SBSD VPN User Agreement

The South Burlington School District (SBSD) is providing Virtual Private Network (VPN) access to some SBSD network resources for South Burlington teachers and administrators.

This connection will provide employees with access to their network file storage (the users' J: drives), the K: and S: drives, and to a select group of applications (e.g., Microsoft Office, Outlook, Schoolmaster Gradebook, Elementary School Report Cards, the Reservation Database, etc.). This home access is not considered "mission critical" and should be viewed as an optional benefit. Although we do not anticipate problems, if remote connection issues do occur they will be addressed during regular business hours.

The user needs to understand that there are always security risks with any computer use. District Network Services (DNS) and District administrators are aware of many of the potential risks. The remote access we are providing has as high a level of security as current, commercially-available technology is capable of providing. SonicWall SSL-VPN software will encrypt data that users access via connections to a Terminal Server, which will run the applications on the District's network. No actual data, other than encrypted keystrokes and screen images, traverses the public Internet. The actual data will stay protected on the server.

While the VPN/Terminal Server software will keep the original data safe, it does not protect against physical access to the user's home computer. The user must not leave his or her computer unattended while the VPN connection is active. DNS is making a strong effort to secure the connection between the remote user and the District network, but it is the user's responsibility to uphold the security of the connection at the remote location. The user alone is responsible for any security breach arising from misuse or inadequate protection of the remote connection.

The user can connect to the District network via the VPN and Terminal Server through any broadband connection using a current Internet web browser. While the service is available over many publicly accessible computers, such as those commonly found in airports, libraries, and at public kiosks, users should be aware that these computers may cache (store a copy of) sensitive information, may be surreptitiously monitored by data thieves, or may have been infected with malicious software or hardware designed to capture user data and passwords. Therefore, public computers are inherently insecure and should **not** be used for remote access to the SBSD network.

Support for Home Use:
DNS cannot offer support for home Internet connections and devices. If a problem exists off-site and during working hours, DNS will offer phone support only for the Terminal Server connection.

Requirements for Home Use:

- Broadband Internet connection (DSL or cable. Satellite may work, but performance may be unacceptably slow)
- Current Internet web browser (e.g., Internet Explorer 6 or higher, Mozilla Firefox 2 or higher).
- Current Microsoft software patches, applied and updated regularly by the owner
- Anti-virus software installed and kept current by the owner with the most recent anti-virus signatures.

User Agreement for Participation:
I have read the above information. I agree to secure the VPN connection at my home, use secure passwords, and log off the connection when leaving the computer unattended. I understand that the District takes no responsibility for ensuring that the connection will work for me, and I accept the limitations of the support that the District is providing for the connection and my home computer. Although the District does not anticipate that use of the VPN system will result in any damage to software configurations or hardware in my computer, I understand that the District accepts no responsibility for any damage that may occur as a result of my using the VPN connection.

_____	_____	_____
Signature	Name, Printed	Date