

## *PUSD Technology Procedures*

1. Acceptable Use Policy
  - How administered
  - How enforced
  - Filtering in compliance with NCLB
  
2. Purchasing:
  - Procedures
  - Standards for purchasing/hardware and software.
    - With district/site funds.
    - With other funds (donations/teacher purchase)
  
3. Maintenance:
  - Who is responsible for maintenance? Who pays for what?
    - Equipment purchased by district funds
    - Equipment purchased by site funds
    - Equipment purchased by other funds or donations
  - Equipment disposal
  
4. Hardware/software Upgrade/replacement plan
  
5. District Technology support procedures
  - Tech Help desk, work order process
  - Priorities
  
6. Teacher Access Policy
  - Network privileges for downloading and installing software
  - District email to be used as a site/district communication tool
  - “No expectation of privacy” clause in teacher contract
  - Individual teacher web pages, podcasts, wikis, and blogs
  
7. District and Site Tech Plans
  - District responsibilities
  - Site responsibilities
  
8. Technology staff development
  - District
  - Site

## 1. Acceptable Use Policy:

### 1.1 Student Policies

The Paradise Unified School District requires that all students accessing the Internet have a Student Network Responsibility Contract (Appendix 1) signed by the student and parent or legal guardian on file with the school. The contracts will be issued as part of the student registration packet sent home for signatures at the beginning of each school year. Each school site will develop a procedure to monitor student compliance with the contract and Acceptable Use Policy terms.

In addition to the legal issues, students may not:

- Use school computers when unsupervised
- Install software, play personal CD's, or download applications
- Attach electronic devices or storage devices, including USB drives or iPods
- Attempt to bypass security systems or network filters
- Visit chat rooms or post personal information on any site on the web
- Use PDA's, MP3 players or other electronic listening, recording, or communicating devices during classroom hours without the permission of the teacher.
- Cell phones and pagers must be turned off and out of sight during classroom hours. Violation of these rules is grounds for confiscation, and the devices will be returned to the parent or guardian.

### 1.2 Staff Policies

All PUSD employees must comply with District Policies as stated in the Use of Technology Agreement (*Appendix 4*).

Additionally, PUSD employees are requested to abide by the following policies to maintain the integrity of our system and minimize technical support problems.

#### DO

- Log in properly on a computer and log out when you leave the workstation.
- Keep personal use of the network to a minimum during school hours
- Use district databases appropriately to protect the privacy of students and staff; confidential information may be shared only with authorized personnel.

#### DO NOT

- Publish or post on a web page a student's personal information, photo, artwork, or writing without parent/guardian written permission in compliance with the district parent permission form (*Appendix 2*). THIS IS A SERIOUS LEGAL ISSUE.
- Reveal a password entrusted to you. If it becomes compromised, report it to your site technician or representative.
- Install network or wireless devices without consulting with the site or District Technology Department, as you will affect the entire network and may disrupt its use.

- Install hardware or software without the knowledge and consent of the site or District Technology Department. All installed software must be legally licensed and compatible with the workstations and network. Copyright infringement is a serious matter and could result in fines of thousands of dollars.
- Download programs such as Napster or Kazza. They enable downloading of pirated materials and drain the bandwidth of the network.
- Take school equipment home without the knowledge and express permission of the site administrator. You will be personally liable for repair or replacement of any equipment damaged or lost when in your possession off site.

## **2. Purchasing**

### **2.1 Procedures**

Any hardware or software purchases should be made through the District Technology Department. This will ensure that the school will obtain the best price and that the item is compatible with the existing network and hardware of the school site and district. Unauthorized personal purchases will not be reimbursed by PUSD.

### **2.2 District/Site funds**

District funds may be used to support district-required services, such as the implementation of Aeries, the student information system. Site funds, including site grants and School and Library Improvement Block Grants, (SLIP) funds, are to be used for site priorities, and are to be allocated by site-determined protocols, such as School Site Council decision-making. The District Technology Consultant or District Technology Coordinators shall be consulted for purchasing recommendations.

### **2.3 Donations and teacher purchasing**

The District Technology Consultant or District Technology Coordinators of the District Technology Department will review all donated or staff purchased used hardware and software for appropriate compatibility with the district network.

The District Technology Consultant or District Technology Coordinators of the District Technology Department will review and or remove any existing and aging computer hardware and software as needed for compatibility with the current district network.

The school district will accept hardware that meets minimum standards required for compatibility with existing hardware and infrastructure. While other equipment is tempting to accept, the cost of configuration and support as well as the impact on the school site precludes its use. Additionally, all hardware must be verified to be free of computer viruses, spy ware, Trojan Horse files, etc. that can potentially compromise the security of the network. Donated software must also be approved for copyright issues and the reasons stated above.

The District does not support personal inkjet printers. Ink costs and high maintenance requirements preclude their use; a “free” printer may require \$50 in technical time to configure and another \$50 when it malfunctions. Laser printers typically cost a penny a page, while inkjets run approximately \$.05 per page.

