LYON COUNTY SCHOOL DISTRICT
BOARD POLICY _____ GBBP

INFORMATION TECHNOLOGY

~~The District requires employees to use information technology (computer systems, telecommunication, other devices, artificial intelligence (AI) platforms, and electronic information/communication) responsibly, and in a manner, which is not detrimental to the mission and purpose of the District. To maintain a level of professionalism, any publication through any means (electronic or otherwise), which is potentially~~ This policy establishes employee obligations for the responsible, secure, ethical, and lawful use of District information technology (IT), electronic communications, artificial intelligence (AI) tools, social media, and related systems. Any use of District systems, devices, or platforms that is adverse to the operation, morale, or efficiency of the District, or that violates District policy or applicable law, ~~will~~ may be deemed a violation of this policy.

~~Employees are prohibited from engaging in any conduct that violates District policy or procedure.~~ This policy applies to all employees, elected officials, appointed officials, board members, contractors, consultants, volunteers, interns, temporary staff, and any other users granted access to District-owned systems, networks, applications, devices, accounts, data, or communication platforms. Use of personal or District electronic devices, ~~to engage in such conduct can create liability for the District, and as such, obligates the District to undertake reasonable procedures to investigate allegations, including but not limited to the inspection of the equipment. In the event an employee becomes the subject of such an investigation and the allegations include potential violations of District policies, whether on work or personal time, and whether using District or personal devices, the District will undertake an investigation and inquiry by all means allowable under state and federal law.~~

~~The District will periodically provide cybersecurity training to educate employees about the dangers of phishing, ransomware infections, and social engineering.~~ remote access systems, cloud services, mobile devices, or third-party platforms in connection with District business is subject to this policy. An employee's use of any such system to access District files or work-related materials constitutes acceptance of this policy and its requirements.

Nothing in this policy is intended to restrict communications or activities protected by federal or state law, including lawful discussion of wages, hours, working conditions, or other matters protected under labor relations or whistleblower statutes.

Reference: NRS 613.135 and 391

LYON COUNTY SCHOOL DISTRICT
BOARD POLICY _____GBBP

INFORMATION TECHNOLOGY - ADMINISTRATIVE REGULATIONS

1. Privacy and Monitoring

Employees have no expectation of privacy ~~regarding their activities~~ when using the District's systems, accounts, networks, or data, even ~~when using~~ via a personal device~~s~~. The ~~U~~use of passwords, ~~or~~ account ~~numbers~~ credentials, personal devices, encryption, or private browsing tools ~~by employees~~ does not create an ~~reasonable~~ expectation of privacy ~~and confidentiality of information being maintained or transmitted. The District reserves the right to monitor communications and file activity in compliance with privacy laws~~ when accessing District resources.

The District may monitor, access, preserve, review, audit, disclose, or investigate email communications, internet activity, system logs, file activity, application use, network traffic, remote access activity, account activity, security alerts, District-owned social media accounts, District-owned cloud services, District-owned devices, and District data accessed from personal devices. Monitoring will be conducted for legitimate business, operational, security, legal, compliance, records retention, and investigative purposes, and in accordance with applicable law.

Employees consent to such monitoring by use of District systems, even for limited personal use.

In accordance with ~~provisions of~~ NRS 613.135, the District will not request usernames ~~and~~ or passwords for personal social media accounts and will not take ~~any type of~~ employment action against an employee ~~who~~ solely because the employee refuses to provide ~~the~~ a username ~~and~~ or password for ~~their~~ a personal social media account. This ~~provision~~ restriction does not prevent the District from requiring ~~an~~ employees to disclose the username, ~~and~~ password, or access credentials for ~~access to the~~ District-owned systems, District-managed accounts, District social media accounts, or other District~~'s computer or~~ information systems.

