

REMOTE ACCESS TO COMPUTER NETWORK

The purpose of this policy is to establish standards for connecting to the Patchogue-Medford UFSD network from any external host. These standards are designed to minimize the potential exposure to the district from damages that may result from unauthorized use of Patchogue-Medford resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, or damage to Patchogue-Medford internal systems.

This policy applies to all Patchogue-Medford employees, contractors, vendors and agents with a Patchogue-Medford-owned or personally-owned computer or workstation used to connect to the Patchogue-Medford network. This policy applies to remote access connections used to do work on behalf of Patchogue-Medford. Remote access implementations that are covered by this policy include, but are not limited to, VPN (Virtual Private Network), RDP (Remote Desktop Protocol), or similar remote access software.

It is the responsibility of Patchogue-Medford employees, contractors, vendors and agents with remote access privileges to Patchogue-Medford's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Patchogue-Medford. Remote access usage shall not violate any Patchogue-Medford policies, perform illegal activities, or be used for outside business interests.

End-users interested in obtaining remote access privileges shall contact the Executive Director of Technology for consideration and be authorized by the Superintendent or his/her designee. Each request for remote access will be evaluated on a case-by-case basis. A Remote Access Agreement (see Exhibits A and B) must be signed and submitted prior to access being granted.

Secure remote access will be strictly controlled. Control will be enforced via multi-factor ~~authentication~~authentication. At no time should any Patchogue-Medford employee or vendor provide login or email password to anyone. All hosts connected to Patchogue-Medford internal networks via remote access technologies must use the most up-to-date anti-virus/spyware software. This includes personal computers.

The internal claims auditor will review the VPN access logs on a monthly basis. The Business Office will provide these reports to the Board of Education in accordance with indicated agenda review deadlines. Any exceptions will be reported to the Board and Assistant Superintendent of Business and Operations, or designee.

Any employee, contractor or vendor found to have violated this policy shall have remote access rights revoked and may be subject to disciplinary action, up to and including termination of employment or contract as applicable. Restoration of remote access rights will occur on a case-by-case basis in consultation with the employee's supervisor and other authorities as needed. Vendors accessing the Patchogue-Medford network shall be subject to having access rights revoked with no liability on the District's part.

Adopted:

April 15, 2013

Revised:

February 26, 2018

Revised:

June 29, 2020

Revised:

January 23, 2023

Revised:

August 21, 2023

Revised:

September 16, 2024

Reviewed:

August 18, 2025