Teachers who wish to connect their personal computers to the network must first obtain approval from a member of the District Technology Department. Approval is based on the computer's compatibility with the network, submission of the computer for virus and spy ware checking, and compliance with Internet filtering under the Child Internet Protection Act, (CIPA). Again, use of this computer requires costly technical support and time.

### **3. Maintenance**

#### **3.1 Persons responsible for paying for and maintaining equipment**

The District provides technical support by funding the District Technology Consultant and a part-time assistant as needed. The two Library/Technology Coordinators also play a limited role in technical support. District technicians will continue to primarily support servers and network issues.

The District provides sites with WAN access through BCOE, the District's contracted service provider, and funds the T-1 lines connected to the DS3 fiber line distributed through Paradise High School.

As technology use continues to expand, sites will need to explore funding to meet day-to-day maintenance demands. Sites may contract with BCOE for some workstation maintenance. Paradise High School and Ridgeview currently contract with them on an hourly basis to provide technical support.

Equipment purchased with other funds or donations must comply with purchasing procedures and standards as outlined in section 2,

All District equipment shall be identified with a district-assigned asset number engraved on the hardware. The number will be maintained in a district database with necessary information for insurance purposes.

#### **3.2 Equipment disposal**

Equipment disposal requires notification of a District Technology Department representative and must comply with legal requirements for toxic substances. Computer monitors, for example, must be disposed of at hazardous waste collection sites. Tech department representatives must ensure that the discarded item is removed from the asset database.

### **4. Hardware/Software Upgrade and Replacement**

The district and individual site leaders should collaborate to create a process of hardware and software upgrading and replacement, including licensing of the student information system Aries and the library circulation system Athena. Funding sources will need to be identified and targeted to specific needs. Ideally a percentage of older equipment can be discarded and replaced annually to maintain the viability of the technology available to students and staff in order to meet state-mandated technology standards.

### **5. District Technology Support Procedures**

#### **5.1 Tech Help Desk Work Order Process**

The district utilizes an online technology help desk in which a designated representative at each school site will log technology requests. Work orders shall be completed by the requestor and submitted to the representative; no work will be completed without a submission to the help desk (Appendix 3). This will ensure a record of the work, its priority, the person responsible for completing the work, and a completion time. Tracking work orders will also allow the district to evaluate technical support needs and priorities.

### 5.2 Technology Support

The technology support provided district employees is limited to district authorized, school hardware, software, and online accounts that are properly licensed. District support does not extend to home computer interface with district provided technology.

### 5.3 Priorities

Priorities are determined by the nature of the work to be done. Network issues that impact an entire site or the functionality of a site naturally take priority over workstation issues. Additionally, server and server software, such as the student information system Aries, take precedence over other work.

## 6. Teacher Access Policy

### 6.1 Network access and the Children’s Internet Protection Act, (CIPA)

In compliance with the Children’s Internet Protection Act, (CIPA), the district utilizes a filter to block inappropriate web sites within categories such as pornography, graphic violence, drugs, alcohol and tobacco, gambling, personals, chat rooms, and games. Such sites are deemed inappropriate for school, potentially endanger students, or cause classroom distractions. If a blocked site is essential to the learning process and does not violate the intent of CIPA, an instructor may submit a work order to the tech help desk as outlined in 5.1 to have the site evaluated by the technology department for possible unblocking.

### 6.2 Download/Install Software

If an instructor wishes to download and install software, a work order must also be submitted for a technician to do the work to ensure the software is legally licensed, free of viruses and spy ware, and is compatible with the operating system and network infrastructure.

### 6.3 Employee web pages, wikis, and blog sites

Employees are required to submit links to all web pages and blogs to the technology department. Additionally web pages and blogs are to be linked to the district and school site web pages.

Employees are required to obtain and retain signed “Parent Permission Form for World Wide Web Publishing of Student Work” prior to any student web publishing (*Appendix 2*).

### 6.4 District email

All staff will be given a district email account and will be required to check it regularly for school purposes. District and site information will be disseminated in this manner, as it becomes an increasingly essential communication tool.

### 6.5 Privacy

As stated in the “PUSD Use of Technology for Employees” policy, to be signed annually, (Appendix 4), there is a “no expectation of privacy” clause that asserts the District’s right to

“monitor any and all aspects of its computer system and networking including, but not limited to, monitoring any employees’ use of the Internet, chat groups, news groups, web pages, podcasts, wikis, and blogs, reviewing material downloaded or uploaded by any employee, reviewing email sent and received by employees, and any document or data stored on the computer...” Current federal law mandates all electronic transmissions, data, and district email be archived.

## **7. District and Site Technology Plans**

### 7.1 District and Site Responsibilities

PUSD Library/Technology coordinators are responsible for annual review and revision of the state and school board approved District Technology Plan. This plan is developed, updated and reviewed by site administrators and/or site technology representatives and approved by the district technology coordinators.

