Acceptable Use Policy

This policy applies to any computer, networking device, telephone, copier , fax machine or other technologic equipment which is owned, licensed or leased by Core; is owned licensed or leased by member school districts and is used by Core employees. This policy also applies to any technologic equipment which connects directly with Core data or telephone networks, connects to any device owned, licensed or leased by Core or otherwise uses or affects Core information – technology facilities. Furthermore, Core employees are required to adhere to the Acceptable Use Policies of any Core member school district.

Restricted Applications

Restricted applications of Core's technologic equipment include but are not limited to:

1. Threatening Core's tax exempt status such as certain political activity and most commercial activities.
2. Illegal acts such as fraud, harassment, copyright violation and child pornography.
3. Depriving other users of their fair share of Core technologic equipment or interference with the functioning of central networks (ie, mass emails, streaming video, downloading harmful files, intentionally wasting resources)
4. Violating Core's policies.
5. Sending or displaying offensive messages or images
6. Using obscene language.
7. Insulting or attacking others
8. Violating copyright laws.
9. Using others' passwords without permission
10. Trespassing in others' folders, documents or files.
11. Use of the network or any devise for the sale of personal items.

When any of use of Core technologic equipment presents an imminent threat to other users or to Core's technology infrastructure, system operators may take whatever steps are necessary to isolate the threat without notice is circumstances so require. This may include changing passwords, locking files, disabling devices, or disconnecting specific devices or entire sub-networks from Core, regional or national voice and data networks. System operators will restore connectivity and functionality as soon as possible after the threat has been identified and neutralized.

Technologic devices, network connections, accounts, usernames, authorization codes and passwords are issued to identify users of Core technologic equipment. Users are responsible for not sharing their privileges with others, and especially for ensuring that authorization codes and passwords remain confidential. All users of the cooperative's network and devices are responsible for ensuring that unauthorized users do not gain access to the Core network or devices.

Sanctions

The Director will make the initial determination of the policy violation. Once it has been determined that a policy violation has occurred, the director will implement the appropriate sanctions, which include, but are not limited to:

- Verbal warning
- Written warning
- Denial, suspension or revocation of any technologic device or network access
- Employment sanctions
- Notification of law enforcement

Staff will maintain safe, responsible and acceptable use of all technologic equipment assigned to them. In the case of lost or damaged equipment, the Technology Coordinator and Director will review the situation and determine any fees to be assigned to employee. Employee may appeal the decision to the school board if they do not agree with the fee assessment.

_____

Signature & Date