Livingston
PUBLIC SCHOOLS

District Acceptable Use and Information Security Regulation #2361.01

Table of Contents

1 Scope

Information management is an essential part of good IT governance, which in turn is a cornerstone in ensuring a well balanced District wide risk management approach. An integral part of IT governance is information security. This document details the Livingston School District's (the "District") end user acceptable use and information security Regulation (the "Regulation"). This Regulation applies to all Livingston Public Schools offices, departments, and affiliated organizations including all employees, consultants, and vendors ("Users"). For the purposes of this Regulation, affiliated organization refers to any organization associated with Livingston Public Schools that uses district information technology resources to create, access, store, or manage district data including, but not limited to, assessment providers, food service providers, tutoring service providers, after school programs, etc. It also applies to any third party vendor creating, storing, or maintaining District Data per a contractual agreement.

All District Data must be classified according to the Data Classification Schema outlined below and protected according to applicable Data Security Standards. This Regulation applies to data in all formats and media.

2 Regulation Statement

The District recognizes that as new technologies shift the manner in which information is accessed, communicated and transferred that those changes will alter the nature of teaching and learning. Access to technologies will allow users to explore databases, libraries, websites, bulletin Districts and the like while exchanging information with individuals throughout the world. The District supports access by users to information sources but reserves the right to limit in-school use to materials appropriate to educational purposes. The District directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The District also recognizes that technologies will allow users access to information sources that have not been pre-screened using District approved standards. The District therefore adopts the following standards of conduct for the use of District provided system, network, and electronic data resources and declares unethical, unacceptable, inappropriate or illegal behavior as just cause for taking disciplinary action, limiting or revoking network and system access privileges, instituting legal action or taking any other appropriate action as deemed necessary.

The District provides access to District provided system, network, and electronic data resources for administrative and educational purposes only. The District retains the right to restrict or terminate users access to the computer network(s)/computers at any time, for any reason. The District retains the right to have the Superintendent or designee monitor network activity, in any form necessary, to maintain the integrity of the network(s) and ensure its proper use.

This Regulation represents a directive from the District and expresses the expectations and responsibilities of users at the District with respect to the security and the protection of District information assets and resources. Computers, servers, telephone and communication hardware and software systems ("Systems") have been installed and are provided to District users to facilitate efficient and effective business operations, communications, and a safe and supportive teaching and learning environment. Maintaining the security, confidentiality, integrity, and availability of information stored, processed, and transmitted using District Systems, is a responsibility shared by all users of those systems. The District's Systems and the information they contain are a vital District asset and require protection from unauthorized access, modification, disclosures or destruction. All users of the District's Systems are responsible for protecting those resources and the information processed, stored or transmitted as set forth in this Regulation.

3 COMPLIANCE

The District reserves the right to modify this document at any time and may use the District e-mail system to distribute the notification of change. Users agree to be bound by all such modifications and revisions as a condition of continued District Systems usage.

Individuals violating this Regulation shall be subject to appropriate disciplinary actions as defined by Policy No. 3150, Discipline which includes but are not limited to:

1. Use of the network(s)/computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension;
7. Dismissal;
8. Legal action and prosecution by the authorities; and/or
9. Any appropriate action that may be deemed necessary as determined by the Superintendent and approved by the District of Education.

All users must acknowledge and agree annually that they have read and understood this Regulation and must abide by it as a condition of District System usage.

3.1 PRIVACY

Users have no right of personal privacy in any matter stored in, created, received, or sent over any District application, system, service, equipment or infrastructure, collectively ("Systems"). Users should never consider electronic communications to be private when using District Systems. As owner of the Systems, the District reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the Systems for any reason without the permission of any user, and without notice.