2. Acceptable Use of District Technology

~~The computers, associated hardware and software including, but not limited to, electronic mail (e-mail or instant messaging "IM") and access to online services, as well as voice mail, pagers, smart phones and faxes, even when accessed from a personal device, belong to the District and, as such, are provided for business use.~~

DRAFT

Users must use District technology resources in a professional, lawful, and secure manner. District computers, electronic equipment, hardware, software, email, voicemail, smartphones, faxes, and related systems belong to the District and are provided for business use, even when accessed from a personal device. Employees may use these resources for job-related tasks and research, professional communication, approved training, participation in professional associations, and other District business.

a. Limited Personal Use:

Very limited or incidental personal use of District-owned equipment ~~by employees for personal, non-business purposes~~ is acceptable as long as it:

- ~~a)~~ Is conducted on personal time (i.e., during designated ~~breaks~~ rest or meal periods);
- Does not interfere with job duties;
- ~~b)~~ Does not consume system resources or storage capacity;
- ~~c)~~ Does not involve any prohibited use~~s~~; ~~and~~
- Does not expose District systems to security risk;
- Does not involve confidential, non-public, or legally protected District information;
- Does not imply the employee is speaking on behalf of the District; and
- ~~d)~~ Does not reference the District or ~~themselves as an~~ employee~~s~~ role with the District without prior approval~~, including, but not limited to:~~
  - ~~Text which identifies the District;~~
  - ~~Photos which display District logos, patches, badges, or other identifying symbols of the District;~~
  - ~~Information of events which occurs involving the District without prior approval~~
  - ~~Any other material, text, audio, video, photograph, or image which identify the District~~.

b. Software Installation

Employees ~~loading, importing, or downloading files from sources outside the~~ must obtain authorization from their administrator, manager, supervisor, and the IT Director or designee before installing any software on the District's system~~s~~, including ~~files from the Internet, World Wide Web, social media sites, and any computer disk, must ensure the files and disks are scanned with the District's current virus detection software before installation and execution. Compliance to copyright or trademark laws prior to downloading files or software must be adhered to explicitly~~ desktop or mobile applications, browser extensions, remote access tools,

DRAFT

automation tools, AI tools, and any other software or application not approved by the District.

~~Employees may use information technology, including the Internet, World Wide Web, and social media sites during work hours on job-related matters to gather and disseminate information, maintain their currency in a field of knowledge, participate in professional associations, and communicate with colleagues in other organizations regarding business issues.~~

~~An employee's use of the District's computer systems, telecommunication equipment and systems, other District devices, or the employee's use of personally-owned electronic devices to gain access to District's files or other work-related materials maintained by the District constitutes the employee's acceptance of this policy and its requirements.~~

~~Employees must attain authorization from their administrator or manager/supervisor and the District Information Technology (IT) Manager prior to installing copyrighted software to ensure the District has an active license and distributing or copying property protected by copyright, trade secret, patent, or other intellectual property.~~

~~Personal use must not occur during working hours (except for lunch/break periods), reference the District without approval, and/or consume excessive District resources.~~

c. Downloads and External Files
External files must be opened, downloaded, or transferred only through approved systems protected by District-managed security controls. Compliance with copyright and trademark laws is required.

d. Personal Device Access
Employees who use personally owned devices to access District systems, accounts, or data do so subject to this policy. The District may require that personal devices used for District access meet minimum security standards as a condition of continued access. Employees must not use jailbroken, rooted, or unsupported personal devices to access District systems. Employees must immediately report the loss, theft, or suspected compromise of any personal device used to access District systems or data to their administrator, manager, supervisor, and the IT Director or designee.

e. Credential Protection and Multi-Factor Authentication
Employees are responsible for protecting all assigned usernames, passwords, and authentication credentials. Employees must not share passwords, use another employee's account, allow another person to use their account, store passwords in

unsecured locations, or reuse District passwords on personal or unrelated systems. Employees must not share multi-factor authentication (MFA) codes, approve push notifications on behalf of another person, or assist any individual in bypassing authentication requirements. Employees must not approve MFA prompts they did not personally initiate. Unexpected or repeated MFA prompts must be reported immediately to the employee's administrator, manager, supervisor, and the IT Director or designee.

f. Unauthorized Data Storage and Transmission
Employees must not store, transmit, or share District data through personal email accounts, personal cloud storage, unapproved file-sharing services, unauthorized messaging applications, or unauthorized collaboration platforms. Employees must not connect unauthorized removable media (e.g., USB drives, external hard drives, personal storage devices) to District systems without prior written authorization from their administrator, manager, supervisor, and the IT Director or designee. District data must be stored, transmitted, and shared only through approved systems (e.g., District-issued email, designated cloud storage, approved project-management tools) and authorized business processes.

g. Removable Media
Employees may not connect personally owned removable media (e.g., USB drives, external hard drives, memory cards) to District systems unless specifically authorized. District-approved removable media must be scanned for malware before use. Removable media must not be used to bypass District security controls, data protection requirements, or records retention obligations.