Each school site will have a site technology plan in compliance with the district plan to define site needs and program improvement activities. The district library/technology coordinators will consult with site stakeholders in plan development. Site principals and site councils are primary stakeholders. This plan shall be an addendum to the single school plan for student achievement and updated annually. Completion deadline of site plans is early November in order to coordinate with Accountability Report.

## **8. Technology Staff Development**

### 8.1 District Responsibilities

The District shall provide staff development opportunities in accordance with District goals and objectives as appropriate.

Technology training will include but not be limited to:

- Teacher personal productivity
- Teaching students to use technology
- Integrating technology into the curriculum

### 8.2 Site Responsibilities

Sites may offer staff development opportunities to meet site and/or district goals and objectives within the same guidelines as outlined in 8.1. The Superintendent or an Assistant Superintendent must approve site staff development offerings for district staff development credit.

# Appendix

1. Student Network Responsibility Contract (*See attached*)
2. Parental Release Form for publications
3. PUSD Technology Work Order
4. PUSD Use of Technology for Employee

**PARADISE UNIFIED SCHOOL DISTRICT**  
 Parent Permission Form for  
 World Wide Web Publishing of Student Work

Name of Student \_\_\_\_\_

Teacher/Classroom \_\_\_\_\_

As part of our Internet program in the Paradise Unified School District, we would occasionally like to use student artwork, writing or photos on a page on our web site. In order to publish student artwork, writing or photos, we need to have parent/guardian permission.

These guidelines will be followed:

- No individual photos of your child will be published without additional consent.
  - No personal information about the students, such as last name, home address or telephone number, will be published.
  - All student work and/or photos will appear with a copyright notice prohibiting the copying of student work and/or photos without express written permission.
  - If anyone should request such permission, those requests will be forwarded to the child and his/her parent/guardian.
  - The copyright of the work will still belong to the student.
  - A copy of all student work that is published to the Internet will be made available for parental viewing.

Please check (✓) as appropriate:

I understand that my child's artwork, writing and/or class or group photo will be considered for publication on the World Wide Web (WWW), a part of the Internet.

Yes	No	I grant permission for the WWW publishing based on the guidelines listed above. (Please check either yes or no for each of the following.)
<input type="checkbox"/>	<input type="checkbox"/>	My child's work
<input type="checkbox"/>	<input type="checkbox"/>	My child in a group or class photo

Parent Name (please print) \_\_\_\_\_

Parent Signature \_\_\_\_\_ Date \_\_\_\_\_

I, the student, also give my permission for such publishing:

Student Signature \_\_\_\_\_ Date \_\_\_\_\_



# PARADISE UNIFIED SCHOOL DISTRICT

## Use of Technology by Employees

PUSD provides computers and computing facilities and other technology to students, faculty and staff. All persons, employees, independent contractors, consultants, etc., who use these facilities and equipment shall at all times be governed by established policy and guidelines (Board Policy and Regulation 4040). This applies to all computers owned, leased, or in the possession of PUSD and shall also govern all use independent of the location from which these facilities are utilized.

### **DO**

- Comply with PUSD policies and state and federal laws
- Use personal and professional courtesy and consideration in e-mail
- Use district databases appropriately to protect the privacy of students and staff; confidential information may be shared only with authorized personnel.
- Follow precautions recommended to protect system passwords
- Ask if you are unsure about policy or procedures
- Comply with copyright laws

### **DO NOT**

- Use a computer account or password you are not authorized to use
- Use the PUSD network to gain unauthorized access to any computer system, server or network
- Knowingly or negligently perform an act which will interfere with the normal operation of computers, servers, peripherals or networks
- Run or install on any computer system or network a program intended to damage or place excessive load on the system
- Attempt to circumvent data protection schemes or uncover security loopholes
- Use e-mail to harass others
- Violate software license agreements, copyright laws, or provisions of PUSD policy
- Mask the identity of your account or activities on the network

### **NO EXPECTATION OF PRIVACY**

You have been authorized to use a computer, various software, and an Internet connection in the performance of your duties for the District. The computer, software, and all stored data are the property of the District which may access the computer software and data at any time. The District has the right to monitor any and all aspects of its computer system and network including, but not limited to, monitoring employees' use of the internet, chat groups, news groups, web pages, podcasts, wikis, and blogs, reviewing material downloaded or uploaded by any employee, reviewing e-mail sent and received by employees, and any document or data stored on the computer. Pursuant to federal law, electronic transmissions, data, and district email will be archived. The employees do not have any right to privacy in anything on the computer or in anything they create, store, send or receive on the computer or the Internet. No employee has any expectation of privacy with respect to any computer (or software or data thereon) which is owned by the District or used by the employee in the performance of the employee's duties for the District.

*I have read and understand the above.*

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

10/05/05