



**POLICY 350 - TELECOMMUNICATION ACCEPTABLE USE POLICY
AND STAFF SECURITY AGREEMENT**

1. Objective

The Board supports the use of the Internet and other telecommuting / computer resources in the district's education delivery environment, the student record keeping environment and the administrative environment of the District.

The District uses or may use the public Internet for: (List of uses that may include but are not limited to)

- Maintaining a web site that is currently used as an information-sharing device for the general public. Information sharing includes posting of schedules, event descriptions, posting of homework assignments, description of classroom activities and accomplishments.
- Email communication with parents, board members, PTA, vendors, other external business partners
- Distance Learning for staff and students
- Research by staff and students
- Communication with vendors and downloading of services and technology
- Partnering with vendors to enhance the use of technology in the District to reduce costs, improve service and provide expanded training and opportunity for students

The District also maintains Local Area Networks in each facility and a Wide Area Network which, in addition to providing Internet Access, is used for file sharing, operating and accessing both education and business applications and managing public, business only and confidential information. The District will store information both at District facilities and off-site.

Every staff member and student is responsible for safeguarding District information and physical assets. Every staff member and student is also responsible for using resources in an effective, ethical, and lawful manner.

2. Scope

This policy applies to the use of all District telecommunications / computing environment. This policy applies to all District staff (as defined in the Information Security Policy) and students using these resources.

3. Policy

Authorized personnel may only use District telecommunications / computing resources for approved purposes in proscribed manners consistent with all district policies. Occasional, limited, appropriate personal use of such systems is permitted, provided that such use does not preempt, disrupt, interfere, create liability or harm the District or the delivery of education services.

4. Standards

1. Only authorized users may use, or otherwise be granted access by IT Management, to the District's telecommunications / computing environment.
2. All access must be in compliance with the implemented standards, processes and procedures for telecommunications / computer usage including but not limited to Password Management Policies, Virus Protection, Internet Monitoring, Screen Saver Standards, and Backup Standards.

This includes but is not limited to:

- Maintaining strong passwords that are changed frequently
 - Never reveal a password to another
 - For users that have multiple userIDs intended for specific purposes, never using an id for an inappropriate purpose.
 - Never accessing a computer that is logged in under another userID
 - Never leaving a computer without logging off
 - Always using a locking screen saver that is activated within in minutes of inactivity
 - Never saving District information on non-District computer
 - Never placing portable storage devices (diskettes, cds, zip disks, etc (in unsecured locations
3. Any attempt to disable or circumvent security software or processes including but not limited to passwords, Internet monitoring software, virus protection software, network monitoring software, and firewalls, is prohibited.
 4. Auditing, testing, hacking, or bypassing security controls (whether within or outside the District network) is prohibited without written authorization from the Superintendent is prohibited.
 5. The falsification of identity or information is prohibited
 6. Sharing of accounts and/or user passwords is prohibited.
 7. Access by authorized users is limited to those rights specifically granted by IT Management.
 8. District's computer and electronic communication systems may not be used for outside business activities or the dissemination or storage of commercial or personal advertisements, solicitations, promotions, or political materials or any other non-district related business or education purpose.
 9. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, offensive, or otherwise unlawful or inappropriate may not be accessed, displayed, stored, created, or disseminated on or using District's telecommunications / computing environment.
 10. Any use of the District's telecommunications / computing environment that is in conflict with any of the District's explicit or implied policies is prohibited.
 11. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials is prohibited.
 12. Accessing public bulletin boards or chat rooms not specifically related to District business is prohibited.
 13. Expressing controversial or inflammatory opinions or making statements in public forums or email from the district's network such that those statements could be interpreted as representing district opinion is strictly prohibited.
 14. All Illegal activities including but not limited to malicious attempts to inappropriately access, harm or destroy data, hardware or software including parts of the district's telecommunications / computing environment or launching such an attack against another from the district's network is prohibited. This includes but is not limited to

creating, uploading or accessing viruses, installing worms or Trojan horses, launching attacks or inappropriately monitoring or capturing another user or systems activity or data.

15. Abuse or waste of resources is prohibited.
16. All access to District information and information resources is restricted to a need-to-know basis. Ability to access information or information resources does not imply permission to do so.
17. Users may not access, alter, or copy information belonging to another user without first obtaining permission from the owner or IT Management.
18. The ability to access, alter, or copy a file belonging to another user does not imply permission to do so.

5. Exceptions to Policy

The Board acknowledges that under rare circumstances, certain staff will need to employ systems or processes that are not compliant with this policy. The Superintendent must approve in writing all such instances in advance.

6. Reporting

All violations or non-compliances with the Information Security, Acceptable Use or Related Policies must be reported to IT Management and/or the Superintendent's office immediately. Failure to do so implies cooperation with the noncompliance and will be subject to the same consequences as the violator.