3. Prohibited Activities

Any electronic communication or electronic activity that is adverse to District operations, morale, public perception, security, or efficiency may be treated as a violation of this policy.

Users must not use District systems or data in a way that:

- Interferes with District operations;
- Creates unnecessary legal, financial, reputational, or cybersecurity risk;
- Violates applicable law or District policy;
- Discloses confidential, restricted, regulated, or non-public information;
- Harasses, threatens, discriminates against, or bullies another person; or
- Damages the integrity, availability, or security of District systems.

DRAFT

The following activities are strictly ~~forbidden by this policy~~ prohibited:

a. Violations of ~~the rights of any person or entity protected by~~ copyright, trade secret, patent or other intellectual property rights, ~~or similar laws or regulations,~~ including ~~but not limited to the~~ installation or distribution of ~~"~~pirated~~"~~ or ~~other~~ unlicensed software ~~products that are not appropriately licensed for use by the District~~.

b. Unauthorized copying of copyrighted material, including ~~but not limited to digitization and distribution of~~ photographs, ~~from magazines, books or other copyrighted sources, copyrighted~~ music, ~~and the installation of any copyrighted~~ or software for which the District or employee ~~the end user~~ does not have an active license.

c. The installation of software on District ~~computers~~ systems without the prior approval of the IT ~~Manager~~ ~~is prohibited~~ Director or designee.

~~d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The District IT Manager should be consulted prior to export of any material that is in question.~~

~~e~~d. Introduction of malicious programs into the District network or ~~server~~ systems (e.g., viruses, worms, Trojan horses, ransomware, spyware, email bombs).

~~f~~e. Allowing unauthorized persons including family or household members access to confidential or proprietary District information ~~on District systems. This includes family and other household members when work is being conducted at an employee's home~~.

~~g~~f. Using District equipment or systems to ~~actively engage in procuring~~ procure or transmit~~ting~~ material~~s~~ that ~~are in violation of harassment or employee bullying policies and the laws of the State of Nevada~~ violates the District's anti-harassment or bullying policies.

~~h~~g. Making fraudulent offers, ~~of projects, items or services originating~~ representations, or communications from any District account.

~~i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.~~

~~j~~h. ~~E~~Affecting security breaches or disruptions of network communication.

DRAFT

~~k. Port scanning or security scanning, unless conducted by or on behalf of the IT Manager or designee during duties performed on behalf of the District.~~

~~l. 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.~~

~~m~~i. Circumventing user authentication or security controls ~~of~~ on any host, network, or account.

~~n~~j. Interfering with or denying service to any user ~~other than the employee's host~~ (e.g., denial of service attack).

~~o. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/intranet/extranet.~~

~~p~~k. Sending unsolicited email messages, ~~including the sending of "~~junk mail,~~"~~ or ~~other advertising material to individuals who did not specifically request such material (e.g., email~~ spam~~)~~.

~~q~~l. Any form of harassment or bullying via email, telephone or text~~, whether through language, frequency or size of messages~~.

~~r~~m. Unauthorized use~~,~~ or forging~~,~~ of email header information.

~~s. Solicitation of email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.~~

~~t~~n. Creating or forwarding ~~"~~chain letters,~~"~~ ~~or "~~Ponzi~~"~~ schemes, or ~~other~~ pyramid schemes ~~of any type~~.

~~u. Use of unsolicited email originating from within the District's networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the District or connected via the District's network.~~

~~v. Physical alteration or repair of any hardware or software such as computers, laptops, printers, fax machines, phones, online services, email systems, bulletin board systems, recording equipment, copiers, or any other software that is owned, licensed by or operated by the District, as well as monitors, mice, keyboards; users must report any problems with hardware or software to the District help desk ticket system.~~

DRAFT

o. Storing, transmitting, or sharing District data through unauthorized personal email accounts, personal cloud storage, unapproved file-sharing services, unauthorized messaging application, or unauthorized collaboration platforms.

p. Physical alteration or repair of District-owned hardware or software without authorization. Employees must report hardware or software problems to their administrator, manager, supervisor, and the area IT Technician.

q. Using social media to harass, threaten, discriminate against, or disparage employees or anyone associated with or doing business with the District.

r. Disclosing confidential, non-public, or legally protected District information through any electronic means without authorization.

