Print Form

Staff Security Agreement

1 Objective

The West Jefferson Hills computing environment is a vital District asset. As such, to ensure that all District telecommunications/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, and 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. 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.
- Authorized staff may only use District telecommunications/computing resources in compliance with the District Information Security Policy, the District 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
- 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 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

- Remote connections to the District computing environment may only be made via approved, secure, remote access technology.
- Networking District equipment with personal computers is prohibited.
- Saving or storing District information on non-District equipment is prohibited
- 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 telecommunications/computer resources.
- 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 Acceptable Use Policy.

---------- ----------

Printed Name Signature Date

ITEM	DATE RECEIVED/INITIALED	DATE RETURNED/INITIALED