Users should not store, process or transmit any personal information (e.g. personal passwords, financial account information, etc.) that they would not want the District to view and/or retain. If a user chooses to use the District's Systems to engage in personal communications, the user is doing so in full acknowledgement of the potential disclosure of these personal communications as a result of District monitoring and/or operations. Deletion or destruction of messages and communication will not render them inaccessible. Back-up copies of communications and messages are obtained and stored and may be reviewed and accessed when necessary.

3.2 Acceptable Use Regulation

While it is recognized that incidental and occasional personal use of District Systems may occur, personal use must not interfere or conflict with the District's business and the user's responsibilities to the District.

When communicating by or accessing the Internet through the District's accounts or Systems, users will appear to be acting as representatives of the District and any communications may be deemed to have been made by the District. As such, users should act appropriately to protect the reputation of the District and to comply with the laws applicable to the District.

3.2.1 Acceptable Use

- Users are responsible for exercising good judgment in personal use.
- Users must keep passwords secure and may not share accounts. Authorized Users are responsible for the security of their passwords and accounts.
- Users must utilize the District's Single Sign On (SSO) portal (Classlink) which uses a District approved multi-factor authentication system for accessing other systems.
- Users must utilize the District's approved multi-factor authentication system for other Systems classified as containing confidential data and not accessible solely through the District's SSO portal. This includes Genesis Student and Staff Systems, VPN access and Systems 3000.
- All laptops and workstations should be password protected when left unattended.
- Users must use extreme caution when accessing unknown websites, opening email attachments and clicking links received from unknown senders, which may contain malware.

3.2.2 Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities based on circumstances approved by the District.

No user may engage in any activity that is illegal or prohibited under local, state, federal or international law or regulation while utilizing the District owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Internet, System and Network Activities

The following activities are prohibited:

- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the District.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the District's Systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the User's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any District account or Systems.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a System or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited by any user, with the exception of IT.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account (i.e. disabling or interfering with the installation or distribution of security patches, antivirus definitions, etc.).
- Attempt to change the District's networks, setup connections to external networks (including use of VPNs) or ISPs or attempt any other alteration to the District's networks.
- Connecting non-District owned equipment such as personal laptops, computers, printers, routers, switches, wireless access points (e.g. wireless routers), or other personal devices to the internal network via an ethernet cable or wireless connection. The only exception are personal laptops or phones that are connected to the approved wireless staff network only.
- Interfering with or denying service to any User other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
- Although aesthetic personalization is allowed to such areas as the desktop wallpaper, screensaver, etc, the user must exercise professional judgment in the selection of these customizations and cannot display anything that may be considered offensive or insulting. Strictly prohibited, are any images or content that are derogatory, sexual in nature, depict illegal activities or illicit substances, or are offensive to an individual's religious beliefs, gender, sexual orientation, ethnicity, disability, or political views.
- Providing information about, or lists of, District users to parties outside the District, unless part of normal job duties, such as employment verification by Human Resources or communications with payroll administrator.

Email and Communications Activities

Messages sent or received over the District's electronic messaging system are not private or secure. Even if users use a password to access the email system or any District computer, the privacy of any message stored in, created, received, or sent from our email system is not assured. Use of passwords or other security measures does not in any way diminish the District's right to access materials on our system, or create any privacy rights for employees in the messages and files on the system.

Be aware that sensitive material is at risk of unintended disclosure to third parties. Even when a message is "erased" or "deleted," it is still possible to retrieve and read that message. Furthermore, the use of passwords for security does not guarantee privacy. Users must exercise caution and care when transferring such material in any form.

Notwithstanding the District's right to retrieve and read any electronic messages, such messages should be treated as private and confidential by other users and accessed only by the intended recipient. Staff members are not authorized to retrieve or read any electronic messages that are not sent to them unless given prior approval by the intended recipient or by any other person to whom the intended recipient has assigned proxy rights. Users may not use a password, access a file or retrieve any stored information, unless authorized to do so. Users should not attempt to gain access to another user's messages or data files without that person's permission.