NOTE: *This section does not prohibit authorized IT administration, cybersecurity testing, incident response, legal review, law enforcement activity, or other investigative activity conducted within the scope of assigned duties and written authorization.*

4. ~~Permitted Activities~~ **Public Records and Records Retention**

~~Use of District computers and electronic communications resources are for program and business activities of the District. All use of such resources shall be conducted in a framework of honest, ethical and legal activities that conform to applicable license agreements, contracts, and policies regarding their intended use. Employees consent to District monitoring by using District systems, even for limited personal use.~~

District-related communications and work products created or transmitted by employees may constitute official records or public records subject to applicable law, including NRS 239. This includes email, text messages, chat messages, social media posts, AI-generated work products, electronic files, reports, and communications sent from personal devices in connection with District business.

Employees must retain, preserve, and dispose of records in accordance with applicable law, District records retention schedules, and any litigation hold requirements communicated by the District. Employees must not delete, alter, conceal, or destroy District records except as authorized by applicable retention policy and law. Questions regarding records retention obligations should be directed to the Communications and Public Relations Officer.

5. Artificial Intelligence Acceptable Use

~~a. Regulation~~

DRAFT

~~This regulation outlines the responsible, ethical, and legal use of artificial intelligence (AI) technologies for employer business purposes.~~

~~b. Purpose~~

~~The purpose of this regulation is to establish the rules for acceptable use of the recent growth of AI technologies relating to District information resources. This regulation applies to all employees, contractors, and third-party vendors who utilize AI technologies on behalf of the District. It encompasses all AI systems, applications, and application programming interfaces (APIs), including, but not limited to, ChatGPT, Gemini, image generators, and other machine learning algorithms, natural language processing, computer vision, and robotic process automation, ensuring AI technologies are used in a manner that aligns with the District's core values and mission, promoting transparency, accountability, and public trust in our AI initiatives.~~

~~c. Responsible Use of AI~~

- ~~*General Rule:* Employees may use District approved AI technologies to generate work-related content or complete work tasks under the supervision of their administrator/supervisor and District administration.~~
- ~~*Lawful Use:* AI technologies are quickly evolving and should be used in compliance with all applicable laws, regulations, and policies. Any use that violates legal requirements or infringes upon the rights of individuals is strictly prohibited. NRS 391 prohibits AI from performing the functions and duties of a school counselor, school psychologist, or a school social worker.~~
- ~~*Data Privacy and Security:* All AI activities must prioritize the protection of personal information and respect privacy rights. Any data collected or processed by AI systems should be handled in accordance with relevant privacy and security policies. Uploading personal or confidential information into AI systems is strictly prohibited.~~
- ~~*Transparency and Explainability:* Whenever AI systems are deployed, efforts should be made to disclose the use of AI where required by employer policy, or law, ensuring transparency and explainability. Users should have access to information regarding the functioning of AI systems, the data used, and the algorithms applied.~~
- ~~*Bias Mitigation/Fairness and Equity:* AI systems should be designed and implemented with measures to mitigate bias. Special attention should be given to promote fairness and equity, and avoid discrimination based on race, gender, religion, or any other protected characteristics. Bias mitigation efforts should be included in the prompt and may be subject to review by appropriate District personnel.~~

