

---

*Rescinds Policy Number:**Issued: 06/05/06*

---

With the increased utilization of technology and networked software to provide access to important information, it becomes increasingly important that all users understand the role they play in protecting the confidentiality of information. Whether information is accessed locally from a single workstation, a network server, or over a dedicated internet circuit, each user has significant responsibility to safeguard that data. Users must be cognizant of their personal responsibility in safeguarding confidential school system information.

All Orange County Schools users including permanent employees, contract staff, and temporary employees must be properly identified and authenticated with the Directors of Human Resources before they are allowed to access systems containing confidential data. When hired the Staff Acceptable Use Policy, which includes the requirements for compliance with the Security Awareness Policy, will be signed by the employee and placed in their permanent employment folder.

The combination of a unique user identification (user-ID) and a valid password is the minimum requirement for granting access to the Orange County Schools network. A unique user-ID must be assigned for each employee so that individual's accountability can be established for all network activities. Administrative approval is required for each user-ID creation and a process is in place to remove, suspend or reassign inactive user-IDs arising from employee or contractor movements. The authentication system shall limit unsuccessful logon attempts. Password management capabilities and procedures are established to ensure secrecy of passwords and prevent exploitations of easily guessed passwords or weaknesses arising from long-life passwords.