O'BRIENS
AVEDA INSTITUTE

400 Cornerstone Drive, Williston, VT 05495

O'Briens Aveda Institute Information Security Policy

1. **Purpose**

The purpose of this policy is to ensure the secure use and handling of all school data, computer systems and computer equipment by employees.

2. **Policy**

2.1 Technology Security

It is the policy of O'Briens Aveda Institute to support secure network systems within the school, including security for all personally identifiable information that is stored on paper or stored digitally on school-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the O'Briens Aveda Institute, its students, or its employees.

O'Briens Aveda Institute will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the school network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of school devices and the network. When an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the school's owner, Wiliam H. O'Brien, with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to O'Briens Aveda Institute critically sensitive data. All third-party entities will be required to have permission from the Information Security Officer before accessing our systems or receiving information.

It is the policy of O'Briens Aveda Institute to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq.

Professional development and training for staff regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals. O'Briens Aveda Institute supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protectO'Briens Aveda Institute's data, users, and electronic assets.

3. **Procedure**

3.1. Definitions:

3.1.1. Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

3.1.2. Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

3.1.3. Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

3.1.4. Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

3.1.5. Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

3.1.6. Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

3.1.7. Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

3.1.8. Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

3.1.9. Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for deanonymizing anonymous data can be considered protected data

3.1.10. Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

3.1.11. Sensitive data - Data that contains personally identifiable information.

3.1.12. System level – Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

3.2. Security Responsibility

3.2.1.O'Briens Aveda Institute has appointed William H. O'Brien, owner, as responsible for overseeing school-wide IT security with duties that include development of school policies and adherence to thestandards defined in this document.

3.3 . Training

3.3.1. O'Briens Aveda Institute, led by the IT manager, shall ensure that all school employees having access tosensitive information undergo annual IT security training which emphasizes their personal responsibility for protectingstudent and employee information.

3.4. Physical Security

3.4.1. Computer Security

3.4.1.1.O'Briens Aveda Institute shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screen savers should be used to enforce this requirement.

3.5. Network Security

3.5.1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (school) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

3.5.2. Network Segmentation

3.5.2.1.O'Briens Aveda Institute shall ensure that all untrusted and public access computer networks are separated from main school computer networks and utilize security policies to ensure the integrity of those computer networks.

3.5.2.2. O'Briens Aveda Institute will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

3.5.3S. Wireless Networks

3.5.3.1. No wireless access point shall be installed on O'Briens Aveda Institute's computer network that does not conform with current network standards. Any exceptions to this must be approved directly in writing by the Information Security Officer.

3.5.3.2. O'Briens Aveda Institute shall scan for and remove or disable any rogue wireless devices on a regular basis.

3.5.3.3. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

3.5.4. Remote Access

3.5.4.1. O'Briens Aveda Institute shall ensure that any remote access with connectivity to the school's internal network is approved by the school's Information Security Officer. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

3.6. Access Control

3.6.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

3.6.2.1 Password Protection

3.6.2.2 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

3.6.2.3. Passwords must not be inserted into email messages or other forms of electronic communication.

3.6.2.4 Passwords must not be revealed over the phone to anyone.

3.6.2.5 Do not reveal a password on questionnaires or security forms.

3.6.2.6. Do not hint at the format of a password (for example, "my family name").

3.6.2.7. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.6.3. Authorization

3.6.3.1. O'Briens Aveda Institute shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.6.4. Administrative Access Controls

3.6.4.1. O'Briens Aveda Institute shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

3.7. Incident Management

3.7.1. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.8. Business Continuity

3.8.1. To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of school IT operations.

3.8.2. O'Briens Aveda Institute shall develop and deploy a business continuity plan which should include as a minimum:

- Backup Data: Procedures for performing routine daily/weekly/monthly backups to OneDrive.
  Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for
- ensuing a full head count of all.
-

3.9. Malicious Software

3.9.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

3.9.2.O'Briens Aveda Institute shall install, distribute, and maintain spyware and virus protection software on all school-owned equipment, i.e. servers, workstations, and laptops.

3.9.3.O'Briens Aveda Institute shall ensure that malicious software protection will include frequent updatedownloads (minimum monthly), frequent scanning (minimum monthly), and that malicious software protection is inactive state (real time) on all operating servers/workstations.

3.9.4. O'Briens Aveda Institute shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.

3.9.5. All computers must use the school approved anti-virus solution.

3.10. Data Privacy

3.10.1. O'Briens Aveda Institute considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

3.10.2.O'Briens Aveda Institute protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act U.C.A. §62G-2 ("GRAMA").

3.10.3. O'Briens Aveda Institute shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.11. Security Audit and Remediation

3.11.1.O'Briens Aveda Institute shall perform routine security and privacy audits.

3.11.2. O'Briens Aveda Institute personnel shall develop remediation plans to address identified lapses.

3.12. Disciplinary Actions

3.12.1 Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and school policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with O'Briens Aveda Institute.

O'Briens Aveda Institute
400 Cornerstone Drive
Williston, VT 05495

Phone – 802.876.7044

I have read and understand the above policy. As an employee of O'Briens Aveda Institute, I further understand that any mishandling or abuse of student information or mishandling or abuse of O'Briens Aveda Institute's digital technology and/or network systems is cause for termination.

_____ _____

Signature Date