Technology Security Plan

Freedom Preparatory Academy

Freedom Preparatory Academy (FPA) supports secure network systems, including security for all personally identifiable information that is stored on paper or stored digitally on FPA-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the district, schools, students, or employees at FPA.

FPA will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the FPA network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of devices on the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the network administrator with the relevant information.

This policy also covers third party vendors/contractors that contain or have access to FPA critically sensitive data. All third-party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing our systems or receiving information.

It is the policy of Freedom Preparatory Academy to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq. and Utah Administrative Code R277-487.

The Administration directs the FPA IT Director to develop procedures to support this policy. Employees are required to follow the procedures developed by the IT Director. Professional development for staff regarding the importance of network security and best practices is to be included in the procedures. Students are also required to follow the procedures as applicable. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network. The Administration supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect data, users, and electronic assets.

FPA Security Procedures

Definitions

Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

Encryption or encrypted data: The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered Protected data

Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

Sensitive data: Data that contains personally identifiable information.

System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Security Responsibility

District IT security shall be the primary responsibility of the District IT Department, led by the IT Director. The IT Department shall be responsible for the development of policies and adherence to the standards defined in this document.

Employee Security Awareness Training

1. Overview

Freedom Preparatory Academy, led by the IT Director, shall ensure that all employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all employees.

2. Purpose

These methods help ensure employees have a solid understanding of our security policy, procedures, and best practices. Employees shall also have a basic understanding of the following security related topics: email and messaging security, safely browsing the internet, social networking threats, mobile device security, password best practices, data classification, data transmission and encryption, data destruction, WiFi security, working remotely, insider threats from students and staff, physical security

issues, protecting personal/work computers, copyright infringements, malware and virus protection, sharing files with local and state entities, and workspace security.

3. Procedure

All FPA employees shall receive security specific trainings Annually.

Security for Workstations

1. Overview

The workstations at FPA contain sensitive information and data. FPA IT Department will implement procedures to ensure that this information will be secure.

2. Purpose

FPA shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.

3. Procedure

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information; including personally identifiable information (PII) and that access to sensitive information is restricted to authorized users.

- FPA employees using controlled workstations shall consider the sensitivity of the information, including personally identifiable information (PII) that may be accessed and minimize the possibility of unauthorized access.
- FPA will implement physical and technical safeguards for all workstations that access electronic personally identifiable information (PII) to restrict access to authorized users.
- Appropriate measures include:
    - Restricting physical access to workstations to only authorized personnel.
    - Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
    - Enabling a password protected screensaver with a 15 minutes or less to ensure that workstations that were left unsecured will be protected. The password must comply with FPA Password Procedure.
    - Complying with all applicable password policies and procedures. See FPA Password Procedure.
    - Ensuring controlled workstations are used for authorized business purposes only. Never installing unauthorized software on controlled workstations.
    - Storing all sensitive information, including personally identifiable information (PII) on secured network servers

- Securing laptops that contain sensitive information by locking laptops up in drawers, cabinets or in a classroom/office.
- Users are not set up as computer administrators

Network Security

1. Overview

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network. The primary goals of network security are Confidentiality, Integrity, Availability and Accountability.

2. Purpose

The minimal security configuration required for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Freedom Preparatory Academy. FPA shall ensure that all untrusted and public access computer networks are separated from main computer networks and utilize security policies to ensure the integrity of those computer networks. FPA will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

3. Procedure

Network perimeter controls will be implemented to regulate traffic moving between trusted internal (FPA) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

Wireless Network Security

1. Purpose

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network. The primary goals of network security are Confidentiality, Integrity, and Availability.

2. Purpose

No wireless access point shall be installed on FPA computer network that does not conform to current network standards as defined by the IT Department. FPA shall scan for and remove or disable any rogue wireless devices on a regular basis. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA2 encryption for any connections. Open access networks are not permitted with the exception of a managed guest network.

3. Procedure

Wireless Network controls will be implemented to regulate traffic moving between trusted internal (FPA) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

Remote Access Procedure

1. Overview

Remote access allows a user to connect from outside the FPA organization network. This procedure applies to all FPA employees, contractors, vendors and agents with a FPA owned or personally owned computer or workstation used to connect to the FPA network. This procedure applies to remote access connections used to do work on behalf of FPA

2. Purpose

The purpose of this procedure is to define standards for connecting to FPA network from any host. These standards are designed to minimize the potential exposure to FPA from damages, which may result from unauthorized use of FPA resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical FPA internal systems, etc. Remote access implementations that are covered by this procedure include, but are not limited to DSL, VPN, and SSH.

