INFORMATION SECURITY

District Information Resources are some of the most valuable assets owned by a District. A District produces, collects, and uses many different types of data/information in fulfilling its mission. Laws and Board of Education policy mandate confidentiality and protection of certain types of data/information. District data/information shall be classified as Confidential, Controlled, or Published. Data/information will be considered Controlled until identified otherwise.

This procedure will help Fitzgerald Public School employees to classify any data/information created, stored or transmitted by the District for the purposes of determining the level of protection required and applicable policies and laws.

This procedure applies to all types of data/information:

A. Electronic data/information.

B. Data/information recorded on paper.

C. Data/information shared orally, visually, or by other means.

For purposes of this procedure, "Published Data/Information" means data/information made available to the public through posting to public websites, or distribution through e-mail, social media, print publications, or other media. This includes data/information that can be disclosed without restriction, such as unrestricted directory information, District maps, syllabi and course materials, and meeting minutes.

"Controlled Data/Information" means data/information that is not generally created or made available for public consumption, but may be subject to release through a public records request or pursuant to another State or Federal law. This includes operational/business records, select personnel information (e.g., employees' salaries), District expenditures, and internal communications that do not contain Confidential Data/Information.

"Confidential Data/Information" means data/information that is exempt or must be protected from unauthorized disclosure or public release based on State and/or Federal laws or regulations or applicable legal agreements. This includes "protected health information" covered by HIPAA, student records as defined by FERPA and State law, Social Security numbers, credit/debit card information, security records, personal employee information, critical infrastructure information (e.g., physical plant detail, IT systems information, system passwords, security plans, etc.) and documents protected by attorney-client privilege.

Below is a summary of the minimum standard protection requirements for each category of data/information when being used or handled in a specific context (e.g., Confidential Data/Information sent in an e-mail message). These protection standards are not intended to supersede any regulatory or contractual requirements for handling data/information. Some specific data/information sets, such as student records data/information, credit/debit card data/information, healthcare data/information, and financial accounting data/information may have stricter requirements in addition to the minimum standard requirements listed below.

Published Data/Information:

When it comes to Published Data/Information, there are no protection requirements when it comes to:

A. collecting/using it;

B. granting access or sharing it, including disclosing it, publicly posting it, or electronically displaying it;

C. exchanging it with third parties, services providers, cloud services, etc.;

D. storing it on removable media (e.g., thumb drives, CDs, tapes, etc.);

E. electronically transmitting it, including e-mailing it or sending it via other electronic messaging services/platforms;

F. printing, mailing or faxing it; and

G. disposing of it (subject to the District's record retention policy, a litigation hold, and administrative guidelines).

With respect to public records requests, Published Data/Information can be readily provided upon request; however, individuals who receive a request must coordinate with District administration before providing the information.

When Published Data/Information is stored or processed in a server environment, and the server is connected to the District's network, the server must comply with Minimum Security Standards for Networked Devices.

When Published Data/Information is stored or processed in an endpoint environment (e.g., laptop, smartphone, desktop computer, tablet, etc.), the endpoint device if connected to the District's network must comply with Minimum Security Standards for Networked Devices.

Controlled Data/Information:

When it comes to Controlled Data/Information, there are no protection requirements when it comes to:

A. collecting or using it;

B. storing it on removable media (e.g., thumb drives, CDs, tapes, etc.)

C. electronically transmitting it, including e-mailing it or sending it via other electronic messaging services/platforms, except reasonable methods shall be used to ensure Controlled Data/Information is only included in messages to authorized individuals or individuals with legitimate need to know;

D. disposing of it (subject to the District's record retention policy, a litigation hold, and administrative guidelines).

When it comes to Controlled Data/Information, reasonable methods must be used to ensure only authorized individuals or individuals with a legitimate need-to-know access or shared it. Further, reasonable methods must be used to ensure Controlled Data/Information is only disclosed or electronically displayed to authorized individuals or individuals with legitimate need-to-know.

When it comes to storing, transmitting and retrieving Controlled Data/Information with or utilizing third party service providers, cloud services, etc., reasonable methods must be used to ensure the third parties' responsibilities for confidentiality/privacy of the data/information are defined and documented.

Printed materials, including those being mailed or faxed, that contain Controlled Data/Information must be distributed or made available only to authorized individuals or individuals with legitimate need-to-know.

Individuals who receive public records requests involving Controlled Data/Information must coordinate with District administration before providing the requested data/information.

