – Open and Closed

In 1973, the Texas Legislature enacted the Texas Open Records Act, which was recodified in 1995 as Chapter 552, Public Information, of the Texas Local Government Code. Chapter 552 makes all information in the possession of local governments available to the public with certain exceptions. Any request for records not specifically related to an individual student is a Public Information Request. A Public Information Request must be made in writing, and if the records are not readily available, requestors must agree to pay any charges before the overhead expense in reproducing or gathering then is incurred.

Records containing information deemed confidential by law, either Constitutional, statutory, or by judicial decision, are called protected or closed records, and may not be released. Releasing protected information may be a civil or criminal offense. **The Records Management/Public Information Officer has been appointed Public Information Officer and should immediately be notified of any requests.** If a member of the public asks for information that may be protected for any reason, the district has exactly ten (10) days to ask the Attorney General's Office for an opinion. If they agree, the records may not be released. If they disagree, we must release it. If, however, we do not ask in ten (10) days, the information automatically becomes an open record and must be released; therefore, it is extremely important to notify Records Management upon receipt of the request.

Section 1.05 Student Records

According to federal law, student records include the cumulative folder and clinic health files. They generally do not include other files, such as counseling or discipline files, if those files are maintained separately from education records and are only accessible to the creators of those files. Texas State law, specifically Chapter 26 of the Texas Education Code (Senate Bill1), mandates that parents have access to all written records maintained on an individual student. Handling requests for student information is covered in detail in Section 2 of this guide.

Section 1.06 Subpoenas for Records

A valid subpoena is a court order, and must be obeyed. Subpoena for records are often delivered to the building or department where the record is stored. Advise any process server who hand-delivers a subpoena that the Records Management/Public Information Officer is the designated Custodian of Records for all district records.

A subpoena to appear as a witness will be hand-delivered to the witness being subpoenaed. Please forward a copy of all subpoenas to appear as a witness regarding school related business to the Records Management/Public Information Officer for review. The witness must obey and appear in court on the date noticed, unless otherwise advised by Administration.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Failure to appear on the date noticed or respond in the time allowed by law to a subpoena may result in being charged with contempt of court. It is the responsibility of the Records Management/Public Information Officer to respond on the district's behalf to all subpoenas for records. **Please forward all subpoenas, along with a copy of the requested information, if it is readily available, to Records Management immediately upon receipt.**

Section 1.07 Records Control Schedule

In accordance with the Local Government Record Act, Tyler ISD by declaration has adopted the following Retention Schedules from the Texas State Library and Archives Commission (herein referred to as TSL):

Local Schedule SD – Retention Schedule for Records of Public School Districts;
Local Schedule GR – Retention Schedule for Records Common to All Local Governments;
Local Schedule PS – Retention Schedule for Records of Public Safety Agencies;
Local Schedule EL – Retention Schedule for Records of Elections and Voter Registration; and
Local Schedule TX – Retention Schedule for Records of Property Taxation.

Inventories and audits are conducted by Records Management to ensure compliance with the retention schedules and so supplemental schedules can be filed with TSL as needed.

We must control and dispose of district records according to the control schedules. If we have records, which are not listed in our schedules, the District must ask permission from the TSL before they can be destroyed and/or submit a Supplemental Records Control Schedule for the unaccounted for record series. The Records Management/Public Information Officer is responsible to secure such permission and/or submit the Supplement Records Control Schedule.

Section 1.08 Tyler ISD Records Management Program

Tyler ISD is committed to effective records management, including meeting legal standards for record retention and protection of privacy, optimizing the use of space, minimizing the cost of record retention, and properly destroying outdated records. These procedures apply to all records, regardless of whether they are maintained in hard (paper) copy, electronically, or in some other fashion.

The efficient management of local government records is necessary to the effective and economic operation of local and state government. Local Government Records Act, Chapter 201.002(1)

The primary duty of Tyler ISD is the education of children. Changes in reporting requirements, a more mobile population, and increasing demands for all types of information result in an administrative incubus of files and record handling. The vision of Records Management is to provide leadership and direction to promote effective records management in support of Tyler ISD; to establish and maintain procedures that ensure proper access to all public and confidential information for our students/alumni, the community, Board of Trustees, and staff now and in the future; and to establish Tyler ISD as a recognized leader in the field of records retention and preservation of District Official Records. Our ultimate goal is to reduce handling time of records for educational staff; in turn, increasing the time and money spent in our primary focus – serving our students and community.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

The District's Records Management Program is headed by the Records Management/Public Information Officer, overseen by the Deputy Superintendent and Board, and implemented by Records Coordinators in each department, school, and building.

"Records Management" means applying management techniques to the creation, use, maintenance, retention, preservation, and disposal of records. The intent is to reduce overall costs and improve the efficiency of recordkeeping.

The District's program includes:

- Establishment of record control schedules;
- Management of filing and information retrieval systems;
- Protection of essential and permanent records,
- Economical and space-effective storage of inactive records;
- Management of creation and distribution of forms;
- Control over release of student education records;
- Management of micrographics;
- Electronic and other records storage systems; and
- Control over requests for public information.

Article II. RECORDS MANAGEMENT ORGANIZATION

Section 2.01 Role of the Records Management/Public Information Officer

The Records Management/Public Information Officer shall be the person designated by the Board of Trustees and registered with the State. In addition to other duties assigned in this operating instruction, the Records Management/Public Information Officer shall:

- Administer the records management program and provide assistance to administrators and employees in its implementation.
- Plan, formulate, and prescribe records disposition policies, systems, standards, and procedures.
- In cooperation with administrators and employees, identify vital records and assist in establishing a disaster plan for each district department and school to ensure maximum availability of the records to re-establish operations quickly and with minimum disruption and expense.
- Develop procedures to ensure the permanent preservation of the historically valuable records of Tyler ISD.
- Establish uniform standards for filing and storage equipment and for record-keeping supplies.
- Establish a uniform filing system for all district offices and schools of Tyler ISD.
- Establish a forms management program for Tyler ISD.
- Provide records management advice and assistance to all Tyler ISD departments by preparing a guide of procedure and policy and by providing training.
- Monitor records retention schedules and administrative rules issued by the TSL to determine if the records management program is in compliance with state regulations.
- Disseminate to the Superintendent of Schools and department heads information concerning state laws and administrative rules relating to local government records.
- Instruct Records Coordinators or other personnel in policies and procedures of the records management program and their duties in the records management program.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

- Direct and assist Records Coordinators or other personnel in conducting records inventories to ensure compliance with the record control schedules and to supplement schedules for additional record series as required and needed.
- Ensure the maintenance, preservation, microfilming, destruction, or other disposition of district records management program and requirements of state law.
- Maintain records on the volume of records destroyed under approved record schedules, the volume of records microfilmed or stored electronically, and the estimated cost and space savings as the result of such disposal or disposition.
- Report annually to the Superintendent of Schools on the implementation of the records management plan in each department and school of Tyler ISD.
- Bring to the attention of the Superintendent of Schools non-compliance by administrators or other Tyler ISD personnel with the policies and procedures of the records management program of the Local Government Records Act.

Section 2.02 Selection of Records Coordinators

One or more Records Coordinators will be selected by administrators in each department and school to assist with the implementation of the Records Management Program. An administrator or director may serve as the records coordinator for his or her office.

Persons selected as Records Coordinators shall be familiar with and have full access to all records created and maintained by their office, school, or department. In the event of resignation, retirement, dismissal, or removal of a person designated as Records Coordinator, the department or school administrator shall promptly designate another person to fill the vacancy.

Section 2.03 Role of Records Coordinators

In addition to other duties assigned in this operating guide, Records Coordinators shall:

- Assist with the inventories of the records of department or school.
- In cooperation with the Records Management Office, coordinate and implement the policies of the records management program in their department or school.
- Disseminate information to departmental or school staff concerning the records management program.
- Advise Records Management regarding the creation, use, and improvement of existing forms and filing systems.
- Replace outdated forms with current forms and ensure the use of approved forms and filing systems.

Section 2.04 Records Control

All records of Tyler ISD are hereby declared to be under the management of and are the responsibility of the District's Records Management Program.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Article III. HANDLING STUDENT RECORDS REQUESTS

Section 3.01 Student Information Requests

Consider the following situations:

- A relative calls trying to locate a student.
- Child Protective Services wishes to verify enrollment.
- A reporter wants to interview students about national issues.
- A high school senior needs transcripts sent to three colleges.
- A business wants a student mailing list to send discount coupons.
- An old friend is trying to locate a parent by checking student enrollment.
- The PTA needs a list of parent addresses and phone numbers.
- Teachers are asked to comment on the tragic death of a student.
- A potential employer needs a copy of a student transcript.

All of these are requests for student information and are governed by 20 U.S.C. §1232(g), the Family Educational Rights and Privacy Act (FERPA). Schools gather and create a tremendous amount of personal information about student and parents. FERPA ties the District's federal funding to our handling this confidential information responsibly. A request for student information must be made in writing, with signature, proof of identification, and confirmation of a right to access of the records (as discussed further in this section), Student Records Request (RMO-0001) may be completed and submitted.