The following activities are prohibited:

- Conducting District business communications using personal email systems is strictly prohibited (e.g. Gmail, Yahoo, etc.).
- Register their personal email address on any websites or subscription services that are used with students or for school related purposes.
- Register their District provided email address with websites or services unrelated to District operations. For example, do not register your District provided email address on dating websites or any personal social media platform such as Facebook.
- The use of any file storage/transfer website or application not explicitly authorized and/or provided by the District for the transfer, storage or sharing of District data is strictly prohibited.
    - Users may use a secure file storage/transfer website that is provided by the requesting party to assist with data transmission
- Sending unsolicited email messages that are not business related including the sending of "junk mail".
- Engage in personal commercial activities, including offering services or merchandise for sale, except as otherwise authorized by the District.
- Create, send, receive or store material that is fraudulent, discriminatory, harassing, obscene, sexually explicit, profane, intimidating, defamatory, or otherwise unlawful, inappropriate or unprofessional, including any derogatory or inflammatory material about issues such as age, sex, race, creed, color, religion, disability, national origin, citizenship, marital status, physical attributes, sexual orientation or any other characteristic protected by applicable law.
- Disseminate, receive, copy or print copyrighted materials without required permissions or licenses unless the proposed use qualifies under the Copyright Act as a "fair use."

A decision that any use is a "fair use" requires clearance from the District's General Counsel.

- Unauthorized use of email header information
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

3.3 Malware, Network and System Protection

The District deploys various security and operational tools to protect the District's systems, data and network against malicious software, unauthorized access and unplanned disruptions.

Users must:

1. Never purposely introduce a malicious program into the systems, applications, or network.
2. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Report suspicious emails to IT and delete these attachments immediately.
3. Never attempt to circumvent the malware and/or any other security protections implemented by disabling, modifying, interfering or uninstalling the application(s).
4. Never download files from unknown or suspicious sources.
5. Never insert an untrusted removable storage drive into the District's equipment.
6. Store District data in approved locations (e.g., Google Drive) that are protected with backups.
7. If a user receives what is believed to be malware, or suspects that a computer is infected with malware, the IT department must be notified immediately.
8. Any malware-infected computer will be removed from the network until it is verified as malware-free.
9. Never utilize any software or tools to scan, probe, or monitor the network
10. Never connect any router, switch, or wireless access point to the network, unless approved by the Director of Technology & Innovation.
11. Never instruct a guest to the District to directly plug-in to a network port or provide them the pre-shared key or password of the private (i.e. employee only) wireless network.

3.4 Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify District Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

The data classification schemes are as follows:

Public - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the District, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:

1. District's public web site
2. Directory information for students, faculty, and staff except for those who have requested non-disclosure (e.g., per the Family Educational Rights and Privacy Act (FERPA) for students)

3. Course descriptions
4. Semester course schedules
5. Press releases

Internal - Data intended for internal District business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the District. Unauthorized disclosure could adversely impact the District, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

1. Financial accounting data that does not contain confidential information
2. Employee ID numbers
3. Student ID numbers
4. Directory information for students, faculty, and staff who have requested non-disclosure (e.g., per FERPA for students.)
5. Lesson Plans

Confidential - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by appropriate District personnel is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the District, the personal privacy of individuals, or on compliance with federal or state laws and regulations. Confidential data have a very high level of sensitivity. Examples include:

1. Social Security Number
2. Personal identity information (PII)
3. Personnel records
4. Medical records
5. Student educational records
6. Information technology transaction logs

3.5 STUDENT DATA

Livingston Public Schools classifies all student Personal Identifiable Information (PII) as private and confidential information. This type of data may be obtained, stored, and reviewed for legitimate educational purposes related to student achievement, accounting, pupil services, operations, compliance, and audit purposes. The maintenance and security of all student health records shall be in accordance with N.J.A.C. 6A:32-7.4 and 6A:16-2.4.

