DISD provides and maintains an information technology infrastructure that promotes teaching, learning and the administration of DISD. Access to and use of DISD information technology (DISD IT) resources imposes certain responsibilities on users, in accordance with existing DISD policies and local, state and federal law. This Data: Acceptable Use, Protection and Privacy Policy (Data Policy) provides information to students, faculty and staff about the lawful and appropriate use of DISD IT resources, including computers, printers, networks, and related equipment, software, and data files that are owned and/or managed by DISD or wireless networks. To help ensure that these resources are used appropriately, this Data Policy provides guidelines for the appropriate use of DISD IT resources as well as for DISD's access to information about and oversight of these resources, data retention, data privacy protection methods, and disciplinary measures for violation of the Data Policy. This Data Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT resources;
- To ensure that use of DISD IT resources is consistent with the principles and values that govern use of other DISD facilities and services;
- To ensure that DISD IT resources are used for intended purposes;
- How DISD data is managed, protected, stored, and disposed;
- Implementation of data privacy compliance; and
- To establish processes for addressing policy violations and sanctions for violators.

Appropriate Use

The appropriate use of IT resources should always be ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to freedom from intimidation, harassment, or unwarranted annoyance. Appropriate use of DISD IT resources included instruction, study, research, communication, and official work of DISD.

When using DISD IT resources, you must:

- Comply with all federal, state and other applicable laws; all generally applicable DISD rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "Cracking", and similar activities; the *DISD Copyright and File Sharing Policy*; the *DISD Sexual Harassment Policy*; and all applicable software licenses.
- Use only those computing resources that you are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. You are responsible for ascertaining what authorizations are necessary and obtaining them before proceeding.
- Respect the finite capacity of DISD IT resources and limit your use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. DISD does place limits on the amount of email and file storage. Although there is no set bandwidth, CPU time, or other limit applicable to all uses of DISD IT resources, DISD may require

you to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all relevant circumstances.

- Maintain the security of your own DISD IT accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person. You are presumed to be responsible for any activity carried out under your DISD IT accounts. Password requirements are as follows:
    - Passwords must be at least seven characters in length.
    - Passwords must contain characters from **each** of the following:
        - Uppercase letters (A through Z)
        - Lower case letters (a through z)
        - Base 10 digits (0 through 9)
        - Special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
        - Passwords cannot contain the account name or variations, i.e., no "JDoe" or "DISD".

Passwords will expire every 180 days and users will reset their own passwords via the supplied login interface. Password requirements may be updated and revised as necessary.

To ensure that network speed remains adequate for the educational and administrative functions of DISD, most streaming music and video sites are blocked on the DISD network, with the exception of certain sites, including YouTube, that are regularly used for educational purposes. If you feel you need access to a particular blocked site for educational purposes, please contact the IT Department at support@disd.edu with the name and purpose of the site. Each request will be reviewed on an individual basis.

Personal use of DISD IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of your job or other DISD responsibilities, and is otherwise in compliance with this Data Policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

If you engage in electronic communications with persons in other states or countries or on other systems or networks, you should be aware that you may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. You are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to your particular use.

Prohibited Use

When using DISD IT resources, you must not:

- Deny or interfere with, or attempt to deny or interfere with, service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding and individual, group, or system with numerous or large email messages).
- Engage in harassing, offensive or threatening use, including but not limited to messages, materials, or communications with contain sexual implications, racial or ethnic slurs, or other comments that offensively address someone's age, sex, sexual orientation, religion, national

identity, ancestry, or disability; or which are defamatory, derogatory, obscene, or otherwise inappropriate.