The Communications Department, in conjunction with the Records Management/Public Information Officer, will handle all media requests for student information.

Section 3.02 Definitions

The following definitions apply to student information:

Personally Identifiable Information – is information, which would personally identify the student. This includes the student's name, address, telephone number, social security number, student identification number, and names of parents or other family members. **Personally identifiable information must not be released without the prior consent of the parent, guardian, or adult student.**

Directory Information – is information, which under normal circumstances, would not be harmful, or an invasion of privacy if disclosed. Tyler ISD defines directory information as: student's name, address, telephone number, photograph, date and place of birth, dates of attendance, grade level, participation in officially recognized activities and sports, weight and height of members of athletic teams, honors and awards received, the most recent school attended.

NOTE the overlap between Personally Identifiable Information and Directory Information!

Education record – are those records directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. Education records do not include records about

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

students that are maintained separately from the student's education record and are not open to anyone but the creator of those records.

Parent – refers to the student's natural parent, court-appointed guardian, or person acting in the capacity of parent. For instance, this may include a step-parent who is clearly identified to be active daily in the child's life or a grandparent/other family member who has physical custody of a child. Parents have the right to review their child's records at any time during normal business hours.

Eligible Student – means a student who may access his or her own education records. Eligible students must be 18 years old or attending a postsecondary institution. When a student turns 18, the right of accesses passes from the parent to the eligible student.

Section 3.03 Privacy and Student Information

FERPA and district policy allows parents to choose whether or not directory information about their child may be published or released. The Tyler ISD Student & Parent Handbook and annual enrollment form, sent home with each student for parent signatures, both state our directory information policy. The policy is also published on the Tyler ISD website and in the TISD Policy Online. It is the responsibility of parent to give written notice if they wish to elect privacy. If a parent chooses the privacy option, we may not release information about the parent or child except to other education institutions or in case of emergency.

Whether enrollment confirmation, address, or phone number should be released over the telephone or by email is sometime difficult to determine. Investigators, non-custodial parents, even a bill collector, etc. use any available resource to locate parents and children. We simply do not have enough information to make the right judgment based on a phone call and sometime not enough based on an email. The District's general counsel advises that we not release directory information without a written request. In some cases, we might wish to relay a request to the parent rather than releasing information. The parent or legal guardian may give permission for the District to release information to a third party not enumerated by law as discussed in Section 2.5 of this guide. A Third Party FERPA Release (RMO-0004) or similar authorization from the parent must be obtained before disclosing information to the third party. If you have a question whether information should be released, please contact Records Management before releasing student information. If you are concerned that the request might impact the welfare of the child involved, contact Student Services. If the request might impact the District's public image, contact Communications.

Before you confirm directory information for a caller or an email from another district or Child Protective Services, please ask for the caller's name and number and make a call to verify identity or require the caller to fax a written request on letterhead.

Before releasing directory information about any student, please verify whether the parent has asked for "privacy," which restricts the release of directory information.

Section 3.04 Record of Information Requests and Release

A record of each request for access to and each disclosure of personally identifiable information from a student's record must be maintained for requests which:

1. Are not pre-authorized by the parent or eligible student;

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

2. Are from education institutions outside the District; or
3. Are outside the boundaries of “typical” requests for directory information.

In accordance with FERPA and the TSL, this record must be maintained as long as the student’s records are maintained. This record shall be maintained in the student’s cumulative folder by placing a copy of the request in the folder. The requests and documentation of disclosure must include the parties requesting information and the legitimate interests the parties had in requesting or obtaining the information. Family Educational Rights Privacy Act, 20 U.S.C. §1232(g).

Section 3.05 Parental Access to Student Records

Either parent may review their child’s education records any time during normal business hours, unless the District has received a copy of a court order terminating the parent’s rights or forbidding access.

Parental access to education records is guaranteed under the law:

An educational agency of institution shall give full rights under the Act to either parent, unless the agency or institution has been provided with evidence that there is a court order, state statute, or legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights. Family Educational Rights Privacy Act, 20 U.S.C. §1232(g).

It is the responsibility of the managing conservator to provide us with documentation that limits the possessory conservator’s access to the student or the student’s records. Without legally binding document, the District must allow equal parental access to all of a student’s education record, regardless of which parent enrolled the student or completed forms. Please note whether the non-custodial parent is restricted from learning the address or phone number of the custodial parent and student(s). If such a restriction exists, all evidence of addresses and phone numbers must be redacted before the non-custodial parent may view the records.

Records Management will review custody documents and court orders as requested. According to FERPA and the District’s general counsel, unless the document specifically denies the non-custodial parent the right to access student records, the right must be granted.

If a parent requests to restrict a non-custodial parent’s access to their child or their child’s records, and no legally binding document exists, the parent should be instructed to contact Student Services.

The parent or legal guardian can request to inspect the student’s records during normal business hours. A Notification of Approval/Denial of Request to Inspect Educational Records (RMO-0010) has been provided for your convenience, should you receive a request to inspect student records.

Section 3.06 Request for Student Records to be Amended/Corrected

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g, states:

Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

A parent or legal guardian requesting an amendment be made to student records should make a request to amend. The District must notify the requestor that their request has been either approved or denied. If the parent does not agree with the decision, they may request a hearing on the matter with the District. If a request for hearing is made, please notify and send request to the Director of Student Services. The following forms have been provided for your convenience, but are not required as long as the process has been adequately documented in the educational records of the student:

- Request for Amendment of Education Records (RMO-0011);
- Notification of Approval/Denial of Request to Amend Education Records (RMO-0012);
- Notification of Hearing on Amendment to Education Record (RMO-0013).

One of the most common requests from parents is to change a student's name. However, House Bill 1276 enacted by the Legislature in 2000 added [§25.0021](#) to the Education Code that requires a student to be identified by either the name on the birth certificate or a court order changing the student's name. The only way to identify a student by a different name would be to have his name legally changed. If you are have any questions regarding a request to change a student's name, please contact Student Services or the PEIMS Coordinator.

Section 3.07 Release of Student Information without Consent

In accordance with FERPA and 34 CFR §99.31, district employees may release student information without prior parental consent to:

1. School officials with legitimate educational interest;
2. Other schools to which a student is transferring;
3. Specified officials for audit or evaluation purposes;
4. Appropriate parties in connection with financial aid to a student;
5. Organizations conducting certain studies for or on behalf of the school;
6. Accrediting organizations;
7. To comply with a judicial order or lawfully issued subpoena;
8. Appropriate officials in cases of health and safety emergencies; and
9. State and local authorities, within a juvenile justice system, pursuant to specific State law.

District employees may verbally confirm basic enrollment information, including current and previous school, graduation or withdrawal date, and health record verification to officials of other educational institutions, Child Protective Services, and law enforcement without parental consent. The procedure for telephone or email verification is to take the name and number of the caller, then call back to confirm their identity before releasing information or require the caller to fax a written request on letterhead.

A Checklist for Disclosure to a Third Party outside the Student's School of School System (RMO-0008) is provided for your assistance to ensure compliance.

If student records are provided to an organization conducting certain studies for or on behalf of the school or an accrediting organizations a Certificate of Nondisclosure (RMO-0009) must be obtained.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 3.08 Student High School Transcript Requests

District employees may not provide copies of student transcripts to anyone without a specific, signed, and dated release from the parent or eligible student, except to the parties listed above in Release of Student Information without Parental Consent. 20 U.S.C. §1232g(b)(1) and (b)(2)(A).

Transcripts for current year students and last year's graduating class (1 year) can be requested from the school of attendance. PACE graduates and all other Tyler ISD graduating classes must make requests from Records Management.

Transcript requests may be made online at <https://tylerk12.scribonline.com/foldreq/request.html> or in person/by mail by filing out the Student Transcript Request Form (RMO-0002), or by sending a written request Records Management with the following information:

1. Name at the time of graduation
2. Date of birth
3. School from which you graduated
4. Year of graduation
5. Phone number where you can be reached
6. Address to send transcript
7. Copy of picture identification

The requests should be processed within 2 to 5 business days of receipt of the request. It is the goal of Records Management to provide the transcript as soon as possible, but due to the amount of requests and records maintained this is not always possible.

Picture identification is required when a transcript is being requested. If the student is 18 years or older, school records will not be released to a parent without the student's written consent as mandated by the Family Educational Rights and Privacy Act (FERPA). A transcript may not be provided to a party other than the parent or eligible student without the parent or eligible. If records are sent to a home address, the seal on the envelope must not be broken to be a valid official transcript.

Section 3.09 High School Transcript Charges

Current students needing transcripts for college applications will be charged \$2.00 per transcript. For former students, there is a \$5.00 fee for the first verified official transcript copy and \$2.00 for each additional verified official transcript. For current and former students, there is a \$2.00 fee for a non-verified official transcript copy and \$0.10 for each additional copy. Checks or money orders should be made payable to Tyler ISD. Upon request, a receipt or statement of charges will be provided. See schedule of Records Charges Form in Section 4 of this guide.

