System Access Form Instructions

- Form is to be filled out by the employee's designated supervisor.
- Form must be completed to add a user to systems, modify, or remove their system access.
- Access cannot be granted or terminated without the signature of the Technology Coordinator\Superintendent or official designee.
- Access can not be granted without training.
- Access can not be granted without the employee signing the AUP.

Supervisor Tasks:

- Fill out top portion of form (make sure the employee's Official Title is their exact title).
  - Most full time teaching staff are awarded the following access:

o Network login o Staff_Shared o Student_Shared o District_Shared	o E-mail o eSchoolPlus (check it and file separate form) o Web Site Editing
"Financial System" is related to District Office Personnel only at this time.	

- Complete top portion and forward to the Tech Coordinator\Superintendent.
- Schedule training for new employee or one gaining new access with the designated trainer.

Tech Coordinator Tasks:

- Review form for accuracy and return if modifications are needed or forward to Network Specialist for completion if all information is correct.

Network Specialist Tasks:

- Complete access tasks as needed. If new employee or new access for an existing employee setup or modify access without activation until training is completed.
- If applicable, train employee to use systems if no other trainer has been designated.

Designated Trainer:

- Train employee regarding access in regard to District policies and procedures.
- Read over the "Acceptable Use Policy" that is included with the "System Access Form" and discuss with the employee as necessary to discuss any issues they may have with the policy.
- Obtain employee signature on bottom of "System Access Form" and give employee the "Acceptable Use Policy" sheet.

Otselic Valley Central School District
Systems Access Form

Action To Be Taken: **Add** ☐ **Modify** ☐ **Delete** ☐	
First Name:	**Last Name:**
Primary Building:	**Official Title:**
Room assignment:	**Telephone Extension:**
Start Date:	**End Date:**

Network Access Security Items:

☐ **Network Login**	☐ **E-Mail**
☐ **Staff_Shared** (District Staff Only)	☐ **eSchoolPlus** (Principal Files eSchoolPlus form)
☐ **Student_Shared** (Students/Staff Only)	☐ **Financial System**
☐ **District_Shared** (Full Time Employees Only)	☐ **Web Site Editing** (specify sections below)
☐ **Internet**	☐ **Other** (specify below)

Comments:

Network Items:

Network ID Created:

Email Address:

Trained Date: **By:**

Administrator Requesting: **Date:**

Tech Coordinator/ Supt Approval: **Date:**

Change Implemented By: **Date:**

I have received, read, understand and agree to adhere to the District's "Acceptable Use Policy for All Voice, Video, and Data Systems Guidelines for Students, Staff and Other Users" as found in the District's Technology Plan and agree to adhere to these guidelines as it pertains to my access outlined above.

Systems User: **Date:**

Otselic Valley Central School

Acceptable Use Policy for All Voice, Video, and Data Systems
Guidelines for Students, Staff and Other Users

This document has been developed by the District Technology Team to govern and guide in the use of all voice, video, and data systems. All equipment is District property. Information or data created or stored on the District's computers or data systems assumed to be the responsibility of the individual whose name is assigned to the password accessed when the information was created. These systems include, but are not limited to: television monitors, satellite receivers, computers, electronic mail, servers, stored digital data, Intranets, and the Internet. All users accessing the computer network should not expect nor does the District guarantee privacy for any user of the District computer network. The District reserves the right to monitor all technology resource activity and files created on or conveyed over its system as the District deems necessary. The Otselic Valley Central School District provides these resources to promote educational excellence by facilitating sharing, innovation, and communication with the support and supervision of parents, administration, teachers, and support staff.

The District's equipment is for education and/or research use only and must be used in a manner consistent with the District's goals and purposes. With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Proper behavior, as it relates to the use of technology resources, is no different from proper behavior in all other aspects of Otselic Valley Central School activities. All users are expected to use the technology resources in a responsible, polite, and ethical manner. Use of the equipment which violates any aspect of District policy, the Code of Conduct or federal, state or local laws/regulations is strictly prohibited. The intent of this document is to give an overview of user responsibility, and to outline acceptable and unacceptable use of these resources without exhaustively enumerating all such responsibilities, uses and misuses.

District policies pertaining to accessing electronic information or communications sent or received at school as well as the risks associated with Internet access appear in the Student Handbooks or similar documents and are published annually in the district newsletter. The use of the District's equipment is a privilege, not a right. With notice of policies as outlined above, **any person** using the District system has implicitly consented to adhere to all policies. Inappropriate use may result in disciplinary action, including suspension or cancellation of the privilege.

User Responsibility for Staff and Students

- Staff and Students will comply with all existing school board policies (including the Code of Conduct) as they may be interpreted to apply to technology resources.
- Respect the privacy of other users. Do not obtain copies, or modify files, other data or passwords belonging to other users.
- Comply with legal protection provided by copyright and license to programs, data, and documents.
- Protect your password. You are responsible for anything done under your account(s). Sign on to systems only under your account(s).
- Comply with the acceptable use policies of all technology resources to which the district has access.
- Conserve server resources. Save only what you need. Limit network use to business and/or educational activities associated with your position at OVCS.

Acceptable

- Use that encourages efficient, cooperative, and creative methods to perform the user's job duties or educational tasks.
- Use related to instructional, administrative, and supervised extra-curricular activities.
- Use of District technology resources for appropriate access to voice, video, and data systems, both locally and at other sites.

Unacceptable

- Providing, assisting in, or gaining unauthorized or inappropriate access to the District's technology resources, including any type of voice, video, or data information server. This includes disclosing others' passwords or sharing your account(s).
- Activities that interfere with the ability of students/staff members to use the District's technology resources or other network connected services effectively.
- Distribution of any material in such a manner that might cause unnecessary or excess congestion of the voice or data networks.
- Creating, distributing, collecting, reviewing, downloading, displaying or otherwise gaining access to obscene, pornographic, abusive, harassing or threatening material using District technology resources.
- Use of technology resources for a commercial, political, or profit-making enterprise.
- Downloading, installing or using any unauthorized software or tampering with hardware on any technology system.
- Using the network to provide addresses, phone numbers or other personal information unless otherwise as specified in District policies/documents.

Consequences of Improper Use

Improper or unethical use may result in disciplinary actions consistent with existing District policies. This may include revoked, limited or supervised access to District technology resources as well as referral to law enforcement agencies. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's technology resources.