West Park School District
Employee Use of Technology

This policy is not intended to exhaustively enumerate all possible uses or misuses. These guidelines are subordinate to local, state and federal statutes.

The District provides technological resources (i.e., computers, Internet and Intranet access, server-based storage, local and web-based applications, mobile devices, e-mail and voice mail) to support the educational plan of the District

A. General Use

1. Employees shall be responsible for the appropriate use of technology and shall use the District's technological resources primarily for purposes related to their employment and consistent with the objectives of the District.

2. Employees should never allow their computers to be used by students or non-District employees for any purpose or at any time.

3. The Superintendent or designee may decide that particular uses are or are not related to employment or consistent with the objectives of the District.

B. Permitted Uses

Employees may use technology resources for the following purposes:

1. To communicate with outside researchers and educators in connection with research or instruction.

2. To communicate and exchange information for professional development, to maintain currency, or to debate educational issues.

3. For disciplinary, university, association, government, advisory, or standards activities related to the employees' research and instructional activities.

4. For any other administrative communications, applications or activities in direct support of research and instruction.

5. For interaction within the District as well as with other school districts or governmental agencies.

6. For posting or publishing instructional materials on web pages or certain sites on the Internet, so long as such postings and/or publication do not violate copyrights or the policies and procedures of CUSD.

7. For use in applying for or administering grants or contracts for research or instruction.

8. For limited communication incidental to otherwise acceptable use, except for illegal or specifically unacceptable use.

C. Prohibited Uses

Employees may not use technology resources for any inappropriate use at work or at home. The District may use forensic software to analyze suspected violations of the Employee's Use of Technology Agreement. Unacceptable use of the District's technology resources include, but are not limited to the following:

1. Promoting unethical practices or any activity prohibited by law, Board Policy or Administrative Regulations.

2. Accessing, posting, submitting, transmitting, publishing or displaying harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

3. With malicious intent, renaming, or making unusable any systems or services or anyone else's computer files, programs or media storage systems.

4. Without prior authorization, accessing another's system, resources, materials or password.

5. Advertising for personal profit.

6. Selling or purchasing illegal items or substances.

7. Introducing destructive or disabling software (bugs, viruses, worms, etc.).

8. Subscribing to online fee-based services charged to the District without prior written approval from administration.

9. Tampering with computers, networks, printers or other associated equipment.

10. Remailing or use of "anonymous" or "aliases" to protect or conceal individual identities while using District information technology systems or equipment.

11. Attempting to circumvent District security measures and systems including, but not limited to web filters and firewalls.

12. Sending mass electronic mail messages on an "All District" basis without prior consent from the appropriate designated administrator.

13. Placing software on the District's network hardware, computer hardware, or peripherals that have not been District certified.

14. Unauthorized transmission of confidential/identifiable information about students, employees or District operations information. Authorized transmissions outside of the District must be secure and encrypted.

15. Using a mobile device while operating a motor vehicle unless the mobile device is hands-free approved.

16. Use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

17. Posting information that could cause damage or danger of disruption.

18. Engaging in personal attacks, including prejudicial or discriminatory attacks such as "cyberbullying."

19. Harassing another person. Harassment is persistently acting in a manner that distresses or annoys another person.

20. Knowingly or recklessly posting false or defamatory information about a person or organization.

21. Accessing, transmitting or downloading large files, including “chain letters” or any type of “pyramid schemes.”

22. Using District internet or intranet property for personal benefit or for political activity.

23. Using the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

24. Gaining unauthorized access to a District system, another staff member’s computer or files by any means, including the use of keyloggers or related software utilities.

25. Sending chain e-mail messages.

26. Storing documents, pictures, or photos that are of a sexual nature or otherwise inappropriate.

27. Surfing the Internet, playing online games, or using P2P applications during duty time.

28. Downloading or installing software without the required license agreements in violation of copyright or licensing requirements.

D. Public Records

1. Information stored on the District’s information and communications systems and equipment, including e-mails, e-mail attachments, web postings, and voice mail messages may become records of the District. All permanent or archived District records, whether paper or computerized, may be considered public records and governed by the California Public Records Act (PRA).

2. Electronic mail is not intended for permanent storage. Electronic mail in-boxes and out-boxes may be purged on a minimum 90-day basis by the District's Technology Department. Electronic mail is not backed-up on a permanent basis and is archived for a one year period of time. The District stores electronic mail only to the degree that allows the District to restore current electronic mail in the event of a system failure. It is the responsibility of employees to back-up any electronic mail they want to access, or that is required to be kept by law, on a permanent basis. If electronic mail exchanges need to be retained as permanent or interim records, they should be printed and filed accordingly.

3. The District reserves the right to access and disclose all messages and other electronic data sent over its electronic mail system or stored in its files.

4. The District has the right to delete or retain any or all electronic files including e-mail of a District employee who is no longer employed by the District.