- *Human Oversight:* AI should be used as a tool to assist decision-making, and human oversight should be maintained. Final decisions should not solely rely on AI outputs and should involve critical evaluation by qualified individuals.
- *Accountability:* Individuals responsible for the use, development, deployment, and maintenance of AI systems will be accountable for their actions. They should ensure that AI systems are designed to minimize harm and maximize benefits for all stakeholders.
- *Closed-Universe AI Requirement:* All AI systems used for employer business purposes must operate within a closed-universe or enterprise-controlled environment. A closed-universe AI environment is defined as an AI system that does not use employer data, prompts, or outputs to train public or third-party models, and restricts data access to authorized users only. Use of public, consumer, or open AI platforms that retain, reuse, or train on submitted data is prohibited unless explicitly approved in writing by the superintendent or designee.
- *Public, Consumer/Open AI Tools Restriction:* Public or consumer-facing AI tools include, but are not limited to, freely available or subscription-based AI services that are not operated, hosted, or contractually controlled by the employer. Use of public/open AI tools for employer business purposes is prohibited unless explicitly approved in writing by the superintendent or designee. Employees shall not input, upload, or process employer data, internal communications, confidential information, or work product into public/open AI tools under any circumstances. This includes personally identifiable student data and other student information or records. Public/Open AI tools may not be used where prompts or outputs are retained, logged, shared, or used to train third-party models outside of the employer's control.
- *Prompt and Output Preservation:* All prompts, inputs, uploaded materials, and AI-generated outputs created by employees while using AI systems for employer business are considered employer records and employer intellectual property. The employer reserves the right to log, monitor, retain, review, and audit AI prompts and outputs in accordance with records retention, legal, and information security requirements. For public entities, such materials may constitute public records under NRS 239. A record is subject to retention and preservation requirements when it is created, received, or retained by a public officer or employee in the course of public business, and must be preserved without destruction upon receipt of a public records request or other applicable legal hold.

d. Responsible Data Usage

- *Data Collection and Consent:* Data collection through AI systems must be limited to what is necessary for the intended purposes. Appropriate consent should be obtained from individuals when their personal data is being processed.

- ~~*Data Quality and Integrity:* AI systems should be developed using accurate and reliable data. Efforts must be made to ensure data integrity, prevent data tampering, and maintain data quality throughout the AI lifecycle. AI platforms may produce inaccurate or misleading results, warranting cross-reference and validation.~~
- ~~*Data Retention and Disposal:* Personal data collected by AI systems should be retained only for as long as necessary and securely disposed of when no longer needed according to District policy. AI-generated records, including prompts and outputs, shall be retained, classified, and disposed of in accordance with employer records retention and legal hold requirements.~~

This section establishes employee obligations for the responsible, ethical, and lawful use of AI tools in connection with District operations. It applies to all AI systems, applications, browser extensions, plug-ins, Application Programming Interfaces (APIs), image generators, transcription tools, meeting assistants, automation platforms, natural language processing tools, computer vision tools, and robotic process automation tools used for District business.

For purposes of this policy, "public AI tools" means free or consumer-grade AI platforms, browser-based AI tools, personal AI accounts, AI plug-ins, and any tool where District data may be used for model training or retained outside District control.

Employees must comply with these regulations and those outlined in *LCSD Board Policy IAA - Use of Artificial Intelligence (AI)* when using AI.

a. Approval Requirements

The Lyon County School District has approved district sponsored AI systems which are closed and secured for work-related use.

Employees must obtain written pre-approval from their administrator, manager, supervisor, and the IT Director or designee before using public AI tools to generate, process, analyze, summarize, or automate District work products. Approval should identify the approved tool, the approved business purpose, the type of data permitted and prohibited for use, any disclosure or citation requirements, and the person or department responsible for oversight.

b. Lawful Use

AI technologies must be used in compliance with all applicable laws, regulations, and District policies. Any use that violates legal requirements or infringes upon the rights of individuals is strictly prohibited.

c. Prohibited Data

DRAFT

Employees must not enter, upload, paste, summarize, transmit, or process the following into public AI tools:

- Social Security numbers, driver's license numbers, dates of birth, or other government-issued identification numbers;
- Personnel records, employment information, or employee disciplinary records;
- Student education records, assessments, medical records, or any other data associated with students;
- Medical or health information;
- Law enforcement records, reports, or criminal justice information;
- Legal advice, attorney-client privileged communications, or non-public contracts;
- Security or network infrastructure information, including network diagrams, firewall rules, vulnerability reports, penetration testing results, and incident response records;
- Authentication credentials, including passwords, MFA codes, API keys, access tokens, and private keys;
- Financial account information, vendor banking details, or payment information, or vendor W-9 or ACH information;
- Investigative records;
- Confidential meeting notes or non-public operational information; and
- Any records protected under state or federal statute, regulation, or court order.