These fees vary slightly for requests made online due to processing and transaction fees associated with online payment by credit/debit card.

Section 3.10 Student/Parent Mailing List Requests

A request for student or parent mailing lists is a directory information request and will be handled under public information request procedures. Mailing list requests from any party are handled centrally through Records

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Management. See Public Information Requests in Section 16.3 of this guide. Under no circumstances will a list of student or parent telephone numbers be sold. Parents who elect privacy of directory information will be excluded from all mailing lists. Parents must elect privacy as stated in Section 2.2 Privacy and Student Information in this guide. Charges for mailing lists depend on the number of schools and output format of the report. Contact Records Management for exact charges.

Article IV. HANDLING ADMINISTRATIVE RECORDS REQUESTS

Section 4.01 Public Information Requests (Open Records)

Any request for information that is not part of student education records is a public information request and is governed by Texas Public Information Act, Government Code Chapter 552, Public Information. Members of the public are not always aware that their requests for information are public information requests. Chapter 552 specifies that all local government records are open to the public with only certain exceptions listed in Section 3.3 of this guide.

The District is not required to create special reports or to excerpt specific information from a format in which it already exists. We are required, however, to make reasonable efforts to locate the type of information being requested, even if it does not exist in the exact form the requestor specifies. The District policy is to make public information available to the public as quickly as possible, GBA (Legal) and GBAA (Legal). Please remember, however, that the release of closed or protected records may be a criminal offense.

Section 4.02 TPIA Request Procedures

The following procedures have been established to ensure a consistent method of handling public information requests. All requests for public information should be submitted to the Records Management/Public Information Officer. This procedure allows the district to accurately document the date each request is received and comply with the Public Information Act to respond to the requestor promptly. If the records cannot be produced within ten (10) business days, the Records Management/Public Information Officer will notify the requestor in writing of the reasonable date and time when it will be available. For any items that the District wishes to withhold, the District will ask for a ruling from the Office of the Texas Attorney General prior to the ten (10) day deadline from receipt of the request.

With the exceptions of viewing a normally available public document and demographic information available by phone, all public information requests must be in writing. The request must ask for records or information already in existence. The Act does not require the District to create new information, to do legal research, or to answer questions. Media requests should be forwarded to the Communication Department and are considered separate requests from public information requests.

A Public Information Request may be made by email to the Records Management/Public Information Officer, by fax, via the website, or by filing out and submitting Public Information Request (RMO-004a). However, any form of written request is sufficient if it contains the following information:

1. Name, address, and phone number of requestor;
2. Date of the request;
3. Sufficient description of the requested information; and
4. Whether the information is requested for review or duplication.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

You are not allowed to ask the requestor why they want the information or any personal questions about the requestor other than their name, address, phone number, and information needed to produce the records.

Refer all requests and questions regarding public information to the Records Management/Public Information Officer. The Records Management/Public Information Officer will correspond with the requestor, as well as the department or school that retains and must produce the records being requested.

Section 4.03 Open or Protected

Every record not specifically closed by an exception or decision of the Attorney General is assumed to be open under the law. **If you are asked to provide records to the Records Management/Public Information Officer in response to a public information request and you believe it may be protected or should not be released, please contact the Records Management/Public Information Officer IMMEDIATELY.** It is the responsibility of the Records Management/Public Information Officer to determine if records are protected and to request a ruling from the Attorney General. Under Chapter 552, all records are presumed to be open records and must be made available to a member of the public unless they fall under one of these exceptions:

- Information deemed confidential by law, either Constitutional, statutory, or by judicial decision.
- Information in personnel files, which would constitute a clearly unwarranted invasion of personal privacy.
- Information, which if released, would give an advantage to competitive bidders.
- Information pertaining to the location of real or personal property for public purposes prior to public announcement if the project and information pertaining to appraisals or purchase price of real or personal property for public purposes prior to the formal award of contracts therefore.
- Private correspondence and communications of an elected office holder relating to matters the disclosure of which would constitute an invasion of privacy.
- Inter-agency or intra-agency memorandums or letters, which would not be available by law to a party in litigation with the agency.
- Information relating to the home address, home telephone number, or social security number, or that reveals whether the person has family members of each employee and official and each former employee and official that has elected privacy under Section 552.024 to the main personnel officer in a signed written notice not later than the 14th day after the date of hire, election, or the end of service.
- Curriculum objectives and test items developed by educational institutions that are funded wholly or in part by state revenue and test items developed by licensing agencies or governmental bodies.
- Student records at educational institutions funded wholly or in part by state revenue, but such records shall be made available upon request of educational institution personnel, the student involved, that student's parent, legal guardian, or spouse or a person conducting a child abuse investigation required by Section 34.05, Family Code.

Section 4.04 Administrative Record Charges

The District is responsible to the entire community for proper use of public funds. Therefore, when an individual member of the public requests records be made available for their personal inspection, or requests copies of district records for personal reference, the individual making the request must pay any costs to the District incurred in providing the information.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Furthermore, these costs must be paid prior to the District releasing the information to the applicant. A governmental body is required to provide a requestor with an itemized statement of estimated charges if charges for copies of public information will exceed \$40, or if a charge in accordance with §70.5 of the Texas Administrative Code (relating to Access to Information Where Copies Are Not Requested) will exceed \$40 for making public information available for inspection. The itemized statement of estimated charges is to be provided before copies are made to enable requestors to make the choices allowed by the Act. A governmental body that fails to provide the required statement may not collect more than \$40. The itemized statement must be provided free of charge and shall contain the following information:

- (1) The itemized estimated charges, including any allowable charges for labor, overhead, copies, etc.;
- (2) Whether a less costly or no-cost way of viewing the information is available;
- (3) A statement that the requestor must respond in writing by mail, in person, by facsimile if the governmental body is capable of receiving such transmissions, or by electronic mail, if the governmental body has an electronic mail address;

If after starting the work, but before making the copies available, the governmental body determines that the initially accepted estimated statement will be exceeded by 20% or more, an updated statement must be sent. If the requestor does not respond to the updated statement, the request is considered to have been withdrawn by the requestor.

The District may require a deposit or bond if the estimated charges are \$100 or more. If the District cannot produce the public information for inspection and/or duplication within 10 business days after the date the written response from the requestor has been received, shall certify to that fact in writing, and set a date and hour within a reasonable time when the information will be available. Texas Administrative Code §70.7.

It is important that the department(s)/school(s) responding to a public information request provide the Records Management/Public Information Officer with an estimated amount of time, fees, and charges associated with responding to the request.

A list of authorized charges in accordance with the Texas Public Information Act, Texas Administrative Code, and Board Policy GBAA (Exhibit) appears in Section 4.2.1 of this guide.

Section 4.05 Employee Mailing Lists

Requests for mailing lists of current and former District employees are open records requests and will be handled centrally by the Records Management/Public Information Officer. Requests for mailing list will be handled under procedures described in Section 3.0 TPIA Request Procedures in this guide.

Current and former employees who elect privacy of home address will be excluded from all mailing lists. Contact Human Resources regarding questions regarding privacy election, see Section 3.2 Open or Protected of this guide.

Charges for mailing lists depend on the number of names and output format of the report. Contact Records Management for exact charges.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Article V. REQUEST FORMS AND RECORDS CHARGES

The District is responsible to the entire community for proper use of funds. Therefore, when an individual member of the public requests that records be made available for their personal inspection, or requests copies of district records for personal reference, the individual making the request must pay any costs to the District in providing this information. A cash prepayment is required for all information requests costing over \$100.00.

Section 5.01 Records Available at No Charge

There is no charge to review any normally available public document; for example, an Annual Financial Report, or a Budget Public Hearing document. Furthermore, there is no charge for the inspection of readily available documents in district offices during business hours.

Section 5.02 Record Charges

Charges for copies of available records must be according to the District's record charges schedule, which follows the recommended rates set by the Texas Attorney General. See Schedule of Record Charges in Section 4.1.2 of this guide.

If records must be edited for review, including computer processing and screening confidential information in an otherwise public record, the charge will be for the actual overhead in editing the requested records.

An estimate of record charges shall be provided to the applicant, who shall then agree to proceed with the request before the overhead cost in gathering the requested information is incurred.

Monies collected will be deposited to the account provided by the department or school which produced the documents, thus incurring the fees.

Section 5.03 Procedure for Copy Charges

If an individual requests copies from any district office, it should first be determined if the request is for more than 50 pages. If more than 50 copies are needed, the requestor must be advised of the clerical labor charge of \$15.00 an hour with an additional overhead charge of 20%. See Statement of Charges (RMO-0019) in Attachment 1 of this guide.

