Data Confidentiality Policy for Alpha Academy Inc.

Introduction

Alpha Academy Inc. ("Alpha Academy," "we," "our," or "us") is committed to maintaining the confidentiality of personal and sensitive information entrusted to us by students, parents, guardians, staff, and other stakeholders. This Data Confidentiality Policy outlines our practices to protect confidential information from unauthorized access, use, disclosure, or loss. As a tuition-free public school, we prioritize the confidentiality of all data to foster a safe and secure educational environment.

Scope of the Policy

This policy applies to all confidential information collected, used, stored, and disclosed by Alpha Academy, including but not limited to information about students, parents, guardians, staff, and visitors. Confidential information includes any data that, if disclosed, could potentially harm individuals or compromise the integrity of Alpha Academy.

Definition of Confidential Information

Confidential information refers to any data or information that is not publicly available and is intended to be kept private. This includes but is not limited to:

- **Student Information:** Academic records, health information, disciplinary records, special education needs, and personal identifiers such as Social Security numbers.
- **Parent/Guardian Information:** Contact details, financial information, and any communications with the school.
- **Staff Information:** Employment records, payroll information, performance evaluations, and personal identifiers.
- **Operational Information:** Strategic plans, financial records, internal communications, and other proprietary information.

Principles of Confidentiality

Alpha Academy is guided by the following principles to ensure the confidentiality of information:

- **Need to Know:** Access to confidential information is granted only to individuals who require it to perform their job duties.

- **Minimum Necessary:** We limit the collection and use of confidential information to the minimum necessary to achieve the intended purpose.
- **Security Measures:** We implement robust security measures to protect confidential information from unauthorized access, use, disclosure, or loss.
- **Accountability:** All staff members are responsible for safeguarding confidential information and adhering to this policy.

Collection and Use of Confidential Information

Collection

Confidential information is collected through various means, including but not limited to:

- Enrollment forms and other school-related documentation.
- Online forms and applications.
- Direct communication with students, parents, guardians, and staff.
- Automated collection through our website and online platforms.

Use

Confidential information is used for purposes directly related to the functioning of Alpha Academy, including:

- Providing and managing educational services.
- Communicating with parents, guardians, and staff.
- Ensuring the health and safety of students and staff.
- Managing school operations, including enrollment, attendance, and staffing.
- Complying with legal and regulatory requirements.

Access to Confidential Information

Access Control

Access to confidential information is restricted based on the principle of least privilege. This means that individuals are granted access only to the information necessary for their job functions. Access control measures include:

- **Authentication:** Strong password policies and multi-factor authentication for accessing electronic systems.

- **Authorization:** Role-based access controls to ensure that only authorized personnel can access specific types of information.
- **Physical Security:** Secure storage for physical records, including locked filing cabinets and restricted access to sensitive areas.

Staff Responsibilities

All staff members are responsible for maintaining the confidentiality of information. This includes:

- Adhering to this policy and other relevant policies and procedures.
- Completing training on data confidentiality and security best practices.
- Reporting any suspected breaches of confidentiality to the designated authority.

Security Measures

We employ a range of security measures to protect confidential information, including:

- **Technical Measures:** Encryption, firewalls, intrusion detection systems, and regular security updates for electronic systems.
- **Organizational Measures:** Confidentiality agreements, regular training, and clear policies and procedures.
- **Physical Measures:** Secure storage for physical records, access controls for sensitive areas, and surveillance systems.

Disclosure of Confidential Information

We do not disclose confidential information to third parties except in the following circumstances:

- **With Consent:** When we have obtained explicit consent from the individual or their parent/guardian.
- **Legal Requirements:** To comply with legal obligations, such as court orders or subpoenas.
- **Health and Safety:** When necessary to protect the health and safety of students, staff, or the public.
- **Service Providers:** To third-party service providers who perform functions on our behalf, provided they agree to comply with our confidentiality policies and applicable laws.

Data Breach Response

In the event of a data breach, we will take immediate action to mitigate the impact and prevent further unauthorized access. Our data breach response plan includes:

- **Identification:** Identifying the nature and scope of the breach.
- **Containment:** Containing the breach to prevent further unauthorized access.
- **Assessment:** Assessing the impact of the breach on affected individuals and systems.
- **Notification:** Notifying affected individuals and relevant authorities as required by law.
- **Remediation:** Implementing measures to prevent future breaches and improve security.

Data Retention and Disposal

We retain confidential information only for as long as necessary to fulfill the purposes for which it was collected or as required by law. Once confidential information is no longer needed, we will securely delete or destroy it. This includes:

- **Electronic Data:** Secure deletion using industry-standard data wiping techniques.
- **Physical Records:** Shredding or incinerating paper records.

Training and Awareness

We provide regular training and awareness programs for staff on data confidentiality and security best practices. This includes:

- **Initial Training:** Comprehensive training for new staff members on confidentiality policies and procedures.
- **Ongoing Training:** Regular refresher courses and updates on new threats and best practices.
- **Awareness Campaigns:** Promoting a culture of confidentiality through posters, newsletters, and other communications.

Monitoring and Compliance

We regularly monitor compliance with this policy through audits, assessments, and reviews. Non-compliance may result in disciplinary action, up to and including termination of employment. Our compliance measures include:

- **Audits:** Regular audits of access controls, data handling practices, and security measures.
- **Assessments:** Periodic assessments of risks and vulnerabilities.
- **Reviews:** Regular reviews of policies and procedures to ensure they remain effective and up-to-date.

Updates to This Policy

We may update this Data Confidentiality Policy from time to time to reflect changes in our practices or legal requirements. When we make changes, we will update the "Effective Date" at the beginning of this policy and provide notice as required by law.

Contact Us

If you have any questions or concerns about this Data Confidentiality Policy or our data handling practices, please contact us at:

Alpha Academy Inc.
8030 Raeford Rd
Fayetteville, NC , 28304
it@alphaacademy.net
910-479-6355 Ext. 405

Conclusion

Alpha Academy Inc. is committed to protecting the confidentiality of personal and sensitive information. By adhering to this Data Confidentiality Policy, we aim to ensure that all confidential information is handled with the utmost care and in compliance with applicable laws and regulations. Thank you for supporting our commitment to data confidentiality.