Exceptions require written approval from the District and confirmation that the AI tool meets applicable security, privacy, legal, and contractual requirements.

d. Transparency and Disclosure

Employees must disclose when AI substantially assisted in producing an official work product submitted on behalf of the District, including reports, or policies, public-facing materials, grant narratives, disciplinary documents, legal summaries, investigative summaries, or other official District work products. AI-generated content must not be represented as independently verified work unless the employee has reviewed and validated it.

e. Human Oversight and Decision-Making

AI should be used as a tool to assist decision-making; human oversight must be maintained. Final decisions should not solely rely on AI outputs and must involve critical evaluation by qualified individuals. AI must not serve as the sole basis for decisions involving employment, discipline, hiring, promotion, benefits, eligibility determinations, legal conclusions, financial approvals, or other decisions affecting individual rights or District obligations.

f. Accuracy and Verification

DRAFT

AI platforms may produce inaccurate results. Employees are responsible for reviewing and verifying AI-generated content before use, including factual claims, citations, legal references, calculations, names, dates, summaries, and public-facing content. AI output must not be treated as authoritative without independent review.

g. Bias and Fairness

Employees must not knowingly use AI tools to discriminate against individuals based on race, gender, religion, or any other protected characteristic. When AI tools are used for analysis or decision support, employees must consider the possibility of bias, incomplete data, or inaccurate outputs.

h. Accountability

Employees responsible for the use of AI tools are accountable for ensuring those tools are used appropriately and in accordance with this policy. AI tools used for District business may require review by the IT Director or designee, Legal, HR, or Risk Management department(s) before approval.

i. AI Meeting Assistants and Transcription Tools

Employees may not use AI meeting assistants, transcription tools, recording bots, or automated note-taking tools in District meetings, executive sessions, personnel matters, legal meetings, or other confidential discussions unless specifically authorized in advance by the Superintendent or designee. Use of such tools must comply with applicable consent, privacy, confidentiality, and public records requirements.

j. Training

The District will periodically provide training on responsible AI use, ethical obligations, and applicable policy requirements.

e6. Reporting Violations

Employees must immediately report any actual or ~~perceived~~ suspected violations of this policy to their immediate administrator, supervisor, manager, or the Executive Director of Human Resources and the IT Director or designee as appropriate. Reportable events include, but are not limited to: cybersecurity incidents, unauthorized access, confidentiality breaches, AI misuse, social media violations, lost or stolen devices, suspicious emails or attachments, ransomware indicators, malware alerts, unexpected MFA prompts, accidental data disclosure, unauthorized account access, unauthorized software installation, and suspicious financial, payroll, vendor, or payment change requests.

DRAFT

Employees must report suspected phishing attempts, ransomware infections, or social engineering attempts through the Phish Alert Button (PAB) on their email application and/or to the IT department immediately.

Employees must not attempt to independently investigate, delete, forward, or remediate suspected malware, ransomware, phishing, or unauthorized access without instructions from the IT department or authorized personnel.

~~f~~7. Cybersecurity Training

~~AI is growing rapidly and being integrated into existing architecture during vendor updates to hardware, software, and firmware. Regular monitoring and AI ethics training will be provided to employees.~~

The District will periodically provide cybersecurity training covering phishing, ransomware, social engineering, password security, MFA, data protection, incident reporting, AI risks, social media risks, and other relevant topics. Employees may be required to complete assigned training within designated timeframes.

~~g~~8. Violations ~~of Policy~~ and Enforcement

Employees in violation of ~~the provisions of~~ this policy may be subject to disciplinary action, up to and including termination, depending on the nature, severity, intent, frequency, and impact of the violation. The District reserves the right to take legal action where necessary against employees, volunteers, vendors, consultants, or contractors who engage in prohibited or unlawful conduct. The District will promptly investigate and respond to all reported violations.

~~Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.~~

9. Prohibition Against Retaliation

The District prohibits retaliation against any person who reports a suspected violation of this policy, cooperates with an investigation, participates in a review, or raises a good-faith concern. Employees who believe they have been retaliated against should immediately notify the EEO Officer or designee. The District will promptly investigate reports and take appropriate action.

DRAFT