Information Security Policy for the North West Aerospace Alliance

1. Purpose
The purpose of this Information Security Policy is to safeguard the information assets of the North West Aerospace Alliance (NWAA) and its stakeholders, including third parties, clients, customers, and the general public, within a secure environment. This policy outlines the principles and guidelines for the handling, use, and disposal of information to protect against unauthorised access, misuse, or loss, and ensure compliance with regulatory, legal, and contractual obligations.

NWAA aims to:

- Protect information against unauthorised access or misuse.
- Maintain the confidentiality of sensitive information.
- Ensure the integrity of information is preserved.
- Ensure the availability of information and systems to support business operations.
- Maintain business continuity processes.
- Comply with regulatory, contractual, and legal requirements.
- Maintain physical, logical, environmental, and communications security.
- Dispose of information securely when no longer needed.
- Investigate all information security incidents thoroughly.

Infringement of this policy may result in disciplinary action or criminal prosecution. This policy applies to all types of information, including:

- Electronic information systems (software, hardware, computers, and peripherals) owned by NWAA, whether accessed on or off business premises.
- NWAA's computer network.
- Paper-based materials.
- Electronic recording devices (video, audio, CCTV systems).

2. Policy Details

NWAA requires all users to exercise due care in the operation and use of its information systems.

2.1 Authorised Users of Information Systems
Except for information intended for public consumption, all users of NWAA's information systems must be formally authorised by the Data Protection Manager. Authorized users will have a unique user identity, and any passwords associated with these identities must not be shared.

Authorised users are responsible for the protection of NWAA's information that is in their possession. Confidential, personal, or private information must not be copied or transported without consideration of the following:

- Permission from the information owner.
- The risks associated with loss or misuse.
- How the information will be secured during transport and at its destination.

2.2 Acceptable Use of Information Systems

Users of NWAA's information systems are expected to use them in a lawful, honest, and responsible manner. Users must respect the rights and sensitivities of others and ensure that their use of the systems does not interfere with others' legitimate interests.

2.3 Information System Owners
The Directors of NWAA are responsible for ensuring that information systems under their control are adequately protected from unauthorised access, theft, and damage. They must ensure the availability of these systems to support business continuity and disaster recovery, particularly in the event of system failure or loss.

Key responsibilities of system owners include:

- Securing systems against unauthorized access and physical threats.
- Backing up data and ensuring data can be restored in the event of failure.
- Maintaining data accuracy.
- Using systems as intended and addressing misuse promptly.
- Retaining electronic access logs only for a justifiable period, ensuring compliance with data protection and legal requirements.
- Ensuring that any third parties entrusted with NWAA's data understand their security responsibilities.

2.4 Personal Information
Authorized users of information systems do not have a right to privacy in relation to their use of NWAA's information systems. Authorised officers may access or monitor personal data contained in any NWAA information system, including emails, web access logs, and file storage.

2.5 Breaches of Policy
Individuals in breach of this policy will be subject to disciplinary action, initiated by the CEO responsible for the relevant information system. This may include referral to the Police if necessary. NWAA will take legal action to prevent unauthorised use of its information systems and to protect its data assets.

3. Ownership and Responsibility

3.1 Data Protection Manager
The Data Protection Manager, has direct responsibility for maintaining this policy and providing guidance and advice on its implementation. The Data Protection Manager will oversee compliance and ensure that all employees are aware of and follow the policy.

3.2 Information System Owners
Information system owners within NWAA are responsible for implementing this policy within their areas of responsibility and ensuring adherence to its guidelines.

4. Conclusion
The North West Aerospace Alliance is committed to ensuring the security and integrity of its information assets. By adhering to this Information Security Policy, NWAA will protect sensitive data, maintain business operations, and comply with legal and regulatory requirements, ensuring a secure environment for all stakeholders.

For further information or queries about this policy, please contact:
DPO

Email: membership@aerospace.co.uk
Phone: 01772 648800