7. Consequences of Inappropriate Use

The violator of Information Security, Acceptable Use or Related Policies will be responsible for damages to equipment, systems and software resulting from deliberate or willful acts. General rules of behavior and communications apply when using the telecommunications computing environment including all policies related to privacy, harassment, vandalism and theft. Vandalism, is defined as malicious attempt to inappropriately access, harm or destroy data, hardware or software including parts of the district's telecommunications / computing environment or launching such an attack against another from the district's network. This includes but is not limited to creating, uploading or accessing viruses, installing worms or Trojan horses, launching attacks or inappropriately monitoring or capturing another user or systems activity or data.

In the event that a staff member or student violates any of the District's security measures, the Incident Handling Policy covers investigation of any such incident. A substantiated charge of non-compliance against a staff member or student shall subject such staff member or student to restriction of use or access to computer / telecommunications resources and/or other disciplinary action up to and including discharge or expulsion. Illegal use of the telecommunications / computing environment, deletion or damaging of files or data, copyright violations, theft of services, hacking, or bypassing security controls, violations of the privacy standards of another user, student, staff or the district or misrepresentation of another's identity, or vandalism, will be reported to the appropriate legal authorities for possible prosecution.

Staff Security Agreement

1. Objective

The West Jefferson Hills computing environment is a vital District asset. As such, to ensure that all District computing resources are used in an appropriate manner for approved purposes, The district has established the following Secure Access Agreement to protect this asset from unauthorized access and use.

2. Scope

This agreement applies to all District employees, contractors, consultants, temporary employees, and other staff at all District locations who access District information resources directly or remotely. Throughout this document, the term staff will collectively refer to these individuals.

3. Equipment

- Only properly configured District equipment will be permitted to access the District internal network.
- The District will provide authorized individuals with all hardware and software required, including anti-virus and firewall software, Internet monitoring capabilities to provide secure access to the District's computing infrastructure.

4. Terms and Conditions

- Authorized staff may only use District telecommunications / computing resources for District purposes. Occasional, limited, appropriate personal use of such systems is permitted, provided that such use does not preempt, disrupt, interfere, create a liability or harm the District or the delivery of education services
- Authorized staff may only use District telecommunications / computing resources in compliance with the District Information Security Policy, the District Telecommunications Acceptable Use Policy, and all other District explicit and implied policies standards and procedures and all access must be in compliance with the implemented standards, processes and procedures for telecommunications / computer usage including but not limited to Password Management Policies, Virus Protection, Internet Monitoring, Screen Saver Standards, and Backup Standards
- All illegal activities including but not limited to malicious attempts to inappropriately access, harm or destroy data, hardware or software including parts of the district's telecommunications computing environment or launching such an attack against another from the district's network is prohibited
- District's computer and electronic communication systems may not be used for outside business activities or the dissemination or storage of commercial or personal advertisements, solicitations, promotions, or political materials or any other non-district related business or education purpose.
- Any attempt to disable or circumvent security software or processes including but not limited to passwords, Internet monitoring software, virus protection software, network monitoring software, and firewalls, is prohibited
- Auditing, testing, hacking, or bypassing security controls (whether within or outside the District network) is prohibited without written authorization from the Superintendent.
- Falsification of identity or information is prohibited as is sharing of accounts and/or user passwords.

- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, offensive, or otherwise unlawful or inappropriate may not be accessed, displayed, stored, created, or disseminated on or using District's telecommunications computing environment.
- Accessing public bulletin boards or chat rooms not specifically related to District business is prohibited. Expressing controversial or inflammatory opinions or making statements in public forums or email from the district's network such that those statements could be interpreted as representing district opinion is strictly prohibited.
- Abuse or waste of resources is prohibited.
- All access to District information and information resources is restricted to a need-to-know basis. Ability to access information or information resources does not imply permission to do so.
- Users may not access, alter, or copy information belonging to another user without first obtaining permission from the owner or IT Management. The ability to access, alter, or copy a file belonging to another user does not imply permission to do so.

5. Additional Terms and Conditions for Remote Users

- Networking District equipment with personal computers is prohibited.
- Saving or Storing District information on non-District equipment is prohibited
- Remote connections to the District computing environment may only be made via approved, secure, remote access technology.
- Computers connected to the District network will not be left unattended.
- District employees, authorized partners, consultants, and contractors are liable for any misuse of their access or District information or data in their possession.
- Remote access privileges will be terminated if there is any evidence of non-compliance with the requirements stated in this policy.

I have read and agree to abide by this agreement and all District policies, standards and procedures related to the use of telecommunications / computing resources in particular the Information Security Policy and the Telecommunications Acceptable Use Policy.

 Printed Name -----
Signature

Date