RESPONSIBLE USE POLICY (RUP) INFORMATION AND ACKNOWLEDGMENT FORM FOR EMPLOYEES

Purpose

The purpose of the District's Responsible Use Policy ("RUP") is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information and to comply with legislation including, but not limited to, the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), and the California Electronic Communications Privacy Act (CalECPA). Furthermore, the RUP clarifies the educational purpose of District technology.

As used in this policy, "user" includes anyone using computers, the Internet, email, and all other forms of electronic communication or equipment provided by the District (the "network"), regardless of the physical location of the user. The RUP applies even when District provided equipment (laptops, tablets, etc.) is used outside of District property. Additionally, the RUP applies when non-District devices access the District network or sensitive information.

The District uses technology protection measures to block or filter access, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, or harmful to minors over the network. The District reserves the right to monitor users' online activities and to access, review, copy, store, or delete any communications or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network, and/or Internet access or files, including email. Users understand that the District has the right to take back possession of District equipment at any time.

The District will take all necessary measures to secure the network against potential cybersecurity threats. This may include blocking access to District applications, including but not limited to email, data management and reporting tools, and other web applications outside the United States and Canada.
The RUP also applies to the use of artificial intelligence (AI) tools, including, but not limited to, generative AI tools that can generate new content, including text, images, video, audio, structures, computer code, synthetic data, etc., in response to prompts generated by users.

Employee Responsibility

If you are supervising students using technology, be vigilant to ensure students are meeting the provisions outlined in the RUP.

Digital Citizenship

- All employees are responsible for modeling and actively practicing positive digital citizenship.
- Employees are responsible for implementing the District's Screen Time policy. This includes monitoring student screen time and ensuring adherence to grade-level limits and content restrictions.
- Do not generate or distribute images, recordings, videos, or statements that misrepresent or seek to misinform others.
- Employees using classroom technology are explicitly required to teach students about positive digital citizenship.
- What employees do and post online must not disrupt school activities or compromise school safety and security.

Privacy

- Do not share personal information about students and employees, including, but not limited to, names, home addresses, birth dates, telephone numbers, student ID numbers, employee numbers, and visuals.
- Do not share confidential, sensitive, or private information about yourself or others in AI prompts, including generative AI tools, including but not limited to pupil or employee record information or images, videos or voice recordings of pupils or employees.
- Only use e-mail accounts created and contained within the District's network systems e.g., those ending in "@LAUSD.NET") to transmit Personally Identifiable Information (PII) from students' education records to other District e-mail accounts of District employees who have a legitimate educational or business interest in the information.
- The transmission of student information to external parties (including public agencies such as the Los Angeles County Probation Department, Los Angeles County Department of Children and Family Services, Los Angeles County Office of Education, etc.) by District e- mail must be encrypted.
- Requests for information from external parties shall be referred to the appropriate District office.
- Do not automatically forward messages from a District email account to any non-District account(s) for the purpose of creating a personal email archive or for using a single email account to access both personal and District email.
- If Protected Information must be shared via a file sharing or collaboration service, only use a service that the District has approved for sharing such information.

- Be aware of the privacy policy on websites and how they collect and share District information.
- Abide by all laws, this Responsible Use Policy, and all District security policies.

Passwords

- Adhere to District policy regarding password management.
- Under no circumstances are District provided email accounts to be used for personal, unauthorized, non-SSO integrated and/or non-District related applications.
- Under no circumstances are District usernames and/or passwords to be shared with others, including other District staff and students, either directly or indirectly.

Professional Language

- Use professional language in all work-related communications, including email, social media posts, audio recordings, conferencing, artistic works, and in prompts for AI tools, including generative AI tools.

Cyberbullying

- Bullying in any form, including cyberbullying, is unacceptable both in and out of school.
- Report all cases of bullying to the site administrator or other authority.

Inappropriate Material

- Do not seek out, display, or circulate material that is hate speech, sexually explicit, or violent while at school or while identified as a District employee.
- Exceptions may be made in an appropriate educational context.
- The use of the District network and equipment for illegal, political, or commercial purposes is strictly forbidden.
- Transmitting large files unrelated to District business and disruptive to the District network is prohibited.

Security

- All users are responsible for respecting and maintaining the security of District electronic resources and networks.
- Only use software and hardware that has been authorized for use by the District.
- Do not use the District network or equipment to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users.
- Do not try to bypass security settings and filters, including through the use of proxy servers to access websites blocked by the District.
- Do not install or use illegal software or files, including unauthorized software or apps, on any District computers, tablets, smartphones, or new technologies.

- Remote access to the District network must occur through an authorized channel(s) as described in BUL- 1597, Acceptable Use Policy for ITD Virtual Private Network (VPN) Services.
- Review any outputs from AI tools, especially generative AI tools for accuracy and appropriateness, as these tools have been shown to generate false information as accurate.
- Employees must guide students on the ethical and responsible use of AI, including proper citation, if students are permitted to use AI for class assignments.

Equipment and Network Safety

- Equipment, information, or software, regardless of its form or storage medium, may not be taken off-site without prior written permission by an employee's administrator.
- Take all reasonable precautions to protect District equipment and if equipment is authorized for use off-site, it must only be controlled by the person who was granted permission for its removal.
- Use caution when downloading files or opening emails, as attachments could contain viruses or malware.
- Vandalism in any form is prohibited and must be reported to the appropriate administrator and/or technical personnel.
- Report lost or stolen equipment to IT Security immediately.
- Report system weaknesses or security events related to protected District data or information systems housing protected data to IT Security.

Clear Desk and Screen

- Employees who are not at his/her assigned workplace must ensure that all protected paper documents, as well as data storage media with protected data, be removed from the desk or other places (e.g., printers, fax machines, photocopiers, etc.) to prevent unauthorized access.
- Employees who are not at their assigned workplace must ensure that all protected information be removed from their computer screen, and access is denied to all systems for which the employee is authorized to use by logging off the District network, locking the screen with a password, or turning off the computer.

Copyright

- While there are fair use exemptions, all users must respect intellectual property.
- Follow all copyright guidelines when using the work of others.
- Do not download illegally obtained music, software, apps, and other works.
- Cite outputs of AI tools, including generative AI tools, when used.

Consequences of Irresponsible Use

- Failure to uphold the responsibilities listed above is misuse. Misuse of District devices and networks may result in:
  - Restricted access or account cancellation
  - Disciplinary action
  - Legal action against employees, including personnel action and/or criminal prosecution by government authorities.
  - The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

The District makes no guarantees about the quality of the services provided and is not liable for any claims, losses, damages, costs, or other obligations arising from use of the network or District accounts. Users are responsible for any charges incurred while using District devices and/or network. The District also denies any liability for the accuracy or quality of the information obtained through user access. Any statement accessible online is understood to be the author's individual point of view and not that of the District, its affiliates, or its employees.

Instructions:

After having read the above information, sign below, and return it to your administrator or other designated supervisory personnel.

I have read, understand, and agree to abide by the provisions of the Responsible Use Policy of the Los Angeles Unified School District.

School/Office:_____

Employee Name:_____Employee Number: _____

Employee Signature:_____Date:_____

Please return this form to your supervisor or administrator, where it will be kept on file. It is required for all employees who will be using a computer network and/or Internet access.