Note: For Board member use of ESC technology resources, see BBI.

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

Availability of Access

Access to the ESC's technology resources, including the internet, shall be made available to employees primarily for work-related purposes and in accordance with administrative regulations.

Limited Personal Use

Limited personal use of the ESC's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the ESC;
2. Does not unduly burden the ESC's technology resources;
3. Has no adverse effect on an employee's job performance or on a student's academic performance; and
4. Is not for personal financial gain.

Use by Members of the Public

Access to the ESC's technology resources, including the internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the ESC; and
2. Does not unduly burden the ESC's technology resources.

Acceptable Use

The Executive Director or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the ESC and with law and policy.

Access to the ESC's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the ESC's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with ESC policies. [See DH]

Violations of law may result in criminal prosecution as well as disciplinary action by the ESC.

Internet Safety

The Executive Director or designee shall develop and implement an internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

Each ESC computer with internet access and the ESC's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Executive Director or designee.

The Executive Director or designee shall enforce the use of such filtering devices. Upon approval from the Executive Director or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Monitored Use

Electronic mail transmissions and other use of the ESC's technology resources by employees and members of the public shall not be considered private. Designated ESC staff shall be authorized to monitor the ESC's technology resources at any time to ensure appropriate use.

Disclaimer of Liability

The ESC shall not be liable for users' inappropriate use of the ESC's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The ESC shall not be responsible for ensuring the availability of the ESC's technology resources or the accuracy, age appropriateness, or usability of any information found on the internet.

Record Retention

An ESC employee shall retain electronic records, whether created or maintained, using the ESC's technology resources or using personal technology resources in accordance with the ESC's record management program.

Electronically Signed Documents

At the ESC's discretion, the ESC may make certain transactions available online, including student admissions documents, student

grade and performance information, contracts for goods and services, and employment documents.

To the extent the ESC offers transactions electronically, the ESC may accept electronic signatures in accordance with this policy.

When accepting electronically signed documents or digital signatures, the ESC shall comply with rules adopted by the Department of Information Resources, to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the ESC;
- Maintain all records as required by law;
- Ensure that records are created and maintained in a secure environment;
- Maintain appropriate internal controls on the use of electronic signatures;
- Implement means of confirming transactions; and
- Train staff on related procedures as necessary.

Security Breach Notification

Upon discovering or receiving notification of a breach of system security, the ESC shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The ESC shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the ESC has electronic mail addresses for the affected persons.
3. Conspicuous posting on the ESC's website.
4. Publication through broadcast media.