3. Procedure

It is the responsibility of FPA employees, contractors, vendors and agents with remote access privileges to Freedom Preparatory Academy network to ensure that their remote access connection is given the same consideration as the user's on-site connection to FPA.

Please review the following procedures to ensure protection of information when accessing the FPA network via remote access methods, and acceptable use of FPA network:

- Encryption Procedures
- Wireless Infrastructure Communications Procedure
- Acceptable Use Procedure

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass phrases. For information on creating a strong pass phrase see the Password Procedures.
- At no time should any FPA employee provide his or her login or email password to anyone, not even family members.
- FPA employees with remote access privileges must ensure that their FPA owned or personal computer or workstation, which is remotely connected to FPA network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- The FPA director must approve non-standard hardware configurations. Security configurations for access to hardware must also be approved.
- All hosts that are connected to FPA internal networks via remote access technologies, must use the most up-to-date anti-virus software, this includes personal computers.
- Personal equipment that is used to connect to FPA networks must meet the requirements of FPA owned equipment for remote access.

- Organizations or individuals who wish to implement non-standard Remote Access solutions to the FPA production network must obtain prior approval from FPA director.

Password Procedure

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the entire network. This guideline provides best practices for creating secure passwords.

2. Purpose

The purpose of this procedure is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. This procedure applies to all personnel and entities working on behalf of FPA, who have or are responsible for any account (or any form of access that supports or requires a password) on any system that resides at or is connected to FPA.

3. Procedure

To minimize the possibility of unauthorized access, all passwords should meet or exceed the guidelines for creating strong passwords.

Password Characteristics

Strong passwords

- Contain at least 10 alphanumeric characters
- Contain both upper- and lower-case letters
- Contain at least one number (for example, 0-9)
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

Protection of passwords

- Users must not use the same password for FPA accounts as for other non-FPA access (for example, personal email accounts, shopping sites, social media, and so on
- Where possible, users must not use the same password for various FPA access needs or user accounts that have system-level privileges granted through group memberships or programs such as FileMaker must have a unique password from all other accounts held by that user to access system-level privileges; unless account has 2-factor authentication enabled
- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually.
- Password cracking or guessing may be performed on a periodic or random basis by the UETN team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it
- Default passwords must be changed during initial setup and configuration

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information
- Passwords must not be inserted along with the username into email messages or other forms of electronic communication
- Do not reveal a password on questionnaires or security forms
- Do not share your FPA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption
- Never use the “Remember Password” feature of applications (for example, web browsers)
- Any user suspecting that his/her password may have been compromised must report the incident to their supervisor and change all passwords immediately

Access Control

1. Overview

Access control is the process of authorizing users, groups, and computers to access objects on the network or computer. It is a good practice to assign permissions to groups because it improves system performance when verifying access to an object.

2. Purpose

The purpose for setting access control in the FPA organization provides system and application access based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

3. Procedure

This procedure is directed to the IT Management Staff who is accountable to ensure proper access is given to individual employees.

- FPA shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.
- FPA shall ensure that user access should be granted and/or terminated upon timely receipt, and management’s approval, of a documented access request/termination.
- FPA shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.
- FPA shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

Security Response Plan Procedure

1. Overview

A Security Response Plan (SRP) provides the impetus for security and operational groups to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines.

2. Purpose

The purpose of this procedure is to establish the requirement that all operational groups supported develop and maintain a security response plan. This ensures that the security incident response team has all the necessary information to formulate a successful response should a specific security incident occur. This procedure applies any established and defined operational group or entity within the FPA.

3. Procedure

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the FPA director and network administrator.

Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

Triage

The SRP must define triage steps to be implemented with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact.

Disaster Recovery Plan Procedure

1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives FPA an advantage. This procedure requires management to financially support and diligently attend to disaster contingency

planning efforts. Disasters include but are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

2. Purpose

This procedure defines the requirement for a baseline disaster recovery plan to be developed and implemented by FPA that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. Procedure

This procedure is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up to date. This procedure is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub plans. The FPA director and IT director will develop the following contingency plans.

