

MCPS Remote Access

Terms for Use

1.0 Purpose

The purpose of this document is to provide standards and guidelines for remote access to connect to the MCPS educational network.

2.0 Scope

These criteria apply to all Montgomery County Public School (MCPS) employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing remote access to the MCPS network.

3.0 Remote Access Approval

MCPS employees and authorized third parties can request remote access to the MCPS network by obtaining approval by submitting the MCPS-OCTO Remote Access Request form. All authorization requests must be submitted by the requestor's division/department directors. Remote access authorization is given only to persons who require access to MCPS resources to carryout official MCPS duties.

4.0 Criteria

Approved MCPS employees and authorized third parties may utilize the benefits of remote access, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing/maintaining any required software, and paying associated fees for their personal home service.

1. It is the responsibility of MCPS remote access users to ensure that unauthorized users do not allow access to MCPS internal networks using his/her MCPS credentials.
2. Remote access is to be controlled using user name and password authentication. Storing or saving MCPS login information in the remote access client is prohibited.
3. All computers connected to MCPS internal networks via remote access must use the most up-to-date anti-virus software, definitions, and critical operating system updates.
4. The remote access connection will close after 60 minutes of user inactivity and users will be automatically disconnected from the MCPS network. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
5. Users of computers that are not MCPS-owned equipment must configure the equipment to comply with IGT-RA.
6. Sensitive data must be safeguarded at all times.
7. By using remote-access technology with personal equipment, users must understand that their machines are a de facto extension of the MCPS's network, and as such are subject to the same rules and regulations that apply to MCPS-owned equipment, i.e., their machines must be configured to comply with Regulation IGT-RA, *User Responsibilities for Computer Systems and Network Security*.

5.0 Enforcement

Any MCPS remote access user found to have violated these criteria may be subject to disciplinary action, up to and including termination of employment in accordance with Regulation IGT-RA.