office@newalternative.co.uk 07365 22517 https://newalternative.co.uk/

Information Security Policy

At **New Alternative Path**, we recognize that protecting the confidentiality, integrity, and availability of information is critical to maintaining trust with our students, partners, and stakeholders. This policy sets out our commitment to safeguarding all personal, academic, and organizational information against unauthorized access, disclosure, alteration, and loss.

Scope

This policy applies to all employees, consultants, contractors, systems, processes, and third parties that handle or have access to information owned or managed by the consultancy.

Objectives

1. **Confidentiality** – Ensure that sensitive information (e.g., student records, financial data, institutional agreements) is only accessible to authorized individuals.
2. **Integrity** – Protect information from unauthorized modification to guarantee accuracy and reliability.
3. **Availability** – Ensure that critical information and systems are available to authorized users whenever needed.

Policy Commitments

1. **Data Protection** – All personal and academic information will be collected, processed, and stored in compliance with applicable data protection laws and regulations.
2. **Access Control** – Access to information and systems will be restricted based on roles and responsibilities, using strong authentication and authorization mechanisms.
3. **Secure Communication** – Confidential data will be transmitted through secure, encrypted channels.
4. **Incident Management** – Any information security incident (e.g., data breach, unauthorized access) will be promptly reported, investigated, and resolved to minimize impact.
5. **Awareness & Training** – All staff and contractors will receive regular training on information security best practices and their responsibilities.
6. **Third-Party Security** – Partners and service providers handling sensitive data must adhere to equivalent security standards.
7. **Monitoring & Review** – Security controls, risks, and policies will be regularly reviewed and updated to address evolving threats.

8. **Business Continuity** – Measures will be in place to ensure the continued operation of critical services in the event of system failures or disasters.

Responsibility

- **Management** is responsible for implementing this policy and allocating resources for information security.
- **Employees and contractors** are responsible for adhering to security practices and reporting incidents.
- **Information Security Officer (or designated staff)** will monitor compliance and coordinate risk management.

Policy Review

This Information Security Policy will be reviewed annually or as required by changes in laws, technology, or business operations.

Date: 1st July 2025

Signed By: Gotse Gyorshevski

TO BE REVIEWED: SEPTEMBER 2026