Information Security

It is the policy of the ESD to protect information assets from all threats, whether internal or external, deliberate or accidental. The information assets include but are not limited to confidential student and personnel records. ESD's information assets are accessed, created, and used by families, students, employees, contractors, clients, and other constituents across systems that are delivered from external or internal sources. This policy governs actions and expectations of all who use or access ESD's information assets.

Guiding Principles
The following principles will be followed to protect ESD information assets from all threats:

1. Information Confidentiality - The ability to access or modify information assets is provided only to authorized users for authorized purposes.
2. Information Integrity - The information assets used in the pursuit of the ESD objectives can be trusted to correctly reflect the reality it represents.
3. Information Availability - The information assets of the ESD, including the network, the hardware, the software, the facilities, the infrastructure, and any other such resources, are available to support the objectives for which they are designated.
4. Information Privacy – The ability to prevent unauthorized access to information assets the ESD collects about its families, students, and other clients, which may be personally identifiable information (PII), and to prevent the collection of information assets that constitute a person being observed, monitored, or examined without consent or knowledge.

Security Procedures
To protect ESD information assets from threats, the Superintendent or the Superintendent's designee shall prepare security procedures, which will balance safeguarding information assets with the need to support the pursuit of legitimate ESD objectives.

ESD's information security procedures shall:

- Determine information security requirements through risk assessments that consider the harm to ESD as a result of a security failure, which has consequences of loss of confidentiality, integrity, availability, and privacy of information or other assets and the likelihood of a failure occurring in light of existing threats and vulnerabilities given the security controls and mechanisms implemented in the system environment.
- Implement security controls and mechanisms that ensure risks are mitigated to an appropriate level and consider costs associated with implementing them.
- Consider separation of duties where no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.
- Employ multiple methods, tools, and audit processes to monitor and assess whether security controls and measures have been implemented and are being followed.
- Leverage existing technology and cyber security frameworks for best practices unless made mandatory (e.g., PCI-DSS to accept credit cards).
- Include training for applicable employees and contractors.

The procedures that are adopted and implemented must address the following areas, modeled from the international standard ISO 27001:2013 Information Technology – Security Techniques – Information Security Management Systems:

- Information security procedures
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, deployment, integration, and maintenance
- Secure software development
- Third-party relationships
- Information security incident management
- Business continuity management
- Establish programs to monitor required compliance (e.g., PCI-DSS).

Employee Responsibilities
All ESD employees are responsible for the security of the ESD's information assets. Employees must comply with procedures and report information security violations as outlined in the procedures. Failure to protect information assets could potentially result in fines, audits, loss of confidence, and direct financial impacts to the ESD. ESD Employees who fail to follow information security procedures will be subject to discipline, which may include termination of employment and responsibility for the recovery of any loss or damage to ESD, and possibly third parties.

Legal References:	*COPPA – Children's Online Privacy Protection Act* *GDPR – General Data Protection Regulation* *20 U.S.C. 1232g Family Education Rights and Privacy Act* *34 CFR, Part 99 Family Education Rights and Privacy Act Regulations* *RCW 42.56.230 Public records act* *RCW 19.255.010 Personal Information – Notice of security breaches* *RCW 28A.604 Student User Privacy in Education Rights*

Adoption Date: **4-25-23**