The following contingency plans must be created:

- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Data Backup: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- Restoration Plan: Describes how the backups are restored.
- Equipment Replacement Plan: Describe what equipment is required for providing services
- Critical Systems Instructions: Documentation must include:
    - Location of installation software
    - Backup frequency and storage locations
    - Username and passwords
    - Support phone numbers
    - Steps to restart, reconfigure, and recover the system
    - Power up and power down procedures
    - Equipment age
    - Model and serial numbers
    - Warranty and maintenance contract information
    - Software licensing information and storage location
    - IP and MAC addresses
    - Supplier contacts for sources of expertise to recover systems. These might include vendors that sell/support the products, or the manufacturers themselves
    - Website username and password
    - Server username and password

- Assigned computer username and password

Malicious Software Procedure

1. Overview

Malicious Software is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. It may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge.

2. Purpose

The purpose of the procedure is to ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.

3. Procedure

This procedure is directed to the IT Management Staff who is accountable to ensure the security of district networks and data.

- Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
- FPA shall install, distribute, and maintain spyware and virus protection software on all FPA-owned equipment, i.e. servers, workstations, and laptops.
- FPA shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.
- All computers must use the District approved anti-virus solution.
- Any exceptions to malicious software procedure must be approved by the Security Information Officer.

Internet Content Filtering Procedure

1. Overview

Internet content filtering is the use of a program or hardware to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable.

2. Purpose

The purpose of Internet content filtering is to provide best effort to protect students, teachers, and school employees from objectionable material.

3. Procedure

This procedure is directed to the IT Management Staff who is accountable to ensure that Internet content filtering best practices are implemented.

- In accordance with Federal and State Law, FPA shall filter internet traffic for content defined in law that is deemed harmful to minors.
- FPA acknowledges that technology-based filters are not always effective at eliminating harmful content and due to this, FPA uses a combination of technological means and supervisory means to protect students from harmful online content.
- In the event that employees take devices home, FPA will provide a technology-based filtering solution for those devices. However, the District will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content. FPA[1] will cut because we do not provide direct access to students.
- Students shall be supervised when accessing the internet and using district owned devices on school property. [2]

Data Privacy Procedure

1. Overview

Data can be used to facilitate change and improvement, there is however a need to balance the usefulness of this data with the privacy of who the data is about.

2. Purpose

The purpose of protecting data is to provide best effort to ensure that data breaches do not happen and to place into training and procedure steps to protect individuals.

3. Procedure

This procedure is directed to the IT Management Staff who is accountable to ensure that Privacy and data protection best practices are implemented. Data privacy within the district shall be in accordance with the district's Data Governance Plan.

- FPA recognizes its responsibility as the steward for all confidential information maintained within the district.
- FPA considers the protection of the data it collects on students, employees and their families to be of the utmost importance.
- FPA protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA") and Utah Administrative Code R277-487 ("Student Data Protection Act").
- FPA shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.
- FPA shall designate Data Stewards to oversee the collection, storage and maintenance of confidential information within the district. Data Stewards shall manage confidential information/data in accordance with the district's Data Governance Plan.
- All FPA board members, employees, contractors and volunteers shall undergo annual privacy training and shall be required to comply with the district's security policy.

Audit Procedures

1. Overview

Planned and random security audits are important in order to mitigate risk and evaluate our preparedness for a security incident. FPA contracts with UETN to conduct periodic security penetration tests using the CIS Critical Security Controls on devices and networks.

2. Purpose

The purpose of this procedure is to ensure all devices and network are configured according to the FPA security policy. All devices connected to the FPA network are subject to audit at any time. Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Ensure conformance to the FPA security policy

3. Procedure

FPA hereby provides its consent to allow the UETN security audit team or an external auditor to access its devices to the extent necessary, within a predetermined scope; which will be written and approved by the UETN team to allow the auditor to perform scheduled and random audits of any/all devices at FPA.