Student data may only be collected and used when meeting the educational needs of the child and as mandated by state and federal law. Student data shall not be disclosed to any party unless they are designated as the data owner (parent or student beyond the age of majority), an identified “School Official,” or an “Authorized Representative” pursuant to federal FERPA guidelines acting in the best interests of the student’s education. All record release requests shall be authorized by the District’s Business Administrator (Custodian of Records) or designee. All student data requests shall be documented and archived as part of this Regulation.

When providing or delivering data to any stakeholder using any delivery mechanism, Livingston Public Schools maintains compliance with the Family Educational Rights and Privacy Act (FERPA). For more information on FERPA, please visit the United States Department of Education's Family Educational Rights and Privacy Act (FERPA).

Personal Identifiable Information (PII) shall be disclosed only under the following conditions and employees shall be informed of such activity prior to release:

- Disaggregated Individual Student Data including but not limited to:
    - Allocation of state education funding
    - Administering state assessments
    - Calculating individual student growth

Aggregated (Summary and De-Identified) Student Data including but not limited to:

- School and/or District Performance Reports
- Program evaluation and measurement
- School and District Improvement Plans
- Federal reporting/funding
- Public reporting

Legal or Disciplinary Analysis – Student Personal Identifiable Information (PII) may be released to appropriate authorities to indicate the presence of activities that violate Livingston District of Education policies and/or state/federal law. These requests shall be in response to documented Regulation incidents, legal discovery, or judiciary requests.

Student Data Requests - All requests to retrieve and share student data in digital or hardcopy must be submitted to the Business Administrator (Custodian of Records) or designee. Any litigation and legal requests require confirmation by the Chief School Administrator or the Business Administrator (Custodian of Records). Such requests shall include:

- Name and role of the requestor.
- Reason for the request, in accordance with the principles set forth in this and other related district Policies
- Parental notification of the event (unless explicitly barred due to legal or disciplinary investigation) shall be made. In all circumstances, parents shall be notified when individual educational record requests are made that are not bound by legal constraints.

Student data shall not be intentionally shared with third parties outside of legally compliant (e.g. research, compliant third party provider operational contracts, federal and state reporting etc.) activities unless that data is authorized by the parent, guardian, or student of majority. All student data requests shall be documented and stored as part of this Regulation.

Student Health Records The maintenance and security of student health records shall be in accordance with N.J.A.C. 6A:32-7.4 and 6A:16-2.4. Student health records may be stored electronically, microfilm or in paper format and shall be maintained separately from other student records in a secure location accessible only by authorized personnel.

3.6 Document and data storage

The District maintains responsibility for the backup of files maintained in designated network and cloud storage locations. If a user chooses to store files locally in a location other than the approved and designated locations, the user is doing so at the risk of data loss or corruption in the event of software or hardware failure.

The District at all times reserves the right to delete personal files from their Systems and storage locations.

Any documents that are downloaded or saved to the hard drive of ANY device for editing or transport must be saved back to the District's approved storage locations when the work is complete to ensure proper security, backup and availability.

Documents that contain highly sensitive information classified as **Confidential**, should never be saved to a personal device. Highly sensitive data is only to be saved to District owned and controlled equipment.

The use of any file storage/transfer website or application not explicitly authorized and/or provided by the District for the transfer, storage or sharing District data is strictly prohibited

The use of removable media, such as USB drives, is strictly prohibited for the storage of any data classified as **Confidential.**

3.7 Password Regulation

Passwords are in common use, they are easy to create and have been the standard for user authentication for a very long time. That means they are susceptible to attack and users must exercise care when using passwords.

3.7.1 General Password Regulation

All passwords used for internal District systems or third party internet accounts, where technically feasible, will be configured to require the following password parameters:

- **First use:** The initial password assigned to Users for access to any of the District systems and applications must be changed on initial login. If the password is not required to be changed on first use, contact the IT helpdesk immediately to have the issue corrected.

- **Password aging:** All District computer users must change his or her password at a defined interval. This interval will change over time as needed in accordance with industry standards. Attempts to login using an expired password will not succeed.