In accordance with §70.9 Texas Administrative Code, the following tables present a few examples of the calculations of charges for information:

TABLE 1 (Fewer than 50 pages of paper records): \$.10 per copy x number of copies (standard-size paper copies); + Labor charge (if applicable); + Overhead charge (if applicable); + Document retrieval charge (if applicable); + Postage and shipping (if applicable) = \$ TOTAL CHARGE.

TABLE 2 (More than 50 pages of paper records or nonstandard copies): \$.10 per copy x number of copies (standard-size paper copies), or cost of nonstandard copy (e.g., diskette, oversized paper, etc.); + Labor charge (if applicable); + Overhead charge (if applicable); + Document retrieval charge (if applicable); + Actual cost of miscellaneous supplies (if applicable); + Postage and shipping (if applicable) = \$ TOTAL CHARGE.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

TABLE 3 (Information that Requires Programming or Manipulation of Data): Cost of copy (standard or nonstandard, whichever applies); + Labor charge; + Overhead charge; + Computer resource charge; + Programming time (if applicable); + Document retrieval charge (if applicable); + Actual cost of miscellaneous supplies (if applicable); + Postage and shipping (if applicable) = \$ TOTAL CHARGE.

TABLE 4 (Maps): Cost of paper (Cost of Roll/Avg. # of Maps); + Cost of Toner (Black or Color, # of Maps per Toner Cartridge); + Labor charge (if applicable); + Overhead charge (if applicable) + Plotter/Computer resource Charge; + Actual cost of miscellaneous supplies (if applicable); + Postage and shipping (if applicable) = \$ TOTAL CHARGE.

TABLE 5 (Photographs): Cost of Paper (Cost of Sheet of Photographic Paper/Avg. # of Photographs per Sheet); + Developing/Fixing Chemicals (if applicable); + Labor charge (if applicable); + Overhead charge (if applicable); + Postage and shipping (if applicable) = \$ TOTAL CHARGE.

Article VI. CORRESPONDENCE RECORDS

Section 6.01 Definition

Letters sent or received, internal memorandum, and email pertaining to district operations are all forms of correspondence designated as Local Government Records and are governed by the District's Records Control Schedules.

The "**Official Source Record**" is the actual copy of a document received by the District from an external source, or one source copy of a document created by a district officer or employee. Please note that there is **only one official source record** of any document. Additional copies are considered convenience copies and not governed by the control schedules.

Section 6.02 Classification and Retention

We must all be aware of the types of correspondence we create and receive. As governed by Local Schedule GR, correspondence falls into the following record series and groups:

Retention Note: The minimum retention period for correspondence or internal memoranda in categories (a) and (b) below directly linked to another record series or group...is that assigned to the other group or series. For example, a letter from an external auditor regarding an audit of a local government's financial records should be retained for the retention period given under record series number 1025-01(e); a letter concerning a worker's compensation claim should be retained for the period given under record series number 1050-32, etc. **THE RETENTION PERIODS THAT FOLLOW ARE FOR CORRESPONDENCE AND INTERNAL MEMORANDA THAT DO NOT READILY FALL WITHIN OTHER RECORD GROUPS.**

RECORD SERIES NO.: 1000-26

RECORD SERIES TITLE: CORRESPONDENCE AND INTERNAL MEMORANDA (includes incoming and copies of outgoing correspondence and internal correspondence and memoranda).

- a) **POLICY AND PROGRAM DEVELOPMENT** - Correspondence and internal memoranda pertaining to the formulation, planning, implementation, modification, or redefinition of the policies, programs, services, or projects of a local government. **RETENTION: 5 years.**

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

RETENTION NOTE: Review before disposal; some correspondence of this type may merit permanent retention for historical reasons. Historical value is determined by the Records Management/Public Information Officer; please forward these records to Records Management for classification.

- b) **ADMINISTRATIVE** - Correspondence and internal memoranda pertaining to or arising from the routine administration or operation of the policies, programs, services, and projects of a local government. **RETENTION: 2 years.**
- c) **ROUTINE** - Correspondence and internal memoranda such as letters of transmittal, requests for publications, internal meeting notices, and similar routine matters. **RETENTION: As Long as Administratively Valuable. (Exempt from destruction request requirement)**

Section 6.03 Management of Correspondence Records

The Official Source Copy of correspondence maintained according to state requirements must be filed in such a way that they are easy to locate if needed.

An "Official Source Copy" of *Policy and Program Development Correspondence* and *Administrative Correspondence* **kept in paper format** should be stored with other documentation of the policy, program, service, or project as its retention time will usually be the same as the record series for which it was created (i.e. staffing records, grant records, or audit records).

An "Official Source Copy" of *Policy and Program Development Correspondence* and *Administrative Correspondence* **kept in electronic format** should be filed in a directory dedicated to the policy, program, service, or project to which it pertains, so that there is no doubt as to the content of the correspondence and its retention time. This directory should be copied or retained on a District network drive to guarantee a back-up of the file is maintained. Additionally, the file name should include the FY, the project name, and the record series number (i.e. 08-09 Public Information Requests [GR 1000-34 and SD 3225-02]).

The Official Source Copy of Routine Correspondence may be stored as desired, but you are encouraged to store these documents in electronic form. We recommend you store routine correspondence no less than three (3) months, but no longer than one (1) school year, and then dispose of it by recycling or deleting the electronic copy. Again, if you use date, name, and use the record series to name electronic files, electronic filing becomes manageable.

Section 6.04 Email Correspondence

"Source document" means the local government record from which local government record data is obtained for electronic storage. The term does not include backup copies of the data in any media generated from electronic storage. **Local Government Code, §205.001.**

Effective 2009, email correspondence will be captured in a "blind file" accessible only by the Director of Technology and the Records Management/Public Information Officer in the event of a public information request, litigation, or disaster recovery. **This file is not a backup source for users**, but serves as a backup source for the District. Messages will be stored in accordance with the retention schedules, but for no longer than seven (7) years. If the District is required to produce information from this file, the file will be indexed and only those messages containing one or more keywords will be produced.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

If you have an email correspondence that is part of a record series with a retention period of more than five (5) years, you are required to print this email and file it with your file/project/official record. If the file/project/official record is kept electronically you should save the email to your directory file for retention.

You may wish to archive copies of email messages you send and receive for personal reference, but they are not the "Official Source Copy" and may be deleted according to personal preference. However, if the email related to a record series has a retention of more than five (5) years, you must print or retained the "Official Source Copy" with the related file (i.e. an email regarding a student is part of the student's educational record). If you need assistance filing or archiving email or backing up your data, please contact Network Services or Records Management.

Article VII. RECORDS EVALUATION AND VITAL RECORDS

Section 7.01 Record Evaluation

The inventory of records is necessary to identify, evaluate, and classify department and school records. Records inventory is the basis for supplementation to the Records Control Schedules, categorization of district records according to state record series numbers, and determining how long and in what manner records must be kept in active and inactive storage. Records Management will provide each department and school with a listing of identified record series in their department or school and the retention for each series. The Records Coordinator(s) will be responsible for coordinating a records inventory and disposal to be completed once every fiscal year and will be covered in detail in Section 15 of this guide.

The Records Coordinator(s) will be responsible for identifying new record series to the Records Management/Public Information Officer. For new record series complete a Records Inventory Worksheet (RMO-0017) and submit it to the Records Management/Public Information Officer.

Section 7.02 Records Appraisal

Records appraisal is the process of determining relative value of district records. The appraisal process determines which records have priority in creating backups, off-site storage, fireproof filing cabinets, etc. Records are appraised according to value and classification.

Section 7.03 Records Classification

Based on the outcome of inventory and appraisal, records are further classified as non-essential, useful, essential, and vital for management purposes. The following are appraisal classifications:

Definitions:

Administrative Value – means records with operational day-to-day value. When the transaction to which these records pertain is complete, their value is exhausted. Examples include: requests for publication, meeting notices, routine interdepartmental correspondence.

Organizational Value – means records with value to the organization's function. Examples include: organizational charts, procedure manuals, rules and regulations, operating instructions, delegation of authority, and records of the organization's historical functions.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Legal Value – means records containing information, which could protect or defend the district in litigation. Examples include: deeds, contracts, leases, fiscal records, claims, complaints, and grievances, etc.

Historical Value – means a record with research, historical, or archival value. Examples include: old handwritten ledgers, documentation of building or program dedications, historical surveys or studies, photographs, etc.

Section 7.04 Essential, Useful, and Non-Essential Records

Records that are not absolutely required to resume or continue the operation of the District are considered non-vital. The record class should be identified for each record series as one of the following:

Essential Records – are records that are retained for a specific period of time because they are necessary to conduct business.

Useful Records – are records that, if lost, would cause inconvenience.

Non-Essential Records – are records scheduled for routine destruction, as they have no predictable value to the District after their initial use.

Non-vital records are identified in the inventory and appraisal process by the Records Coordinator and/or the Records Management/Public Information Officer.

Non-vital records may be stored according to departmental or building policy, providing they are filed according to filing system standards outlined in Section 8 and 9 of this guide and their location is documented.