E. Confidential Information, Student Data and Privacy

During the course of normal school business some employees deal with confidential or identifiable information for staff or students.

1. Employees shall exercise caution when sending confidential information on the e-mail system because of the ease by which such information may be transmitted or intercepted.

2. Identifiable staff or student data and/or confidential information sent outside of the District must be authorized by the appropriate designated administrator..

3. Care should be taken in using e-mail to ensure messages are not inadvertently sent to the wrong individual.

4. Employees shall exercise caution when storing confidential information on their local hard drive and/or removable media due to the ease of copying or transmitting such information.

5. Employees shall exercise caution when posting confidential information on any file transfer protocol or website to make sure that site is a "secure" website.

6. Employees must have all agreements with outside vendors, especially those that require an extract of identifiable student data, to be reviewed and approved by administration for compliance with student privacy laws.

7. Employees may not permit identifiable information to be used for targeted advertising.

F. Disclosure of Student Information on District Websites

The following provisions address the disclosure of student information, posting student-created material, and posting pictures of students on the District web pages or District branded pages.

1. Group pictures without identification of individual students are permitted without parent approval.

2. If parents of students have given permission to release information, the following standards apply:

   a. Students will use a limited student identification (first name and last initial), or alternatively, first name only.

   b. Student work may be posted with limited student identification.

   c. All student posted work will contain the student's copyright notice using the limited student identification.

G. Internet and Intranet Services

1. The Technology Department has technical responsibility for setting up and managing Internet and Intranet resources, including user account maintenance.

2. District departments and school sites shall use the District's website for all Internet postings, and shall not initiate new or separate services outside of the District's designated services without the consent of the Superintendent or designee.

3. The decision of the Superintendent's office for appropriateness of materials and usage of Intranet and Internet services shall be final.

4. District departments and school sites have the primary responsibility to ensure timeliness and appropriateness of information posted on the District's Intranet or Internet web sites pertaining to their specific departments and school sites.

5. District departments and school sites shall designate a "content manager" for point of contact with the Technology Department.

H. Classroom, Team and Club Websites

The District recognizes the value of creating and maintaining District, school, classroom and other District-related websites. Employees authorized to create a District, school, classroom or other District-related website are considered the author of said site and shall adhere to the following procedures:

1. It is recommended that only approved, District hosted web services are used to create and maintain classroom, team or club websites. However, if an outside hosting service is used, all District policies continue to apply to the web site.

2. No web mechanism or tool may be used to create a financial benefit for any individual or group.

3. Fundraisers for club or team web sites are allowable in accordance with District policy and prior approval, but include the prohibition of all pay-per-click affiliate advertising programs (e.g. Google AdSense, Microsoft Bing/Yahoo, Criteo ClickZ, etc.).

4. Only District employees are allowed to create, edit or maintain web sites representing District schools, classrooms and/or organizations. Students, parents and subcontractors are not permitted to have access to edit or add content to District or District-affiliated websites.

    a. Student created content is acceptable, but must be provided electronically to the designated District employee for review. Only District employees may directly post content to District or District-affiliated sites after said review.

5. Links and embedded content must be free of copyright infringement, educational in nature and appropriate to the purpose of the web site.

6. Back up and restoration of web site content is the sole responsibility of the site author.

I. Intellectual Property Rights

1. District employees shall not post material on Intranet or Internet services or send material via e-mail which is copyrighted by a party other than the District.

2. District employees shall not download copyrighted materials without prior written consent from the person or entity that owns the copyright.

3. District employees shall not install unlicensed copyrighted materials on their computers.

4. District employees should not install any software on their computers without prior consent of the Technology Department.

J. System Use and Maintenance

Staff should remove or erase their email and/or other files from the District file servers regularly. Information that must be retained in the Education Code as a "Class 1 – Permanent" or "Class 2 – Optional" record should first be printed and filed accordingly by the employee. E-mail or other files stored on District servers are not considered private property and may be removed by the Technology Department.

1. Class 1 Permanent Records are defined in Section 16023 of the Title 5 of the Education Code. Examples in the Education Code include:

a. Annual Reports

b. Official Actions and Minutes of the Governing Board or Committees thereof c. Personnel Records

d. Student Records

e. All records pertaining to any accident or injury involving a minor for which a claim has been filed

f. Property Records

2. Class 2 Optional Records are defined in Section 16024 of the Title 5 of the Education Code as “Any record worthy of temporary preservation but not classified as Class 1 – Permanent may be classified as Class 2 – Optional and shall then be retained until reclassified as Class 3 – Disposable. If the Superintendent and Governing Board agree that classification should not be made by the time specified in Section 16022, all records for the prior year may be classified as Class 2 – Optional pending further review and classification within one year.”

K. Security

The District’s information technology system shall be protected from intrusion from outside sources, as follows:

1. The District shall construct firewalls to prevent outside sources from gaining access to the District system except when authorized by the Technology Department.

