

*Network Access*

*Access*

All staff members of the Tredyffrin/Easttown School District will have access to all network services consistent with their job responsibilities during the school day from specified locations within District buildings.

Remote network access from outside District facilities will be granted and supported for members of the Information Services Department and District administrators, as necessary. Remote network access includes access to District servers, as appropriate.

All other staff members with active email accounts have remote email capability via Outlook Web Access, provided their computer is running version 5 or higher of Internet Explorer or Netscape Navigator.

*Monitoring*

Where reasonable suspicion exists that a specific user has violated District laws or Policies, the District may perform a specific search of that user's account.

Reasonable suspicion may arise from the following circumstances or from other circumstances which would lead a reasonable person to believe that a violation of law or Policy by an identified user or group of users may have occurred:

1. Existence of unauthorized software on a computer operated by a particular user or users;
2. A user is observed to be using the network in violation of the Policy;
3. Information from a reliable source that a user has violated the Policy;
4. Routine maintenance and monitoring leads to the discovery of possible Policy violations by a particular user or users;
5. Excessively high use of the internet;
6. Indication of access to prohibited websites; or
7. Indication of abuse or damage to network resources utilized by a particular user.

Adopted: January 12, 1998

Revised: April 27, 2000

Revised: February 23, 2004

Revised: (Form) November 29, 2007

Tredyffrin/Easttown School District

**Tredyffrin/Easttown School District  
Staff Network Acceptable Use Agreement**  
(Return completed form to Information Systems Department)

**ACCOUNT OWNER (please print)**

First Name \_\_\_\_\_ Middle Initial \_\_\_\_\_ Last Name \_\_\_\_\_  
 Position \_\_\_\_\_ Building \_\_\_\_\_  
 Supervisor/Principal \_\_\_\_\_

**ACCOUNT INFORMATION (please print)**

District Employee  
 Temporary Employee      Start Date \_\_\_\_\_ End Date \_\_\_\_\_  
 Non-District Employee      Relationship to District \_\_\_\_\_  
 Reason for Account \_\_\_\_\_

Staff members are required to act in a responsible, ethical, and legal manner in accordance with District Policy and Regulation 6190, accepted rules of network etiquette, and Federal and State law. Specifically, the following uses of network services are prohibited:

1. To facilitate illegal activities.
2. For commercial or for-profit purposes.
3. For fundraising purposes, except for links approved by the principal to websites of school-related organizations/clubs.
4. For non-school related work on more than an incidental basis.
5. For product advertisement or political lobbying.
6. To transmit hate mail/speech, discriminatory remarks and objectionable, offensive or inflammatory communication.
7. For unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. To access obscene or pornographic material.
9. For inappropriate language or profanity.
10. To intentionally obtain or modify files, passwords, and data belonging to other users.
11. To disrupt the work of other users.
12. To impersonate another user.
13. To share District passwords with, or allowing passwords to be used by, others.
14. To load or use unauthorized games, programs, files, or other electronic media.
15. To destroy, modify, abuse, hack, or attempt to hack network services.
16. To forward personal communications to public spaces without the original author's prior consent.

**The District makes no warranties of any kind and will not be responsible for any damage users may suffer including loss of data or interruption of network services. Communication provided by or through Network Services is not guaranteed to be private. Violation of the Staff Network Acceptable Use Agreement and/or District Policy 6190 or Regulation 6190 may result in suspension or loss of network services, disciplinary action up to and including termination of employment, and/or legal action.**

**→ I have read the above information and in signing below, I agree to adhere to these Policies.**

Account Owner Signature \_\_\_\_\_ Date \_\_\_\_\_  
 Supervisor/Principal Signature \_\_\_\_\_ Date \_\_\_\_\_

**INFORMATION SYSTEMS USE ONLY**

STAFF SIGNATURE	DATE	USERNAME