When Controlled Data/Information is stored or processed in a server environment, and the server is connected to the District's network, the server must comply with Minimum Security Standards for Networked Devices.

When Controlled Data/Information is stored or processed in an endpoint environment (e.g., laptop, smartphone, desktop computer, tablet, etc.), the endpoint device if connected to the District's network must comply with Minimum Security Standards for Networked Devices.

Confidential Data/Information:

When it comes to Confidential Data/Information, its collection and use is limited to authorized purposes as outlined in the District's privacy policy. Departments or schools that collect and/or use Confidential Data/Information must use District-provided or approved servers, devices, systems and/or processes to handle this type of data/information.

If feasible, District web pages that are used to collect Confidential Data/Information will include a link to the District's privacy policy.

Social Security numbers (SSNs) shall not be used to identify members of the District's community if there are reasonable alternatives. SSNs shall not be used as username or password.

When it comes to Confidential Data/Information, access shall be limited to authorized School District officials or agents with a legitimate academic or business interest and a need-to-know as outlined in the Board's privacy policy. All access shall be approved by an appropriate administrator and tracked in a manner that can be audited. Before granting access to or exchanging Confidential Data/Information with third parties, service providers, cloud services, etc., contractual agreements that outline security responsibilities shall be in place and approved by the Board's legal counsel.

Confidential Data/Information may not be disclosed without appropriate consent or unless required by law. Confidential Data/Information shall not be posted publicly; directory information, however, can be disclosed without consent, unless a student/parent opts out of the directory information disclosure.

Confidential Data/Information shall be displayed only to authorized and authenticated users of the District system, and, where possible, identifying numbers or account numbers shall be, at least partially, masked or redacted.

Confidential Data/Information is typically not subject to release pursuant to a public records request. However, some public records requests may be fulfilled by redacting Confidential Data/Information in the record. Individuals who receive such requests must coordinate with District administration before responding to the request.

When Confidential Data/Information is stored or processed in a server environment, the server must comply with Minimum Security Standards for Confidential Devices.

When Confidential Data/Information is stored or processed in an endpoint environment (e.g., laptop, smartphone, desktop computer, tablet, etc.), the endpoint device if connected to the District's network must comply with Minimum Security Standards for Networked Devices.

Storing credit/debit card data/information on servers or endpoint devices is not permitted.

Storing Confidential Data/Information on personal communication devices is not permitted, unless expressly authorized by the Superintendent and stored in an encrypted file format and the device automatically secure locks when not in use.

Unless expressly authorized by the Superintendent, Confidential Data/Information shall not be stored on removable media (e.g., thumb drives, CDs, tapes, etc.). It is to be stored in an encrypted file format or within an encrypted volume, and media is to be stored in a physically secure environment, and the media is owned by the District.

Confidential Data/Information may only be electronically transmitted if it is in an encrypted file format or over a secure protocol or secure, authenticated connection. Confidential Data/Information may only be transmitted via e-mail or other electronic messaging service/platform if the data/information is contained within an encrypted/password protected file attachment. Such messages may only be sent to authorized individuals or other individuals with a legitimate need-to-know.

Printed materials, including those being mailed or faxed, that contain Confidential Data/Information must be distributed or made available only to authorized individuals or individuals with legitimate need-to-know. Access to any area where printed records containing Confidential Data/Information are stored shall be limited by use of controls (e.g., locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.

SSNs shall not be printed on any card required to access services.

When ready for disposal, Confidential Data/Information shall be deleted and unrecoverable. Physical media (e.g., paper, CDs, tapes, etc.) should be destroyed so that Confidential Data/Information on the media cannot be recovered or reconstructed. All disposals must be consistent with State law.

The following are required:

A. enforcement of this procedure throughout the District;

B. a periodic assessment of risk on the procedure;

C. training about classification, retention, access and security of all District data/information;

D. internal controls related to classification, retention, access and security of all District data/information;

E. developing procedures for dealing with unauthorized release of District Confidential Data/Information (See AG 8305C).

Each District department is responsible for implementing, reviewing and monitoring internal policies, practices, etc., to assure compliance with this procedure.

All procedures shall be consistent with public records laws and records retention plans and schedules as required by State and Federal laws and regulations.

Noncompliance with these standards may incur the same types of disciplinary measures and consequences as violations of other Board policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation, or referral to law enforcement.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the District's business network, disabled, etc., as appropriate until the device can comply with this standard.

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, contact the District's Director of Information Technology.

Adopted: 12/07/20