- Specific Concerns
- FPA devices may support critical business functions and store sensitive information. Improper configuration of devices could lead to the loss of confidentiality, availability or integrity of these systems
- Guidelines
- Approved and standard configuration templates shall be used when deploying devices:
    - Host security agents such as antivirus and malware protection shall be installed and updated
    - Perform network scans to verify only required network ports and network shares are in use
    - Verify administrative group membership
    - Conduct baselines when systems are deployed and upon significant system changes
    - Changes to configuration template shall be coordinated with FPA network administrator
    - Must follow all other applicable procedures for deployed new devices

4. Responsibility

The UETN Team or an external auditor shall conduct audits of all devices owned or operated by FPA. Device owners are encouraged to audit their own devices as needed; this does not allow a device owner to perform an audit of the FPA network or on any device not owned by the employee

5. Relevant Findings

All relevant findings discovered as a result of an audit shall be listed in the UETN report to FPA to ensure prompt resolution and/or appropriate mitigating controls

6. Ownership of Audit Report

All results and findings generated by the UETN team or an external auditor must be provided to appropriate FPA management within one month of project completion. This report will become the property of FPA and be considered confidential

Clean Desk Procedure

1. Overview

The purpose of this procedure is to establish a culture of security for all FPA employees. An effective clean desk effort, involving the participation and support of all employees, will protect paper documents that contain personally identifiable and other sensitive information.

2. Purpose

The primary reasons for a clean desk procedure are:

- A clean desk reduces the threat of a security incident since confidential information will be locked away when unattended.
- Sensitive documents left in the open can be viewed and/or stolen by a malicious entity.

3. Procedure

Appropriate measures must be taken to ensure the confidentiality, integrity and availability of sensitive information, including but not limited to Personally Identifiable Information (PII) or sensitive personal information(SPI).

Appropriate measures include:

- Restricting physical access to devices.
- Ensuring that all sensitive/confidential information in hardcopy or electronic form is secure in the work area at the end of each day.
- Securing workstations (screen lock or logout) prior to leaving an area to prevent unauthorized access.
- Enabling a password--protected screen saver with a short timeout period to ensure that devices left unsecured will be protected.
- Complying with all applicable password policies and procedures. See FPA Password Procedure.
- Ensuring devices are used for authorized educational/business purposes only.
- Never sending personally identifiable information (PII) or sensitive personal information(SPI) via email to anyone, including forwarding a message.
- Storing all sensitive information on password--protected drives or secure, restricted, network servers.
- Securing laptops that contain sensitive information by using cable locks, locking laptops up in drawers or cabinets, and/or by locking the door behind you.
- Sensitive working papers should be placed in locked drawers whenever a user is away from their desk.

- At the end of the work--day the employee is expected to tidy their desk by locking up all sensitive papers and devices.

Email Procedure

1. Overview

Electronic email is used pervasively, and is often the primary communication and awareness method within an organization. Misuse of email, however, can pose many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

2. Purpose

The purpose of this email procedure is to ensure the proper use of the FPA email system and make users aware of what FPA deems as acceptable and unacceptable use of its email system. This procedure outlines the minimum requirements for use of email within the FPA network.

3. Procedure

- All use of email must be consistent with FPA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices
- FPA email account should be used primarily for FPA business related purposes; personal communication is permitted on a limited basis, but non-FPA related commercial uses are prohibited
- The FPA email system shall not to be used for the creation or distribution of any disruptive or offensive messages; including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any FPA employee should report the matter to their supervisor immediately
- Users are prohibited from automatically forwarding FPA email to a third party email system.
- Using a reasonable amount of FPA resources for personal emails is acceptable. Sending chain letters or inappropriate joke emails from a FPA email account is prohibited
- FPA employees shall have no expectation of privacy in anything they store, send or receive
- FPA may monitor messages without prior notice. FPA is not obligated to monitor email messages

EMPLOYEE TECHNOLOGY ACCEPTABLE USE

Every FPA employee will be required to sign an acceptable use policy.

All employees are responsible for following FPA policy and procedures.

1. INTERNET & INTERNET USE:

FPA has access to the Internet, which is governed and supported by the Utah Education Network.

Use of the electronic information resources in FPA shall be to improve and support the educational process by providing access to global information and improving communication between our districts, employees of FPA, and community members. FPA desires to provide electronic mail service, electronic conferencing, global information resources via the World Wide Web, to employees of FPA at no cost.

2. ACCEPTABLE INTERNET USE

All Internet or computer equipment use shall be consistent with the purposes, goals, and policies of FPA. It is imperative that users of the Internet or computer equipment conduct themselves in a responsible, ethical, moral, and polite manner. All participants must abide by all local, state, and federal laws. The Internet user accepts the responsibility of adhering to high standards of conduct and the terms and conditions set forth in all parts of this policy.