Each department and school should consider the importance of protecting the essential records in their building or department, whether by storage means or backup. Records Management will consult and/or assist in protecting essential records as needed.

Section 7.05 Vital Records

A vital record is any district record needed to resume or continue operations in the event of an emergency or disaster. All records required to recreate the District's legal and financial status, or to protect and fulfill the District's obligation to the people of the state are vital records. Vital records may exist in any media.

The length of time that a record is vital varies and may not be the same as its retention period. For example, accounts receivable records may be vital until payment is received, while a property deed may be vital as long as the property is owned.

Section 7.06 Identification of Vital Records

Identification of vital records is a part of the inventory process and takes into consideration the effects or consequences of lost information to the department, schools, and the public. General areas for consideration include:

- Financial Records – account receivable, loans and money transactions, general ledgers, registers, and other records proving payments
- Employee Records – payroll and benefits
- Insurance Policy Information
- Ownership Records – deeds, leases, titles, etc.
- Contracts & Agreements
- Student Cumulative Folders

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 7.07 Management of Vital Records

Active vital records, such as accounts payable and personnel records must be available for frequent reference. Active vital records will be stored in vaults, fireproof cabinets, locking cabinets, or in electronic format. In the case of low-volume vital records, such as insurance policies and contracts, Records Management must maintain a backup copy. These records will be kept in electronic format in FileBound with user permission granted only to those users with the proper security and/or need to know permission.

Inactive vital records may be stored electronically in FileBound for cost-effective purposes and protection.

Administrators will take all reasonable precautions to protect vital records in their care. The Records Management/Public Information Officer is responsible for the establishment of a vital records protection program. The Records Management/Public Information Officer will work in close cooperation with Records Coordinators, administrators, and the District's security supervisor to develop and enforce vital records management.

It is the responsibility of the Records Management/Public Information Officer to develop and distribute a Vital Records Master List. The Records Management/Public Information Officer will review the master list of Vital Records on an annual basis and revise it as necessary.

Section 7.08 Protection of Vital Records

Active vital records shall be given priority in the use of available on-site fire resistant cabinets, vaults, or file rooms specifically designed to protect records. Safeguarding records includes protecting them against the ordinary hazards of fire, water, mildew, light, dust, insects, rodents, acids, fumes, and excessive humidity. Vital records must be protected against human hazard such as theft, misplacement, and unauthorized access. Vital records must be protected from loss of legibility to the extent that the record's legality may be questioned. Although all hazards cannot be eliminated, the objective is to reduce them to an acceptable minimum.

Section 7.09 Methods of Vital Records Protection

Duplication: Records that are classified as vital and considered to be "single copy documents" should be sent to Records Management for electronic duplication and return of original.

Dispersal: Duplication copies of vital records (in any media) must not be stored solely in the same location as the original record.

Creation of vital records should allow for a duplicate copy at the time of creation, if possible. Duplicate copies should be forwarded to Records Management for dispersed storage. Records may be duplicated to different media or the same media; cost effective management will be the deciding factor. Vital records may be stored off-site only if kept in a bonded warehouse facility. Records Management must be notified before off-site storage is considered.

Section 7.10 Preservation of Records Relevant to Legal Matters

Any record that is relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action shall be retained at least until final resolution of the matter. In these circumstances, the Superintendent, Deputy Superintendent, or Records Management/Public Information Officer and General Counsel will notify relevant departments and work with staff to identify and preserve any records (including

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

electronic records) and other information that could be relevant to the matter. This will include a directive that the relevant department's normal document destruction policies or protocols temporarily be suspended. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated against their department promptly must notify the Office of the Superintendent, Deputy Superintendent, or Records Management/Public Information Officer who will contact General Counsel, so that all records with potential relevance to the investigation or legal proceeding can be preserved as necessary.

Section 7.11 Disaster Planning

The Records Management/Public Information Officer shall assist each department and school as needed in formulating a disaster recovery plan. Each department or school should have, and periodically test, a written disaster records recovery plan that includes: recovery procedures, disaster team listing, priority records recovery schedules, and recovery of computer applications documentation.

The Records Management/Public Information Officer shall review each disaster recovery plan upon creation and not less than once every two years.

Article VIII. ELECTRONIC RECORDS, FILING, AND STORAGE

Section 8.01 Record Types

The media of a record is unimportant when evaluating a record value, retention and protection.

Machine Readable Record – means a record in such a form that it can only be read, processed, stored, and retrieved by machine. **Example: Computer Generated Documents (Excel, etc.)**

Electronic Record – means a record copy of information stored or output as a machine-readable record. **Example: TIF or PDF files saved in FileBound**

Intermediate Files and Processing Files – mean temporary, machine-readable files used to create, correct, reorganize, update, or derive output from master data files. **Example: TEAMS**

Section 8.02 Standards

Tyler ISD has an obligation to provide accurate, reliable information to authorized recipients and to preserve vital records. Tyler ISD is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and on the computing and networking resources that store, process, and transmit this information. Records created and maintained in electronic form are included in the Institute's definition of archival materials.

All district records stored as machine-readable records must be retained for the same retention period as similar records in other media. All district records stored as machine-readable records must be created and maintained in compliance with Electronic Storage Standards set forth by the TSL in Local Government Code Chapter 205 and Texas Administrative Code Title 13, Chapter 7, §7.71 - §7.79. A complete copy of these standards is available from Records Management.

The Texas Administrative Code §7.75, Security of Electronic Records states: Local governments must implement and maintain an electronic records security program for office and storage areas that:

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

- (1) ensures that only authorized personnel have access to electronic records;
- (2) provides for backup and recovery of records to protect against information loss;
- (3) ensures that personnel are trained to safeguard confidential electronic records;
- (4) minimizes the risk of unauthorized alteration or erasure of electronic records; and
- (5) documents that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

Section 8.03 Preferences and Common Files Types

Rapid changes in technology mean that file formats can become obsolete quickly and cause problems for a records management strategy. A long-term view and careful planning can overcome this risk and ensure that the District can meet our legal and operational requirements.

Legally, our records must be trustworthy, complete, accessible, legally admissible in court, and durable for as long as our approved record retention schedules require. For example, we can convert a record to another, more durable format (e.g., from a nearly obsolete software program to a text file).

A non-proprietary image file header label must be used, or the system developer must provide a bridge to a non-proprietary image file header label, or the system developer must supply a detailed definition of image file header label structure. Texas Administrative Code §7.76.

Common File Formats

File Format Type	Common Formats	Sample Files	Description
Text	PDF, RTF, TXT, proprietary formats based on software (e.g., MS Word)	Letters, reports, memos, e-mail messages saved as text	Created or saved as text (may include graphics)
Vector graphics	DXF, EPS, CGM	Architectural plans, complex illustrations	Store the image as geometric shapes in a mathematical formula for undistorted scaling
Raster graphics	TIFF, BMP, GIF, JPEG	Web page graphics, simple illustrations, photographs	Store the image as a collection of pixels which cannot be scaled without distortion
Data file	Proprietary to software program	Human resources files, mailing lists	Created in database software programs
Spreadsheet file	Proprietary to software program, DIF	Financial analyses, statistical calculations	Store numerical values and calculations
Video and audio files	QuickTime, MPEG	Short video to be shown on a web site, recorded interview to be shared on CD-ROM	Contain moving images and sound
Markup languages	SGML, HTML, XML	Text and graphics to be displayed on a web site	Contain embedded instructions for displaying and understanding the



Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 8.04 Management

Individuals who manage or use the information and computing resources required by the District to carry out its duties must protect them from unauthorized modification, disclosure, and destruction. Information — including data and software — is to be protected, regardless of the form or medium that carries the information. Protection shall be commensurate with the risk of exposure and with the value of the information and of the computing resources.

Electronic or machine-readable records must be included in records management, appraisal, scheduling, and disposition procedures.

Equipment must always be available to interpret and read data stored in machine-readable records. Intermediate files are steps in the creation of records. Even in the absence of a final record copy, which formalizes the information, intermediate files are not records for the purpose of scheduling and disposition.

Destruction of computer output such as printout will be handled in the same way as paper records. Convenience copies of computer printouts that no longer have administrative value will be handled in the same way as paper duplicate records. The method of destruction for records that are maintained in machine-readable form only may be “erase and reuse.” Destruction of machine-readable records must follow the same authorization procedures as destruction of records in other media.

Section 8.05 Privacy of Electronic Communications

Federal laws protect the privacy of users of wire and electronic communications from illegal interception. Individuals who access electronic files or intercept network communications at Tyler ISD or elsewhere without appropriate authorization are in violation and may be subject to criminal penalties.

The law also regulates disclosure of information within an electronic mail system by providers of electronic mail services. Tyler ISD departments who are asked to disclose information from an individual's electronic files without the individual's authorization should seek guidance from the Director of Technology and/or the Records Management/Public Information Officer.

