THE CENTER FOR DISCOVERY Health. Wellness. And Wonders.

PO Box 840, Harris, NY 12742 | 845.794.1400

Computer Resources and Data Management

The Center for Discovery (TCFD) values the protection of Private information in accordance with the applicable law, regulations and best practice. Accordingly, The Chief Compliance Officer and Information Technology (IT) staff will plan, implement, and monitor IT security mechanisms, procedures, and technologies necessary to prevent improper or illegal disclosure, modification, or denial of sensitive information in TCFD's computer system network. Similarly, such IT mechanisms and procedures will also be implemented in order to safeguard TCFD technology resources, including computer hardware and software. IT Network administrators may review TCFD computers to maintain system integrity and to ensure that individuals are using the system responsibly. Users should not expect that anything stored on TCFD school computers or networks would be presumed private.

In order to achieve the objectives to manage computer records, the following steps will be taken:

- Inventory and classify personal, private, and sensitive Information on the network to protect the confidentiality, integrity, and availability of information;
- Develop password standards for all users including, but not limited to, how to create passwords and how often such passwords should be changed by users to ensure security of the TCFD's computer systems;
- Develop procedures to control physical access to computer facilities, data rooms, systems, networks, and data to only authorized individuals; such procedures may include ensuring that server rooms remain locked at all times and the record individuals who have access to this room.
- Establish procedures for tagging new purchases as they occur, relocating assets, updating the inventory list, performing periodic physical inventories, and investigating any differences in an effort to prevent unauthorized and/or malicious access to these assets;
- Periodically grant, change, and terminate user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties;
- Determine how, and to whom, remote access should be granted, obtain written agreements with remote access users to establish TCFD's needs and expectations, as appropriate, and monitor and control such remote access;
- Verify that laptop computer systems assigned to teachers and administrators use full-disk encryption software to protect against loss of sensitive data;
- Deploy software to servers and workstations to identify and eradicate malicious software attacks such as viruses and malware;
- Develop and test a disaster recovery plan appropriate for the size and complexity of TCFD IT operations to ensure continuous critical IT services in the event of any sudden, catastrophic event, including, but not limited to fire, computer virus or deliberate or inadvertent employee action.