- Engage in criminal activity, including but not limited to sending obscene emails over the internet with the intent to annoy, abuse, threaten, or harass another person.
- Defeat or attempt to defeat any DISD IT system's security – for example, by "cracking" or guessing and applying the identification or password of another user or compromising room locks or alarm systems. (This provision does not, however, prohibit the IT Department from using security scan programs within the scope of its authority).
- Knowingly distribute or launch computer viruses, worms, or other rogue programs.
- Remove from the premises or modify any DISD-owned or administered equipment or data without authorization.
- Use DISD IT resources to solicit or proselytize for outside or personal commercial ventures, religious or political causes, outside organizations, or other solicitations that are not job or curriculum related.
- Copy software or other copyrighted materials, unless specifically authorized to do so by the copyright holders. You must comply with all licensing agreements for software installed on DISD-owned computers. DISD does not permit and will not tolerate the use of software that has been copied or installed in violation of copyright and license agreement. Any software found to be in violation of copyright law will be removed immediately. The unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject you to civil and criminal liabilities as well as DISD disciplinary action.

DISD's Right to Monitor

Privacy is an important value for educational institutions. Creative, innovative, and risky thought as well as scholarship and educational accomplishment all depends on interacting in a communication context in which individuals feel free to express and transmit their opinions and ideas. Thus, DISD extends to its students, faculty and staff a reasonable expectation of privacy in the communication that they conduct using DISD IT resources. Files, email messages, and other data stored on the DISD servers are normally accessible only to the user who created or received that data. Recognizing, however, that privacy cannot be guaranteed, even when it is intended, and exercise reasonable caution in your electronic communication.

Any file, email message, or other data created, sent, stored, or received using DISD IT resources may be accessed in accordance with this Data Policy, and this should not be regarded as private or confidential. Even when a message or file has been erased, it may still be possible to retrieve and read or hear that message or file. Although the privacy of such data is protected in normal circumstances, when, upon the judgment of the appropriate authorities, there is reason to believe the law or DISD policies have been violated, DISD may access or disclose the electronic files, mail, voicemail, and/or electronic discussions stored or transmitted by any user of DISD IT resources. In these cases, an individual with appropriate administrative responsibility will make the determination. Authorized representatives of DISD will monitor the use of its systems at its sole discretion, at any time, with or without notice to any user, and may bypass, delete, change and/or modify and password or security code.

The DISD IT department may routinely monitor communications technology and log usage data, such as network connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, and related techniques. Such monitoring is capable of tracking and recording email

and voicemail messages sent and received as well as internet websites visited. The IT Department also has the ability to directly view any file created, sent, stored, or received using DISD IT resources. The IT Department may review this data for evidence of violation of law or policy, to manage campus network resources, and for other purposes. This data is accessed and used only by authorized members of the IT Department responsible for network performance, operations and planning. You should also be aware that many websites routinely collect and store information about individuals and their online activity. This information may include, but is not limited to, names, email addresses, locations, and IP addresses.

Process

Consistent with the privacy interests of users, DISD access without your consent will occur only with the approval of the CEO, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. DISD will log all instances of access without consent. System Administrators will also log any emergency entry within their control for subsequent review by the CEO. You will be notified of DISD access to relevant DISD IT resources. Depending on the circumstances, such notification may occur before, during, or after the access, at DISD's discretion. In the case of a former faculty, staff member or employee, access without consent must be approved by the CEO and no logging or notice is required.

User Access Deactivations

In addition to accessing the DISD IT resources, DISD may deactivate your DISD IT privileges, whether or not you are suspected of any violation of this Data Policy, when necessary to preserve the integrity of facilities, user services, or data. DISD will attempt to notify you of any such action.

Data Protection

DISD attempts to practice the highest-level security and access controls to support transmission, at rest and use, or viewing of confidential information or DISD data. These practices may include, but are not limited to, commercially available and widespread precautionary measures, such as firewall implementation, virus scanning, logical encryption or data as it leaves the data boundary, secure tunnels, and limitation of physical access to DISD's confidential information. DISD shall ensure that all confidential information and DISD data remains in the United States and is not transferred to, backed up in, or otherwise stored in or accessed from any other countries or jurisdictions.

