Website Access Request Form

A **Website Access Request Form** must be signed by each school staff member, parent, or community volunteer who is requesting administrative access to a school website. Account access must also be approved by the principal and cannot be delegated. Once approved, please allow 1 – 3 working days for verification and configuration of permissions. Accounts are created in the following way:

- **Principals:** Principals are automatically made website administrators and they are the sole person who can request website administrative access for others. Principals are also asked to notify webmaster@seattleschools.org when Website Administrative Privileges should be removed.
- **Staff:** All staff accounts are created based on network username and password.
- **Parents and Community Volunteers:** Please provide the email address you wish to use in the table below.

Please send all signed, completed forms to Webmaster using one of the following methods:
District Mail Stop: 21-350 **Fax:** 206-252-0301 or **Email:** webmaster@seattleschools.org

WEBSITE ADMINISTRATOR:

Complete all fields. Parents and community volunteers, you must also complete the Network Use Agreement on the reverse of this form.

School Name	
Full Name	
Phone Number	
Email Address	
*Signature	
Date	
Role (circle) ☐ Staff ☐ Parent ☐ Community Volunteer	

* As Website Administrator:

- You accept responsibility for enforcing the quality, accuracy, safety, and privacy for the above referenced school website.
- You agree to work within the guidelines, standards, and procedures set forth by the School Board and the District's Web Communications Steering Committee.
- You acknowledge that you have reviewed the School Sites – *Roles and Responsibilities, Web Content Standards & Guidelines* and the *Website User Experience Guidelines* with your principal, which can be found at: http://www.seattleschools.org/websitetraining
- Agree not to share or distribute your user account or password with staff, parents, students or other volunteers.
- Agree not to create or modify any other Website Administrator accounts.

PRINCIPAL Complete all fields.

Full name	
*Signature	
Date:	

As Principal:

- You acknowledge that Website Administrators are an extension of your responsibilities.
- You will manage and oversee the activities of your website team.
- You acknowledge that you have reviewed the School Sites – Roles and Responsibilities, Web Content Standards & Guidelines, and the Website User Experience Guidelines with your designated Website Administrator.
- You agree to work within the guidelines, standards, and procedures set forth by the School Board and the District's Web Communications Steering Committee.
- Agree not to create or modify any other Website Administrator Accounts.

ABOUT THIS FORM

This form must be completed by each school principal for each individual that is granted Website Administrator access (required for staff, parents, and community volunteers). Seattle School District policy requires that all Website Administrators and Content Author/Publishers sign and accept the District's Network Use Agreement. Additionally, anyone granted Content Author/Publisher privileges to the school website agree to support the guidelines, best practices, and security procedures.

For more information, contact webmaster@seattleschools.org.

Seattle Public Schools Network Use/Access Agreement

The Seattle School District is pleased to offer its employees access to the District's computer network, which includes word processing, electronic mail, and Internet services. The purpose of District computers and access to the network is to support educational objectives and job responsibilities. All information and services contained on District computers are placed there solely for job related functions. Access to the network is a privilege—not a right—and it may be revoked by the District at any time. For purposes of this use agreement, vendors and independent contractors are considered SPS employees.

The District has the right to review any material stored in a District computer or accessed through the network, including but not limited to email. The District also has the right to edit, remove, or copy any material installed, used, stored, or distributed on or through the District's network or system, which includes the copying of emails sent or received through a District computer. Files stored or materials accessed through the network are not private. The waiver of privacy does not mean that network users or the District waives confidentiality rights with respect to materials that are subject to statutory or common law privileges (e.g., attorney-client, FERPA, medical records) or not subject to disclosure as public records.

The District does not warrant the functions of the Internet service or that any of the networks accessible through the Internet service will meet any specific requirements an employee may have, or that the Internet service will be error free or uninterrupted. Nor shall the District or any administrators be liable for any direct or indirect, incidental, or consequential damages sustained or incurred in connection with the use, operation, or inability to use the network.

The following conduct is prohibited on the District network:

1. Transmitting or accessing obscene, pornographic, graphically violent, or sexually inappropriate material or pictures for a non-educational purpose;
2. Using obscene, graphically violent, or sexually inappropriate language for a non-educational purpose;
3. Engaging in practices that may harm or destroy data on any system or on the network or disrupt the operation of the network;
4. Installing, storing, or distributing copyrighted software or materials in violation of copyright law;
5. Supporting or opposing a political candidate, an election campaign, or a ballot proposition, including a school levy;
6. Sharing computer authorization, including your password, with any person, except to an authorized network administrator.
7. Transmitting or accessing material that discriminates against, harasses, defames, or insults another person, which includes sending or receiving sexually explicit, racial, or gender inappropriate jokes or messages;
8. Using the network to violate District policies;
9. Encrypting communications to avoid District review;
10. Intentional and unauthorized access in another person's folders or work files;
11. Using the network for illegal activities (e.g., sale of drugs, bomb making, or computer "hacking"); and
12. Using District computers or the network for non-District approved commercial purposes, including a private or personal business or consulting practice.
13. Tampering with or disabling any District installed security software such as Anti-Virus, Security Updates Services, Screen-Saver timeout/locks, etc.

Confidential or Sensitive Data

Additionally, SPS employees will maintain the confidentiality of all protected information to which they have access, including student and personnel information.

SPS employees shall comply with all applicable laws and regulations pertaining to the release of student information, including but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g, and District policies and procedures.

SPS employees using electronic or printed confidential or sensitive information should exercise reasonable care in its use, storage, and destruction. It is the individual's responsibility to prevent unauthorized access to confidential data and to prevent dissemination beyond the scope of its original purposes. Immediately report any known or suspected data breaches to the District.

External requests for the disclosure of student and sensitive data shall not be released without authorization and shall be routed through proper channels for approval and delivery.

Reasonable security precautions and protections should be used to ensure that unauthorized persons do not gain access to the data.

Prohibited practices that undermine confidentiality include, but are not limited, to the following:

1. Leaving your computer unattended while student information is visible on the screen or otherwise inappropriately accessible.
2. Sharing personally sensitive / confidential data with unauthorized individuals
3. Failing to exercise reasonable care in student data use, storage, and appropriate destruction
4. Saving or exchanging unencrypted student data via cloud services, including tools like dropbox.
5. Retaining sensitive/confidential information longer than necessary for specific work related task or purpose
6. Intentionally releasing sensitive or private information via printed listings (including rosters) or through viewing of access screens in an attempt to circumvent controls

Signature

The above list is not exclusive and the District is the sole arbiter of what conduct is inappropriate and thus prohibited on the network. A network administrator will report inappropriate conduct to an employee's supervisor and to human resources so that appropriate disciplinary action may be taken. Any other reports of inappropriate behavior, violations, or complaints will be routed to the employee's supervisor or to human resources so that appropriate disciplinary action may be taken. Engaging in prohibited or inappropriate conduct may result in the loss of access to the network as well as other disciplinary action up to and including termination of employment. When applicable, law enforcement agencies may be involved.

In consideration for the privilege of using the District's network or other computer services, I grant the District permission to monitor my activities on the network and I hereby waive any right to privacy which I may otherwise have in such materials. I have also read and understand the above Network Use/Access Agreement. I acknowledge and agree to all the conditions set forth in this document.

Print Name	Signature
Location/Position	Date