Article IX. ELECTRONIC IMAGE MANAGEMENT AND FILEBOUND

Section 9.01 Definition

Electronic Image Management (EIM) means recording, storage, retrieval, and transmittal of documents in digital form by electronic means. EIM is part of the Tyler ISD Records Management Program for these important reasons:

- EIM allows records to be stored using the District’s existing computer network resources instead of creating or maintaining paper records.
- Records stored using EIM techniques may be retrieved in a matter of seconds and may be forwarded or viewed without locating or moving the original record.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

- Copies of records stored using EIM may be printed or faxed within the District in minutes with minimal cost and no risk to the original record.
- Custom interfaces to EIM designed for different departments allow local users to access their records from their workstations.

Section 9.02 Standards

Hardware, software, and media used to store records using EIM and procedures to verify quality of EIM media must meet or exceed Electronic Storage Standards set forth by the TSL in Local Government Code Chapter 205 and Texas Administrative Code Title 13, §7.71 - §7.79. A complete copy of these standards is available from Records Management.

All district records stored using EIM must be retained for the same retention period as similar records in other media.

Section 9.03 Management

All EIM record storage and retrieval is under the direct supervision of the Director of Technology, who must work with the Records Management/Public Information Officer to ensure records compliance. EIM records must be included in records management, appraisal, scheduling, and disposition procedures. Equipment must always be available to interpret and read EIM records. EIM systems must use database security measures, such as password protection and limited access to ensure confidentiality of EIM records. EIM systems must store records in an appropriate format to prevent the alteration of permanent records.

The use of EIM systems will be subject to regular review by the Records Management/Public Information Officer as to cost-effectiveness and administrative efficiency of the system. As EIM technology develops, organization managers are encouraged to consider application of EIM systems for their departments for increase record-keeping and workflow efficiency.

Section 9.04 FileBound – Content Management Program

Documents and information drive a school district, and our long-term success is dependent upon our ability to control, manage, and distribute them. Without the right solution it's very difficult to make informed decisions, profitably process transactions, maintain regulatory compliance, and successfully manage growth. FileBound is an affordable web-based Content Management Solution that addresses these issues.

Document Imaging - FileBound provides document scanning, importing and retrieval functionality.

Digital File Imaging - FileBound delivers the functionality to automate the importing and indexing of digital files from any source.

Physical File and Box Tracking - FileBound provides the ability to manage access and control of your paper files and archival box storage.

The use of Filebound will be subject to regular review by the Records Management/Public Information Officer as to cost-effectiveness and administrative efficiency of the system

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Article X. MICROGRAPHICS

The media of a record is unimportant when evaluating a record value, retention and protection. The purpose of this section is to create an awareness of record qualities that are unique to micrographic records.

Section 10.01 Definitions

Micrographics means microfilm, microfiche, computer output microfilm (COM) and computer-aided retrieval (CAR) of microfilm images.

Reader means any device that allows viewing and/or printing of micrographic images.

Section 10.02 Standards

All micrographics of records will be subject to the approval of the Records Management/Public Information Officer and in accordance with Local Government Records Act §204 and Texas Administrative Code, Title 13, Chapter 7, or minimum procedures and standards authorized by the American National Standards Institute (ANSI) and the Association for Information and Image Management (AIIM).

Section 10.03 Management

All microfilming is under the control of the Records Management/Public Information Officer. Records Management must approve record conversion before a purchase order will be issued for micrographic services. All original microfilm will be stored by Records Management.

As long as micrographic records exist, a reader must always be available to view records and will be maintained by Records Management.

District use of micrographics is subject to periodic review by the Records Management/Public Information Officer as to cost-effectiveness, administrative efficiency, and compliance with commission rules.

Article XI. FILING STANDARDS AND FORMS CONTROL

Section 11.01 Filing Systems

A filing system is any structured system designed to facilitate the retrieval of information. Standardized filing systems are part of the Tyler ISD Records Management Program for these important reasons:

- District records are stored using filing systems; the person who filed a record will not always be available to retrieve it.
- Well-planned, well-organized filing systems save time and money in filing and retrieving information.
- Standardized filing of similar records throughout the district means consistent, timely response to employees and the public, a shorter learning curve for substitutes and transferring employees and fewer lost or misplaced documents and files.
- Standardized filing of electronic records improves data backup protection and simplifies data retrieval.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Tyler ISD filing systems will use recognized alphabetic and numeric filing standards. Records filed alphabetically will have visibly posted rules for filing. Record Management is available to assist in posting such rules for filing.

FileBound can be used to track files and file boxes. Records Management oversees FileBound and will assist in setting up projects for tracking files. Contact the Records Management/Public Information Officer to discuss tracking projects in FileBound.

Section 11.02 Filing Training and Audits

Records Management may require training regarding filing systems for clerical staff and employees that handle various records. Records Management may audit the filing systems at any department or school and make recommendations to the principals, department head, or the Superintendent.

Section 11.03 Definition of Forms Control

A form is any tool designed to communicate data or information in a consistent, pre-formatted, organized manner. This definition includes paper forms filled out by hand or using a computer, as well as online templates.

Section 11.04 Overview of Forms Control

Forms control and management is part of the District's Records Management Program for these important reasons:

- Many of the District's records are created using forms.
- Lack of a formal forms policy has resulted in duplicate outdated forms in use throughout the District.
- Personal computers allow official-looking forms to be created with ease.
- Forms must be designated for efficient transmission over the District's computer network.
- Many forms, including transcript request and consent forms, contain information which is governed by state and federal law. The approval of general counsel may be necessary on particular forms.

The objectives of forms control and management are:

- All forms meet design standards.
- Only needed forms, utilizing only needed information, are approved.
- All externally used forms maintain the District's image.
- Forms are designed to achieve the most efficient image.
- Forms are printed, distributed, replenished, and destroyed in the most economical manner.

Section 11.05 Forms Approval and Management

Each request for a new or revised form should be channeled through department or school management for approval, then to Records Management for review and form number assignment. Records Management's role is to ensure operating efficiency, not to dictate work methods to departments. Each department using forms must be aware of work processes dictated by existing forms and evaluate form redesign as a method to improve operating efficiency.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

The Records Management/Public Information Officer will review and revise District forms as necessary. Employees are encouraged to bring difficulties with current forms to the attention of Records Management.

Records Management will assign a form number, date of creation or revision, and state retention series number and retention period. The series number links the form to its function. The form number and date indicate that the form has been authorized.

Records Coordinators in each department and school are responsible to monitor forms in use, relay forms ideas and requests to department or school management and the Records Management/Public Information Officer, and purge obsolete forms.

Newly released and revised forms shall be distributed by the department or school management or the Records Management/Public Information Officer with any information or instructions, which cannot be printed on the form.

Article XII. RECORDS CONTROL AND DESTRUCTION

Section 12.01 Definition and Purpose

Destroying obsolete records in accordance with our record control schedules saves money, computer space, and office space and is a form of risk management.

Misplaced or lost files are perhaps the most significant of all costs associated with records management. Controlling and tracking files allows an employee to locate any item quickly and precisely no matter where in the office it is located. The result is increased worker productivity and efficiency, allowing personnel to utilize their time in more effective ways.

Records Destruction – means the destruction of records in accordance with the Tyler ISD Records Control Schedules and procedures in this guide. Under no circumstance are any district records to be destroyed without the specific authorization of Records Management.

Unauthorized destruction of Local Government Records may be a Class A misdemeanor, punishable by a fine of \$25 - \$4,000 and confinement in the county jail for three (3) days to six (6) months.

Reasons for record destruction include:

- Efficient use of space and cost-savings.
- Protection from high administrative cost in litigation support.
- Risk management.

Section 12.02 Standards

The Local Government Code limits record destruction to the following methods: burning, shredding, pulping, and burial in a landfill or by sale or donation for recycling purposes, unless such records are protected (closed) under Local Government Code Chapter 552, Public Information.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 12.03 Disposal and Destruction of Records

If you have determined that, consistent with the District's Records Management Procedures, and with the records management practices and procedures applicable to your department, it is appropriate to dispose of any records, they can be destroyed in one of the following ways:

1. Recycle non-confidential paper records;
2. Shred or otherwise render unreadable confidential paper records; or
3. Erase or destroy electronically stored data. (The Technology Service Center can assist you in effectively disposing of this data.)

Shredding is the recommended disposal of records protected or closed under Chapter 552 or FERPA. The method of disclosure must be approved by the Records Management/Public Information Officer. We are required by the Local Government Record Act to retain certain records and these records need to be properly stored, tracked, purged, retained, and preserved.

Section 12.04 Keeping Control of Records

The records inventory is necessary to identify, evaluate, classify, and control department and school records. The Records Coordinator(s) at each department and school will conduct a completed itemized inventory. Records Management will assist with department and school inventories as needed. **Repeat the below 7 inventory steps at least once each fiscal year.** The following seven (7) steps will assist the Records Coordinators in their records inventory.