2. Employees will immediately notify the system administrator if they have identified a possible security problem. Employees are not to go looking for security problems, because this may be construed as an illegal attempt to gain access.

3. The public shall not have direct access to the District’s Intranet servers. All public access will be through the Internet server.

4. Sensitive student and employee information shall be transmitted only through secure connections.

5. Attempts by employees to disable, defeat, or circumvent any District facility, regardless of the success or failure of the attempts are prohibited.

6. Employees must not attempt to access any data or programs for which they do not have authorization or explicit consent.

7. Access to District information technology equipment must be properly documented, authorized and controlled.

8. Computers that the Technology Department has deemed unsafe, unmanageable, unpatchable should not be connected to the network or kept in use due to security risks.

9. Prohibited activities include, but are not limited to the following:

a. Attempts by employees to decrypt operating system, network, application and/or remote system passwords.

b. Attempting to gain unauthorized access to the District data network or to any other computer system through the District data network or going beyond the employee's authorized access. This includes attempting to log in through another person's account or access another person's files.

c. The copying of District network security, operating system security, and/or configuration files.

d. Any attempt to unlawfully secure a higher level of privilege than assigned on any District network or system.

e. Using District information and communications systems or equipment to gain or attempt to gain unauthorized access to other communication systems (hacking).

f. Using District information and communications systems or equipment to connect to a system in order to circumvent the physical security limitations of another system.

g. Any intentional attempts to infiltrate, sabotage, disrupt, disable, or "crash" any network system or program.

h. The willful introduction of computer "viruses," "worms," "Trojan horses," "trap-door code," "denial of service attacks" or any other disruptive programs into the District's computer system or network.

L. Cloud Computing

Cloud computing is a general term for anything that involves delivering hosted services over the Internet by a third party. Cloud computing entrusts remote services with a user's data, software and computation. The District will adopt appropriate guidelines for cloud computing use as technology changes rapidly and capabilities are expanded.

1. All cloud services reserve the right to monitor communications transmitted through their services. As a result, all information placed on the cloud system provided by the District should be considered open and available to the public in perpetuity.

2. Employees who use the cloud service provided by the District should expect to be subjected to advertisements as a related cost of the service.

3. In order to protect student and employee confidential records, cloud services must only be used to store student and teacher files for educational and learning purposes.

    a. All employees who use the cloud service must never upload confidential student records information including, but not limited to, contact information, IEP language, transcripts, discipline records, 504 documentation, accommodations or modification language, or grades.

    b. All employees who use the cloud service must never upload confidential personnel information including, but not limited to, contact information, evaluations, discipline records, employment history, coaching memos, or letters of reprimand.

M. Reporting Misuse

Employees must immediately notify their supervisor or appropriate designated administrator once they identify a possible security problem or breach of District Policy.

N. Accounts and Passwords

1. Employees must obtain an authorized domain account and password from the Technology Department to access technology resources.

2. Employees may be required to change their password for this account a minimum of once per semester.

3. Accounts and passwords are confidential and shall not be shared with any other person.

4. Passwords should be created with the intent of being difficult to decipher or guess. A strong password should contain a minimum complexity of eight (8) characters including a combination of alpha characters, numeric characters, and symbols.

O. Purchasing of Technology Equipment and Software

1. All purchases of computer hardware, software and/or peripherals for use on District computers must be pre-approved by the Technology Department.

2. All commercial software used on District Information Technology systems are copyrighted and designated for District use. Employees must abide by license agreements.

P. Limitation of Liability

1. The District cannot guarantee the functions or services provided through the District's data network will be without error. The District will not be responsible for any damage employees may suffer, including but not limited to, loss of data, interruption of service or exposure to inappropriate material or people. The District is not responsible for the accuracy or quality of the information obtained through the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system. Employees can be held financially responsible for any harm that may result from their intentional misuse of the system.

2. Employees should use the information technology resources in the workplace at their own risk with no expectation of privacy or confidentiality.

Q. Acknowledgement

Each employee who uses any District technology resources must annually acknowledge receipt and understanding of this Governing Board Policy. A record of this acknowledgment will be maintained in the employee's personnel file. Inappropriate use shall result in a cancellation of the employee's user privileges, disciplinary action and/or legal action in accordance with law, Board Policy and Administrative Regulations.

R. Equipment

Employees are responsible for returning all District issued equipment including, but not limited to, computers, tablets, mobile devices, and associated accessories, in reasonable working condition when employment ends or as equipment is updated. Employees must keep their equipment locked up and secure when not attended. Employees must never leave equipment in an unlocked classroom, visible in a parked car or in any other similar situation. Lost, stolen, or damaged equipment will be the financial responsibility of the employee. Failure to return District equipment or failure to pay for lost, stolen, or damaged equipment will result in legal action.

Adopted: Apr 10, 2023
Amended: