



**HAWTHORNE CEDAR KNOLLS UFSD
226 LINDA AVENUE
HAWTHORNE, NEW YORK 10532-3795**

Protection of Confidential Information

As employees of Hawthorne Cedar Knolls Union Free School District you will, in the course of your duties, have the need to use the School District's Internet and Technology systems. By doing such, you will be expected to adhere to School District's policies specific to the use of the Internet and Technology systems. Additionally, you may come across confidential information and data that is subject to the following guidelines:

- Individuals shall not access, copy or disseminate confidential information and data except to the extent necessary to fulfill their assigned responsibilities, and then only to the extent that the individual is authorized. *Improper access to or unauthorized disclosure of confidential information could be a violation of Federal law.*
- Individuals will take appropriate action to ensure the protection confidentiality, and security of School District information. This obligation to maintain confidentiality continues beyond the termination of the individual's relationship with the School District. Persons who exceed their authority in using confidential information or who gain access to such information through unauthorized means are in violation of the School District's policy. Once an individual is granted access to data, he or she is responsible as a custodian of that data. Data custodians are held accountable for maintaining the security and confidentiality of the information to which they are granted access even when that data or information is not adequately secured. Additionally, all staff must comply with the Family Educational Rights and Privacy Act (FERPA) guidelines regarding the release of student information.
- Hawthorne Cedar Knolls UFSD expects e-mail messages to be treated as confidential by all employees and accessed only by the intended recipient. This information may not be shared with non-district employees. District employees are to only have access to information relating specifically to their job responsibility. Employees should not attempt to gain access to another employee's messages; the same applies to any/all voice mail messages on school district telephones.
- User ID's and Passwords are to be kept secure, and accessible only to yourself.
- User ID's and Passwords will not be shared with anyone
- If a User ID or Password is lost or compromised in any manner, you will inform the central office immediately to reassign a new ID and Password.
- Complex passwords should be created using characters including capitals and lowercase letters and numbers. You will not use any family names or other predictable information in the creation of this password. You will change the password when prompted by the system or if you feel it is compromised.
- Discretion is to be used to ensure confidentiality with regard to when and where you access programs (e.g., monitor is not visible to others and to log out of the programs when not in use). This also applies to use off-site (at home, etc.).
- This includes, but is not limited to, all paper documentation, facsimiles, data programs and any software utilized by the District.
- This applies to both Student and Employee/Staff information and records.