1. Utilize the following resources when reviewing records for the inventory to determine disposal and archival (storage) of records:
 - a. Records Retention Schedule(s) or Tyler ISD Inventory Sheet.
 - b. Records Management Office and Forms.
2. Inventory your records to determine records that have met their retention or records with permanent retention that are ready for electronic storage.
3. Prepare a **Records Disposal Approval Form (RMO-0006) for each record series** that has met its retention and submit for approval to Records Management.

****All convenience (duplicate/non-official) copies may be disposed of "after obsolete, superseded, or administrative value is lost" without documenting the disposal. If the "Official Source Record" has met its retention period, make sure to dispose of all convenience copies.**

If you have a need to retain an Official Source Record or a Convenience Copy beyond the retention period, submit notice to the Records Management/Public Information Officer.

4. Upon receipt of an approved Disposition Approval Form, properly dispose of approved records.

****If you are notified of active or pending litigation or an audit relating to your records, all disposals must be "stopped" until the litigation/audit is complete, submit notice to the Records Management/Public Information Officer.**

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

5. Complete a **Disposition Log** (RMO-0005) for all "Official Source Record" documents disposed of, have it signed-off by your principal/department head, and submit it to Records Management with the completed Disposition Approval Form. If you use a vendor to dispose of records, you must obtain a **Certificate of Destruction from Disposal Vendor** (RMO-0014), which should be attached to your Disposition Log.
6. Box up records that are not eligible for disposal, but are not used enough to remain in your "active office files." Provide Records Management with a Records Box Label (RMO-0018a) for all record series to be stored. Records Management will provide the completed Labels to be placed on and in the storage box as shown on the Storage Box Preparation Example Sheet.

**Use file storage boxes only (not copier paper boxes).
7. Complete a **Transfer of Inactive Permanent Records to Electronic Format Form** (RMO-0018) for all records submitted for electronic storage, and submit it to Records Management.

Section 12.05 Archival of Records

Recognizing the need to ensure the preservation and availability of the official records of the District for historical purposes, the following archival procedures have been established.

All records generated or received by the various administrative and academic offices of the District in the conduct of their business, regardless of the form in which they are created and maintained, are the property of the District and constitute archival material. The records covered by this procedure include official printed material, correspondence, machine-readable files, record books, minutes, committee files, financial records, and associated papers.

All administrative officers of the District, as well as those members of the faculty who, by virtue of administrative responsibilities either of a continuing or occasional nature, possess files, records, or documents relating to their official duties, are requested to observe the following:

1. Archival material in district offices may not be destroyed or placed in storage without the approval of the Records Management/Public Information Officer.
2. Material so selected for preservation shall be sent to the Records Management/Public Information Officer and/or campus librarian upon approval of the Records Management/Public Information Officer.
3. The officer in charge of each administrative or academic office, in consultation with the Records Management/Public Information Officer, will be responsible for deciding how long inactive papers are to be retained in and under the direct control of the office concerned.
4. All photographs, other visual material, and artifacts significant to the District's history shall be sent to Records Management for determination of retention method.

The District would also welcome the offer of privately owned material bearing on the history of the District, provided, however, that the District incurs no obligation to retain such material as an integrated collection or in any prescribed form.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Section 12.06 Management of Student Records

Records Management maintains and tracks student records in accordance with the retention schedules once a student has withdrawn or graduated. See the District-Wide Procedures for Transferring Student Records (RMO-0022a) and Records Round-Up (Withdrawn Student Records) (RMO-0022). Elementary and Middle School campuses only retain the current year withdrawal records and forward these records to Records Management pursuant to the Round-Up Procedures. High Schools retain two (2) school years of withdrawal records and current year and previous year graduate records, prior to following the Round-Up Procedures.

The Records Coordinator is responsible for scheduling the yearly inventory and disposal of records. Records Management will assist in scheduling disposal of district records that have reached their retention. Records Management will assist in destroying confidential records as needed.

Unscheduled records may not be destroyed without the specific prior approval of the TSL. The Records Management/Public Information Officer is responsible to request permission to destroy unscheduled records for all department and schools.

Article XIII. CENTRAL AND OFF-SITE RECORDS STORAGE

Section 13.01 Responsibility

Transfer of non-current records and records with low to moderate retrieval rates to a central or off-site records storage location is a sound alternative to the purchase of more storage cabinets and more office space.

Records Management will coordinate the storage and retrieval of all records stored centrally or off-site. Any central or off-site records storage facility will be designed to facilitate rapid retrieval of records stored in these locations. All records stored centrally or off-site will be tracked in FileBound for ease of retrieval.

Section 13.02 Procedures

Records with a permanent retention or retention over ten (10) years should not be stored centrally or off-site. See procedures for in Section 12 of this guide, 12.2 Clean Out and Get Control of Department/School Records, number 6. Records classified as essential or vital records should not be stored centrally or off-site, contact Records Management regarding electronic storage of records (see number 7, Section 12.2).

Article XIV. PRIVACY AND IDENTITY PROTECTION

Section 14.01 Purpose

Tyler Independent School District has implemented a comprehensive Identity Theft Program pursuant to The Fair and Accurate Credit Transactions Act (herein referred to as FACTA) and the FACTA Disposal Rule and established this guide to protect employees, students, contractors/vendors, and the District from damages related to loss or misuse of sensitive and/or confidential information. Sensitive and/or Confidential Information requires the highest level of protection. This information should be treated very carefully and should never be left open to attack (i.e. left on a traveling laptop or left unencrypted). This guide will:

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

-
- Define sensitive information;
 - Describe the physical security of data when it is printed on paper; and
 - Describe the electronic security of data when stored and distributed.

Section 14.02 Scope

This guide applies to employees, contractors/vendors, consultants, temporaries, volunteers, and other workers or agents of the District, including all personnel affiliated with third parties. District personnel are encouraged to use common sense judgment in securing the District's confidential information to the proper extent. If an employee or agent of the District is uncertain of the sensitivity of a particular piece of information, the employee/agent should contact their supervisor or the Records Management/Public Information Officer.

Section 14.03 Sensitive and/or Confidential Information

Many records subject to record retention requirements contain non-public confidential data. Such records are protected by federal, state and local statutes, including the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). In addition to the statutory requirements, any record that contains confidential data should be treated in accordance with the District's privacy and

security policies (see the this Article XIV Privacy and Identity Protection, Section 3.03 Privacy and Student Information, and Tyler ISD's Identity Theft Program).

Personal Information - pertains to any and all sensitive information about students, parents or legal guardians, contractors/vendors, employees, or any other entity doing business with or for the district. Good examples include: financial information, social security numbers, student records, and passwords. Here is a quick list of the most sensitive confidential data:

- Social Security Number
- Business Identification Number
- Employer Identification Number
- Income Tax Records
- Date of Birth
- Financial Information
- Place of Birth
- Drivers License Numbers
- Credit Card Numbers and Information
- Bank Account Numbers
- Personal Address
- Payroll Information
- Insurance Information and Benefit Plan Paperwork (ie. Cafeteria Plan)

District Information – pertains to any and all sensitive information about the District, and third-party companies, vendors, suppliers, contractors pertaining to privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it. Information that is not public knowledge conveyed to an external party due to its position in the procurement process. The District is generally duty bound to desist from making unauthorized use of the proprietary information. Here is a quick list of the most sensitive proprietary data:

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

-
- Business Methods
 - Test Results
 - Trade Secrets
 - Customer Utilization Information
 - Retention Information
 - Marketing and other Company Strategy
 - Computer Codes
 - Screens
 - Forms
 - Sales associates or suppliers or any other non-public information

Section 14.04 Protection of Hard Copy Distribution

Every employee and agent performing work for the District will comply with the following:

1. Keep offices and storage rooms containing identifying information secure.
2. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use and/or supervised.
3. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday.
4. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
5. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
6. Require and keep only necessary identifying information for District purposes.
7. Assign and use identification numbers instead of using social security numbers, when possible, or only use last four numbers of social security number, if possible.
8. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut shredding machine.
9. Ensure complete and secure destruction of paper documents and computer files containing identifying information.

Section 14.05 Protection of Electronic Distribution

Every employee and agent performing work for the District will comply with the following:

1. Internally, sensitive information may be transmitted using approved District email. Remember to be careful with your email, emails are open to public information requests and student records requests. Be professional!
2. Any sensitive information sent external must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in your email signature block:

Confidentiality Notice: This email message, including all attachments, is for the sole use of the intended recipient(s) and may contain confidential student information. Unauthorized use or disclosure is prohibited under the Family Education Rights & Privacy Act (20 U.S.C. §1232g; 34 CFR Part 99). If you are not the intended recipient, you may not use, disclose, copy or

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

disseminate this information. Please contact the sender by reply email immediately and destroy all copies of the original message, including attachments.

or

Confidential Notice: This message may contain confidential and/or proprietary information protected by law, and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited.