Incident Response

In the event of a breach, virus, ransomware, or loss of data (collectively, Data Breach), DISD shall notify any effected students, prospective students, faculty, staff and/or alumnus (Effected Parties) within twenty-four (24) hours of any discovery or suspicion of any use or disclosure of DISD or student data, inconsistent with DISD's directions or applicable laws, including but not limited to, any inadvertent or unauthorized use or disclosure of such information, compromised by computer worm, search engine web crawler, password compromise or access by an authorized individual or automated program. Such notice shall summarize, in reasonable detail, the impact on Effected Parties, if known, of the Data Breach and the corrective action taken or to be taken by DISD. DISD shall cooperate fully with Effected Parties in all reasonable and lawful efforts to prevent, mitigate, or rectify such Data Breach.

Telecommuting

On a case-by-case basis, DISD will determine, with information supplied by the staff and faculty member, the appropriate equipment need, including hardware, software, modems, phone and data lines and other office equipment, for each telecommuting arrangement. The supervisor and IT will serve as resources in this matter. The IT Department will also help install Barracuda VPN Connector, if necessary, for remote access to your DISD desktop and network. Equipment supplied by DISD is to be used for business purposes only. The telecommuter must sign an inventory of all DISD property received and agree to take appropriate action to protect the items from damage or theft. Upon termination of employment, all DISD property will be returned to DISD, unless other arrangements have been made.

Consistent with DISD's expectations of information security for staff and faculty members working at the office, telecommuting staff and faculty members will be expected to ensure the protection of proprietary DISD and FERPA student information accessible from their home office. This includes:

- Locking confidential information in file cabinets and desks;
- Regular password maintenance; and
- Any other measure appropriate for the job and the environment.

By attaching privately owned personal computers or other IT resources to the DISD network, you consent to DISD's use of scanning programs for security purposes on those resources while attaching to the network. If you are using the DISD wireless network from your own laptop or mobile device, you must abide by this Data Policy and the *DISD Telecommuting Agreement* as well as all other relevant DISD policies and procedures.

Staff Training

DISD staff and faculty members are required to complete the Cybersecurity Awareness Training on an annual basis. This training is also part of the required training for new staff or faculty members and shall be completed within a reasonable period of time after commencement of employment at DISD and on an annual basis thereafter. Training for new faculty and staff is assigned and monitored by the Director of Compliance. If you have any questions regarding training requirements, please contact mdishman@disd.edu.

Data Retention and Disposal

Student Records

All student records are maintained for a period of six (6) years from the last date of attendance. Student transcripts and ledger cards are maintained permanently.

Staff and Faculty Records

DISD maintains staff and faculty records for one (1) year after employment ceases, per the Equal Employment Opportunity Commission (EEOC) rules. Further, payroll records, employee benefit plan and written seniority or merit system evaluations are kept for three years after termination.

Disposal of Records

At such point that it is determined that records are no longer required to be maintained, all records are shredded either by personal shredder or utilizing the locked shredding bins on campus that are accessed and disposed of by the contracted professional shredding company per their policy.

Privacy

Website

DISD may collect personal data when visiting our website at www.disd.edu. The information DISD collects and retains about an individual is for the purpose of communicating, processing requests for information or for admission to DISD, and relaying information about additional course offerings or other services. We will not sell, share, or rent information to others in ways other than as disclosed.

DISD collects personal data:

- When filling out forms on the DISD website, such requesting information about our program or completing and submitting an online application for admission;
- When an admission application packet is returned to DISD;
- When communicating with DISD electronically or through mail; and
- Through the use of the DISD website, using cookies and pixel tags.

Types of personal data collection:

- Biographical information, such as name, address, email address and phone number, and work experience information;
- Educational background, such as prior educational information and records;
- The IP address, the type of browser used to connect to the DISD site; device information, and if the browser allows cookies, the pages visited, the time, date duration and number of page views and a description of the page where the tag is places; and
- Sensitive personal data, such as racial or ethnic origin and habitation arrangements.