- **Reuse of old passwords:** New passwords must be different from a defined number of prior passwords; at a minimum, one prior password.

- **Account Lockout:** Entry of an incorrect password after five successive unsuccessful attempts will result in the account being locked for usage. Once the account is locked, login attempts will be unsuccessful for a period of time or until Administrator intervention.

- **Password Strength:** To qualify, passwords selected will be required to adhere to a defined set of standards inclusive of a minimum length and complexity requirement. The use of passphrases are strongly encouraged.

3.7.2 Password Protection Regulation

The District recognizes the challenges of remembering multiple unique passwords; as such, where possible, the District will try to provide an SSO experience to limit the number of passwords necessary.

Users are to adhere to the following with regards to protecting their passwords.

- Always use different passwords for various District systems whenever possible.
- Do not use the same password used for Districts Systems that are used for personal systems and accounts.
- Do not share the District's passwords with anyone. All passwords are to be treated as sensitive, confidential District information.
- Passwords should not be written down, electronically transmitted, or stored electronically in an unencrypted format. For example, do not document your passwords in an unencrypted document or spreadsheet (Word, Excel, Docs, Sheets, etc), or permit your password to be saved by a browser (Chrome, Edge, Safari, etc.).
- Do not reveal a password in email, chat, or other electronic communication.
- Passwords may not be left on sticky notes posted on or under a computer, nor should they be left written down in an accessible location
- Do not speak about a password in front of others.
- Do not hint at the format of a password. (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications. (e.g., Google, Edge, etc.)

The District does utilize multi-factor authentication for many of their Systems. The additional security code (i.e. second factor) or push notification, other than their password, is to be protected the same as a password as noted in this Regulation.

If an account or password compromise is suspected, report the incident to the IT helpdesk immediately.

3.8 Mobile Device Regulation

The District may provide select authorized employees a mobile device (laptop, smartphone or tablet) to facilitate the performance of their assigned responsibilities. In addition, the District will allow users to utilize their personal mobile devices to establish a connection to the District's email system. The District reserves the right to revoke this privilege if the user does not abide by the policies and procedures outlined below.

When placing District email on a non-District mobile device, the user acknowledges that they are subject to the terms of this Regulation and the controls specified herein as a condition of connecting their personal Mobile Device.

The following applies to mobile device usage of District Systems, regardless of the ownership of the device:

- In order to prevent unauthorized access, devices must either be password protected with a five-character minimum passcode. or protected with a pattern or biometrics, depending on the capability of the device.
- Passwords are not to be shared with any person under any circumstance. If an employee has reason to believe his or her password has been compromised, then the password must be changed immediately and the IT department must be contacted.
- The device must lock itself after fifteen minutes of idle activity.
- Employees are expected to treat the assigned devices carefully and keep it secure from loss, theft, damage, abuse or unauthorized use.
- Lost or stolen devices must be reported to the District's IT department without delay, and in all cases within 24 hours.
- The District reserves the right to disconnect devices or disable services without notification.
- The employee's device may be disconnected and email removed if
  - the device is lost,
  - the employee terminates his or her employment,
  - IT detects a data or Regulation breach, a virus or similar threat to the security of the District's data and technology infrastructure.
- The District is not responsible for lost personal data on the device should the device be wiped, e.g. personal pictures.
- The employee must not attempt to tamper with or circumvent the security protections placed on the device by the District.
- Upon termination, the employee is to return the District owned device to the District. The last paycheck will be issued as a live paycheck that the employee must pick up once devices are returned. Should the employee fail to return the device, the District may elect to charge the employee the fair market value of the device.

3.9 Physical Security Regulation

Physical security is a key component of protecting the District's systems, data and network. The following describes the District's physical security policies.