3. IMPERMISSIBLE INTERNET & COMPUTER EQUIPMENT USES

The following uses of the Internet & computer equipment are prohibited:

- Any violation of applicable FPA policy or public law by such use;
- Any activity that is immoral or contrary to the high moral standards which must be maintained in an educational setting;
- Any attempt to bypass state, FPA, district, or school security (e.g. bypassing proxies or hacking servers or work stations) is forbidden;
- Accessing or transmitting of immoral, obscene, pornographic, profane, lewd, vulgar, rude, defaming, harassing, threatening, disrespectful, or otherwise inappropriate images or information, or receiving such information from others;
- Any commercial use, product advertisement, display of private information, or promotion of political candidates;
- Any violation of copyright, trade secret or trademark laws;
- Any attempt to damage, disrupt or interfere with the use of any computer electronic information resource;
- Any attempt to access information beyond the users authorized access to any electronic information resource;
- Any destruction, defacement, theft, or altering of FPA equipment;
- Any storing or accessing of illegal, inappropriate, or obscene material on FPA owned electronic equipment;
- Excessive non-work related computer use during work hours;

4. PRIVILEGE

The use of the Internet and computer equipment within FPA is a privilege. The information produced from Internet access or computer use shall be deemed the property of FPA, this is confidential information to the user unless it is transmitted to others with the user's permission. Violation of this policy can result in the loss of computer access privileges.

5. MONITORING

FPA reserves the right to monitor and review any material on any machine at anytime in order for the service center to determine any inappropriate use of network services.

6. DISCLAIMER OF ALL WARRANTIES

FPA makes no warranties of any kind, whether expressed or implied, for the services provided in connection with use of the Internet or any and all computer equipment. Neither FPA nor any supporting Internet services will be responsible for any damages that an computer or Internet user suffers. FPA expressly disclaims any liability in connection with the loss of data resulting from delays, failure to deliver data, mistaken deliveries, viruses, backup device failure, or service interruptions caused by FPA or the Internet provider or by the users error or omissions. Use of any information obtained via the Internet is at

the user's own risk. FPA expressly denies any responsibility for the accuracy or quality of information obtained through any Internet service. All users must consider the source of any information they obtain and evaluate the validity of that information.

7. SECURITY

FPA will implement security procedures on Internet access to protect against unacceptable use. Employees are responsible for the security of their computer equipment, files and passwords. Employees with access to student records may not use, release, or share these records except as authorized by Federal, State, or Local laws. Employees are responsible for any accounts they may have. Sharing of any usernames or passwords to anyone is not permissible and may result in the loss of account privileges. Employees will be held accountable for any activity under their user account. Any security violations by employees must be reported to Technology Specialist and Director.

8. ENCOUNTER OF CONTROVERSIAL MATERIAL

Internet users may encounter material that is controversial which the user or administrator may consider inappropriate or offensive. FPA has taken precautions to restrict access to inappropriate materials through a filtering and monitoring system. However, it is impossible on a global Internet, to control access to all data which a user may discover. It is the user's responsibility not to initiate access to such material. Any site or material that is deemed controversial should be reported immediately to the appropriate administrator. FPA expressly disclaims any obligation to discover all violations of inappropriate internet access.

9. TERMS OF USE

a. Only registered employees of FPA and Board of Directors members qualify for Internet access under this policy.

b. Only the authorized users who have signed the user agreement shall have computer access. Users are ultimately responsible for all activity while using the Internet and all computer equipment.

c. All Internet or computer equipment access by an employee or Board member is automatically terminated upon retirement, resignation, or termination of employment.

d. All student computer use must be supervised. Employees who supervise students with access to computer equipment must be familiar with the district's Student Computer Acceptable Use Policy and be willing to enforce it. Employees must appropriately secure rooms and areas where school computer equipment is housed.

10. PENALTIES FOR IMPROPER USE

Any violation of this policy or applicable state and federal laws may result in disciplinary action (including the possibility of termination) and/or referral to legal authorities. The Technology Specialist may limit, suspend, or revoke access to electronic resources at any time.

FPA INTERNET USER AGREEMENT

I understand and will abide by the FPA Employee Computer Acceptable Use Policy. I further understand that any violations of the above Computer Acceptable Use Policy, when using FPA electronic information resources, may result in the loss of my access privileges and/or other disciplinary or legal action. This action may include, but not limited to, suspension, probation, or termination of employment. I, therefore, agree to maintain professional standards and to report any misuse of the electronic information resources to the Technology Specialist or Director.

_____

Employee Name (Please Print)

_____

Employee Signature and Date