

Employee Acceptable Use Agreement and Release of District from Liability

The Pleasant Valley School District authorizes District employees to use technology owned or otherwise provided by the District as necessary to fulfill the requirements of their position. The use of District technology is a privilege permitted at the District's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Employee Acceptable Use Agreement. The District reserves the right to suspend access at any time, without notice, for any reason.

The District expects all employees to use technology responsibly in order to avoid cybersecurity threats, potential systems, network or end-user issues, and liability. The District may place reasonable restrictions on the sites, material, and/or information that employees may access through the system.

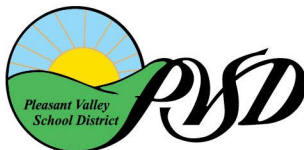
The District makes no guarantee that the functions or services provided by or through the District will be without defect. In addition, the District is not responsible for financial obligations arising from unauthorized use of the system.

Each employee who is authorized to use District technology shall sign this Acceptable Use Agreement as an indication that they have read, understand and will abide by the requirements set forth in the agreement.

Definitions: District technology includes but is not limited to: computers, the District's computer network including network switches, routers, servers and wireless computer networking technology (Wi-Fi)/wireless access points, the internet, WAN/LAN, VPN, email, USB drives, hard drives or other forms of storage, tablet computers, smartphones, smart devices or other mobile technology, telephones, cellular telephones, hotspots, personal digital assistants, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through District-owned or personally owned equipment, system accounts/credentials, or devices.

Employee Obligations and Responsibilities: Employees are expected to use District technology resources ethically, safely, responsibly, and for work-related purposes. Any incidental personal use of District technology shall not interfere with District business and operations, the work and productivity of any District employee, or the safety and security of District technology. The District is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of District technology. District accounts and/or devices should not be utilized for regular personal use or be allowed to be used by children or other family members in the home, etc. District accounts and/or devices should not be used to sign up for personal mailing lists, bank accounts, or other uses that are not work-related.

The employee in whose name District technology is issued is responsible for its proper use and care at all times. Employees shall never share their assigned online services account information, passwords or other information used for identification and authorization purposes with anyone, at



any time, or for any reason. (This includes sharing account credentials with technology services staff or via helpdesk support requests, etc.) Employees shall use District systems and applications only under the account to which they have been assigned. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the District's system for which they do not have direct authorization.

In order to maintain the security and confidentiality of our systems and data, all employees are required to secure their workstation, application, or device by fully logging out and/or locking the device or application whenever the employee is not actively using said technology.

Employees are prohibited from using District technology for improper purposes, including, but not limited to:

1. Access, post, display, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive
2. Disclose or in any way cause to be disclosed confidential or sensitive District, employee, or student information
3. Engage in personal commercial or other for-profit activities
4. Engage in unlawful use of District technology for political lobbying
5. Infringe on copyright, license, trademark, patent, or other intellectual property rights
6. Intentionally disrupt or harm District technology or other District operations (such as destroying District equipment, placing a virus on District computers, adding or removing a computer program without permission, changing system settings, etc.)
7. Install unauthorized software or run unauthorized operating systems or utilities
8. Engage in or promote unethical practices or violate any law or Board policy, administrative regulation, or District practice
9. Attempt to avoid district internet protections and filter systems by utilizing proxies, VPN, or any other means to circumvent these protections

Privacy: Since the use of District technology is intended for use in conducting District business, no employee should have any expectation of privacy in any use of District technology or systems accounts at any time.

The District reserves the right to monitor and record all use of District technology, including, but not limited to: access to the internet or social media, communications sent or received from District technology, posts on district social media sites, or other uses within the jurisdiction of the District.

Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to: record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of District technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any District technology are the sole property of the District. The creation or use of a password by an employee on District technology does not create a reasonable expectation of privacy. All individually-created passwords must meet district password requirements and be sufficiently complex to protect District systems, applications, and data. Typically, this means that a password, at minimum, should be 8-12 characters long, contain upper and lower case letters, a number, and a symbol, or a passphrase.

Student Data Privacy: District employees should have/request authorization to use applications and software utilities in support of students or academic goals prior to the purchase, installation or use of said software. Employees who use software/applications without the proper authorization may be subject to personal liability due to any data breaches or other damages related to the use of unapproved software.

Proper authorization to use a particular software or application requires an accompanying National Data Privacy Agreement (NDPA), or equivalent privacy governing document approved by the District in writing, that has been verified and executed by District leadership holding the necessary signatory authorization. Privacy agreements must be in place prior to the purchase, use or installation of the software or application.

Personally Owned Devices: Personally owned devices must only be joined to approved District network(s) after obtaining proper approval through the Technology Services department helpdesk support system. There is no expectation of privacy when accessing District systems or technology resources using District-issued accounts on a personal device.

No District or school records should be maintained or stored on any personal devices. Messages and other content accessed, sent or received on a personal device that is being used to conduct District business may be subject to disclosure pursuant to a subpoena, public records, or other lawful request.

Records: Any electronically stored information generated or received by an employee which constitutes a District or student record shall be classified, retained, and destroyed in accordance with BP/AR 3580 - District Records, BP/AR 5125 - Student Records, or other applicable policies and regulations addressing the retention of District or student records.

Reporting: If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of District technology, the employee shall immediately report such information to the Superintendent or designee.

Consequences for Violation: Violations of the law, Board policy, or this Acceptable Use Agreement may result in revocation of an employee's access to District technology and/or disciplinary action, up to and including termination. In addition, violations of the law, Board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Employee Acknowledgment: I understand that I shall have no expectation of privacy when using District computing equipment or technological resources, including but not limited to District provided email, file storage systems, software or applications, and other communication and collaboration services.

I further understand that any violation of district or board policies may result in revocation of user privileges and/or disciplinary action up to and including termination and/or appropriate legal action.

I also understand that any electronically stored information generated or received by an employee which consists of District student records shall be classified, retained or destroyed in accordance with BP/AR 3580. As such, I understand this may include such data being removed from technology devices or associated accounts or applications by District personnel.

I understand that if I use a personally owned device to access District technology systems or conduct District business, I shall abide by all applicable Board policies, administrative regulations, and the terms of this Technology Acceptable Use Agreement. I understand that content accessed, sent or received on a personal device that is being used to conduct District business may be subject to disclosure pursuant to a subpoena, public records request, or other lawful request.

I also understand that in order to comply with state and federal student privacy laws, I will not allow people who are not District employees (such as parents, volunteers or students) to use or access my District issued computing device, software, or applications, since confidential or protected student information or sensitive District email communications may be stored or access from there.

I hereby release the District and its personnel from any and all claims and damages arising from my use of District technology or from the failure of any technology protection measures employed by the District.

I have received, read, understand, and agree to abide by this Acceptable Use Agreement, BP 4040 - Employee Use of Technology, and other applicable laws and District policies and regulations governing the use of District technology.

Full Name: _____

Position: _____

School/Work Site: _____

Signature

Date