Use of personal data:

- As necessary for the performance of a contract or to take steps preparatory to such a contract – such as when an application for admission is reviewed, responding to requests, sending messages or notices, or otherwise communicating with regards to an application or admission, and any service or support issue you may have;
- To facilitate the experience through cookies which allow the DISD website to recognize if someone has visited multiple pages during the same session, so that it is not needed to re-enter information multiple times;
- When necessary for compliance with a legal obligation, such as to meet compliance and regulatory obligations, both in the US and, if applicable, the EU, including with respect to any EU member state where DISD's programs are offered, or to assist with investigations (including criminal investigations) carried out by the police and other competent authorities;
- When necessary to protect vital interests, such as in medical emergencies;

- When necessary for the purposes of DISD's legitimate interests, such as analyzing DISD's users' online behavior to measure the effectiveness of the website and advertising, using IP addresses to analyze trends, administer the site, track user movement, and gather demographic information for aggregate use;
- To display interest-based ads when using social media.

With whom DISD may share non-sensitive personal data:

- With the user or any person with the user's credentials;
- With DISD's third-party processors who may perform traffic analysis, online advertising and website improvement of the website, but only after they agree in writing to only use such information for the purpose disclosed to them, and in compliance with DISD's Privacy Policy, including not sharing it with any other third-party;
- Governmental authorities, regulatory bodies, law enforcement, or other authorized persons to the extent required by law or deemed by DISD to be necessary, appropriate, or in the best interest of DISD or the public in connection with a request for the foregoing;
- To the extent the user expressly authorized use to do so, affiliated or unaffiliated third-parties for marketing purposes;
- With a third-party, subject to a reasonable obligation of confidentiality, in connection with any merger, acquisition, asset sale, financing, or other capital transaction involving the sale of all, or substantially all of DISD's assets.

We will share your sensitive personal data only with your explicit consent, when necessary for the establishment, exercise or defense of legal claims, or for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

Governing Laws

DISD complies with applicable data protection laws including, but not limited to, the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). *DISD's Privacy Policy* can be found at https://www.disd.edu/privacy-policy.php .

Staff, Faculty and Students

DISD Staff and faculty records involving employee information, health and medical records, investigation records, and management strategy information is kept confidential and only accessible to the employee and designated DISD personnel.

DISD respects the confidentiality of all student records and complies with the Federal Family Educational Rights and Privacy Act of 1974 (FERPA) as amended. The law provides students access to and the right to inspect and review their educations records and prohibits the disclosure of private information maintained in student files. *DISD's FERPA Policy* can be found at https://www.disd.edu/Policy/FERPA-Policy.pdf

The following additional measure are taken to protect any financial records and Personally Identifiable Information (PII):

- Storing paper files and records in a locked filing cabinet when not is use;
- Shredding documents immediately rather than saving them;

- Logging out of computers when away for the desk; and
- Exiting student records and database(s) completely.

Infraction and Discipline Measures

In keeping with its respect for academic freedom, DISD supports free inquiry and expression by the users of its IT resources. However, users who violate this Data Policy may be denied access to DISD computing resources, including the computer lab facilities, and may be subject to other penalties and disciplinary action, both within and outside of DISD.

Complaints of Alleged Violations

If you believe that you have been harmed by or have observed or are otherwise aware of an alleged violation of this Data Policy, you may file a complaint in accordance with established DISD grievance procedures. You are also encouraged to report the alleged violation to the IT Department, who will investigate the allegation and, if appropriate, refer the matter to DISD disciplinary and/or law enforcement authorities.

Disciplinary Procedures & Penalties

DISD may impose sanctions on anyone who is found to have violated this Data Policy. If an individual is found to have violated this Data Policy, they may be subject to IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the CEO in consultation with the appropriate members of the IT Department and legal counsel. Some violations may constitute civil or criminal offenses and mat be subject to local, state and/or federal prosecution.

In addition, DISD reserves the right to terminate any computer network connection without notice when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of DISD or other computing resources or to protect DISD from liability.

Appeals

If you are found in violation of this Data Policy, you may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

Contact

If you need help understanding this Data Policy, or if you discover a violation of this Data Policy, you may contact the following:

- For technology questions or to report suspicious activity please contact the IT Department at support@disd.edu
- For assistance understanding the policy, to report any potential violations or for assistance with personal questions related to complying with the policy, please contact the Director of Compliance at mdishman@disd.edu