- All users shall attempt to follow a clean desk Regulation as it relates to data classified as confidential.
- District equipment should never be left unattended in an insecure location.
- If a device becomes lost or stolen, the IT department is to be notified immediately.
- File cabinets containing **Confidential** information must be kept closed and locked when not in use.
- Keys used for access to/**Confidential** information must not be left at an unattended desk or area.
- Users should ensure the safety of their key cards to access District locations, offices, and facilities. If lost or stolen, the facilities department must be notified immediately.
- Personnel must not allow any unidentified individual to follow them into a key card protected space.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer and stored in a secure location.
- The disposal of **Confidential** documents should be done in official shredder bins or placed in the locked confidential disposal bins
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

3.10 Remote Access Regulation

The District provides the ability to remotely access its network, applications and data through various technologies. When using any of these, users need to comply with the following policies:

- Internet access is required to access the District's network remotely. The District does not provide or reimburse for home internet access.
- When using remote access, a user is responsible to ensure that no unauthorized person gains access to the District's networks, application and content. Users should be vigilant when accessing District networks in public to avoid disclosure of passwords and/or confidential information.
- Remote access to the District network using the VPN will only be allowed if using a District owned and/or controlled device.
- For direct access to District cloud based applications:
  - Administrative users with access to data classified as confidential are only to use District owned and/or controlled devices.
  - For Faculty, the machine or device being used to obtain remote access must not be a device that is not owned or secured by the User, such as a public terminal. If you do not have reasonable confidence in the security of the device, do not use it to connect to and access District application and data.
    - the machine must have up-to-date virus protection software installed and have all recent critical operating system security patches installed.

- When using remote access, whether from a District, third party or private computer, all other IT policies apply as if working from the District's offices.
- IT staff are not responsible for the technical support of non-District equipment.

3.11 Third Party Services

The District recognizes that there are a multitude of applications that can be used to facilitate education. The District further recognizes the ease in which these applications can be obtained as a result of their cloud nature.

To ensure the security of student and District data, users are prohibited from using any software, mobile applications ("apps") and/or web-based tools that have not been explicitly approved by the District. The District will maintain a listing of approved software, mobile applications ("apps") and/or web-based tools on the district SSO portal. Users may only use the approved list of software to ensure the privacy and security of student and employee data in the District.

Should you identify a software or web based service that you believe may be beneficial to the District, all new software and apps must be submitted by district administration to the Department of Technology. The software or app will be reviewed and vetted to ensure that it meets standards set forth in this Regulation. Once the software is approved, it shall be posted on the district SSO portal and website with a link to the vendor's user agreement and data security Regulation.

It is prohibited to register a personal email address on any software or web based service that is used with students or for school related purposes.

3.12 Incident Reporting

We all have a role in protecting the Systems and Data of the District. Should you identify a breach, have a concern about the security of a device or data, or have knowledge of a violation of this Regulation or any other security incident, please contact the IT Department immediately.

4 Exceptions/Approvals

Requests for exceptions to the Regulation must be submitted in writing to the Director of Technology & Innovation and the Superintendent. The Director of Technology & Innovation and the Superintendent will assess the appropriateness of the request, determine the risk of the exception, and if warranted, obtain any necessary additional approvals. All Regulation exceptions will be recorded and reassessed at a minimum of once annually by the Director of Technology & Innovation and the Superintendent to ensure continued appropriateness. Exceptions may be revoked at any time, as deemed necessary by the District to ensure the continued protection of District systems, data, and business interests.

5 Document Control/Revision History

Version	Date	Description of Change	Author
1.0	2/15/2022	First Draft of Info Sec Regulation to District	Teresa Rehman
1.1	10/4/2022	Updates to Acceptable Use Regulation	Teresa Rehman

Acknowledgement/Signoff

I have read this information security Regulation and understand what is required of me to protect the District's network, systems and data. I agree to abide by this Regulation and understand failure to do so could result in formal disciplinary action, including termination of employment.

Employee Name: ______________________________________

Signature: ______________________________________ Date: ______________________