3. Ensure that office computers are password protected and that computer screens lock after a set period of time.
4. Ensure that reporting procedures for lost, stolen, or compromised laptops and computers are followed by District personnel.
5. Ensure that identifying information is primarily stored on District shared network drives or encrypted external drives and not on laptop hard drives, when possible.
6. If identifying is saved in hard drives or external drives (i.e. thumb drives or CD) and this information is lost, stolen, or compromised that the user can provide an exact replication of the compromised information to provide to the Compliance Officer.
7. Ensure that computer virus protection is up-to-date.
8. Ensure District websites are secure or provide clear notice that the website is not secure.
9. Ensure computer networks are secure and firewall protection is up-to-date.

Section 14.06 Breach of Sensitive and/or Confidential Information

In the event District personnel become aware or detect a breach of information, such personnel shall take one or more of the following steps, depending on the degree of risk posed:

1. Continue to monitor for evidence of Identity Theft;
2. If possible, contact the person whose identifying information is in question;
3. Change any passwords or other security devices that permit access;
4. Notify the Director of Technology Services or Compliance Officer regarding lost, stolen, or compromised laptop or computer;
5. Notify the Compliance Officer for determination of the appropriate step(s) to take; and
6. Notify Tyler ISD Police Department.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

Article XV. GLOSSARY

Active Records	Records that are used three or more times in a month and are stored in very accessible equipment in the office.
Administrative Record	A local government records not related to an individual student.
Administrative Value	Operational day-to-day value.
AIIM	Association for Information and Image Management. Trade association and professional society for the micrographics, optical disk, and electronic image management markets.
ANSI	American National Standards Institute. A standards-setting, non-government organization, which develops and publishes standards for "voluntary" use in the United States.
Basic Enrollment Information	Current or previous campus, graduation or withdrawal date, and health record verification.
Closed Record	A local government record which may not be released to the public under the Texas Open Records Act.
Computer Back-up	The process of creating a secondary copy of data for the purpose of disaster recovery, i.e., being able to recover or restore the data should an unplanned event make the primary data inaccessible. Backups are a daily and weekly snapshot of data as it existed at a specific point in time. Periodic backup media are typically retained for a short time (e.g. 30 to 90 days) and then recycled into the backup process and overwritten.
Convenience Copy	Copy or copies of a document or file created and maintained for ease of access and reference. A convenience copy is never a record copy, although it may be an audit copy. Convenience copies are frequently encountered in reader files.
Correspondence	Correspondence in any form received or created by a District employee in the normal course of district business.
Department	Any department, organization, or staff devoted to a particular district project that generates records.
Direct Access Filing	A system in which a person can locate a particular record by going directly to the files and looking under the given name of the record.
Directory Information	Student information, which under normal circumstances, would not be harmful, or an invasion of privacy if disclosed. Tyler ISD defines directory information as: student's name, address, telephone number, photograph, date and place of birth, dates of attendance, grade level, and participation in officially recognized activities and sports, weight and height of members of athletic teams, honors and awards received, the most recent school attended.
Disaster Recovery Plan	A written, approved, implemented, and periodically-tested program to reconstruct and/or salvage an organization's vital and historical records and to establish procedures for the immediate resumption of business operations in the event of a disaster.

Disclosure	Release of information in any format.
Education Records	Those records directly related to a student and maintained by an educational agency.
EIM	Recording, storage, retrieval, and transmittal of documents in digital form by electronic means.
Electronic Archiving	The process of moving selected data to separate storage for the express purpose of retaining it as a record for a specified period of time based on legal, regulatory, or business requirements. Archived data is not allowed to be updated, overwritten, or erased for the specified retention period.
Electronic Record	Record data stored in electronic format.
Electronic Records System	Any information system that produces, manipulates, and stores records using a computer.
Electronic Storage	The maintenance of record data in the form of digital electronic signals on a computer hard disk, magnetic tape, optical disk, or similar machine-readable medium.
Electronic Vaulting	Transferring data records online to a remote backup location.
Eligible Student	A student eligible to access their own student records: age 18 or attending a post-secondary institution.
Enrollment Card	The annual enrollment form establishing residency and parent information.
Essential Record	Any local government record necessary to the resumption of continuation of government operations in an emergency or disaster, to the re-creation of the legal and financial status of the government, or the protection and fulfillment of obligations to the people of the state. LGC §201.003(5).
FERPA	Family Educational Rights Privacy Act, Appendix I.
File Audit	An examination and verification of a specific activity.
Filing	The process of arranging and sorting records so that they may be filed and retrieved efficiently.
Filing System	The planned method of classifying and arranging records for storage and retrieval.
GSC	General Services Commission
Historical Value	Research, historical, or archival value.
Index List	A list in any media, which identifies micrographic images for the purpose of locating and retrieving them.
Intermediate File	A temporary file created on a computer, which precedes a record. Intermediate files are not records for purposes of public information or retention.
Legal Value	Containing information, which could protect or defend the District in litigation.
LGRA	Local Government Records Act
Local Government Record	Any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under laws of the state, created or received by a local government or any of its officers or employees pursuant to law, including an ordinance, employees pursuant to law, including an ordinance, or in the transaction of public business. LGC §201.003(8).
Machine Readable Record	A record that can be read, processed, stored, and retrieved by a machine.
Managing Conservator	The custodial parent.
Master Copy	The original or source record copy of the record. The record copy is the copy, which must be maintained according to the records control schedule.

Micrographics	Microfilm, microfiche, computer output microfilm (COM) and computer-aided retrieval (CAR) of microfilm images.
Mitigation	Actions taken to either prevent loss or minimize the consequences of a potentially harmful event.
Non-Essential Record	A record with no predictable value.
Obsolete Record	A record series, which is no longer being created.
Official Source Record Copy	The actual copy of a document received by the District from an external source, or one source copy of correspondence created by a district officer or employee. Please note that there is only one official source record of any document. Additional copies are considered convenience copies and not governed by the control schedules.
Office of Record	The office in which a record is originally created, received, or stored.
Open Record	A record, which is open for public access under Section 552. Same as Public Information.
Open Records Request	A request for information in any format that is not part of student education records. Same as Public Information Request.
Organization Manager	Any department head, principal, organization leader, or program leader responsible to document the function of his or her organization.
Organizational Value	Functional value to the organization, including organizational charts, policy and procedure manuals, operating instructions, etc.
Parent	The natural parent, guardian, or person acting in the capacity of parent for a Tyler ISD student.
Permanent Record	A record with a permanent retention period according to the records control schedules.
Personally Identifiable Information	Information, which would personally identify the student. This includes the student's name, address, telephone number, social security number, student identification number, and names of parents or other family members. Personally identifiable information must not be released without the prior consent of the parent, guardian, or adult student.
Possessory Conservator	The non-custodial parent, whose rights of access to a student or the student's education records are defined in the custody document or other court order.
Prevention Plan	A common sense approach to disaster minimization and/or avoidance in the workplace.
Privacy	Parental option to prevent any release of student directory information, except in case of emergency or as provided in Article III of this manual.
Privacy Flag	The data flag on a RIMS file indicating parents have elected privacy of directory information.
Processing File	A temporary file created on a computer, which precedes a record. Processing files are not records for purposes of public information or retention.
Protected Record	A local government records which may not be released to the public under the Texas Open Records Act.
Public Information	Any information in the custody or care of a local government which may be released to a member of the public. Same as Open Record.
Public Information Request	A request from a member of the public for any information, which does not pertain to an individual student. Same as Open Records Request.
Reader	Any device that allows viewing and/or printing of micrographic images.
Readily Available	A record which already exists in a format which does not cause the District to incur additional labor or expense in making it available to the public.
Reading File	A chronological file containing one copy of each letter or memorandum sent.
Record	Any information in any media created or received in connection with

	the transaction of district business.
Record Copy	The official copy of a particular record. The record copy may be an original or duplicate.
Record Series	A group of records, related in form or content, which is arranged under a single filing system or kept together as a unit.
Records Control Schedule	The state mandated schedule of records maintained by the District and their minimum legal retention periods.
Records Coordinator	The on-site liaison for the records management program.
Records Inventory	The inventory of record series maintained by the District.
Records Management	Applying management techniques to the creation, use, maintenance, retention, preservation, and disposal of records.
Records Management/Public Information Officer	The district employee with ultimate responsibility for the records management program and state Records Control Schedules.
Retention Period	The minimum time a record must be maintained based on administrative, legal, fiscal, and historical requirements, and published in the Records Control Schedules.
Section 552	The Section of the Local Government Code, which governs release of public information. Copies of this section are available from Records Management.
Source Document	The original records from which a copy is created.
Student Education Record	Those records directly related to a student and maintained by an educational agency.
Student ID Number	All information gathered and created by the District regarding an individual student.
Student Information	All information gathered and created by the District regarding an individual student.
TORA	Texas Open Records Act, now recodified as Section 552 of the Local Government Code.
Useful Record	A record that, if lost, would cause inconvenience.
Vital Record	Any district record needed to resume or continue operations in the event of an emergency or disaster. Same as Essential Record.
Working Title	The name commonly used for a record.