

Data Protection Policy for the North West Aerospace Alliance

Introduction The North West Aerospace Alliance (NWAA) is committed to ensuring that personal data is handled responsibly and in compliance with relevant data protection laws. As part of its operations, the NWAA may collect and process personal information about individuals, including employees, members, contractors, suppliers, and business contacts. This policy outlines how personal data is collected, stored, and used to meet legal requirements and protect individual privacy.

Purpose of This Policy This policy serves to ensure that NWAA:

- Complies with data protection laws and adheres to best practices in data handling.
- Protects the rights of data subjects, including staff, members, partners, and other individuals.
- Operates transparently in the collection and processing of personal data.
- Safeguards against data breaches and associated risks.

Scope This policy applies to:

- All staff, members, directors, and contractors of NWAA.
- All personal data collected and held by NWAA, which can include, but is not limited to, names, contact details, membership records, employment information, and business relationships.

It applies to all types of data, whether stored electronically or in paper format.

Data Protection Laws This policy aligns with the **General Data Protection Regulation (GDPR)** and the **Data Protection Act 2018**. These regulations govern the collection, storage, and processing of personal data and are designed to protect the rights of individuals. The key principles of data protection are as follows:

1. **Lawfulness, fairness, and transparency:** Personal data must be processed lawfully, fairly, and transparently.
2. **Purpose limitation:** Data must be collected for specified, legitimate purposes and not further processed in a way that is incompatible with those purposes.
3. **Data minimisation:** Personal data should be adequate, relevant, and limited to what is necessary.
4. **Accuracy:** Personal data must be accurate and kept up to date.
5. **Storage limitation:** Data should not be kept for longer than necessary.
6. **Integrity and confidentiality:** Data must be securely stored and protected from unauthorised access.
7. **Accountability:** NWAA must be able to demonstrate compliance with data protection principles.

Data Protection Risks NWAA recognises the following data protection risks and aims to mitigate them:

- **Breaches of confidentiality:** Unauthorised disclosure of personal data.
- **Lack of consent:** Using personal data without obtaining the proper consent or legal basis.
- **Reputational damage:** A breach of personal data security that could damage the reputation of NWAA.
- **Loss or corruption of data:** Data being lost, destroyed, or corrupted due to inadequate security measures.

Responsibilities

- **Board of Directors:** The Board is responsible for ensuring compliance with this policy and all legal data protection requirements.
- **Data Protection Officer (DPO):** The designated Data Protection Officer for NWAA, who is responsible for overseeing compliance with data protection laws, conducting training, and addressing any data protection concerns.

Key Responsibilities of the DPO:

- Maintain up-to-date knowledge of data protection laws and guidance.
- Conduct audits to ensure data protection compliance.
- Provide guidance and support for data protection queries.
- Address subject access requests (SARs) and other data rights.
- Ensure data security measures are effective and regularly updated.
- Approve any data processing contracts with third parties.

General Guidelines for Data Handling

- **Access to personal data:** Only authorised individuals should have access to personal data. Access should be based on job roles and responsibilities.
- **Training:** All employees and relevant individuals will receive training on data protection and privacy principles.
- **Confidentiality:** Personal data must not be shared informally or without consent, and unauthorised individuals should not have access.
- **Data accuracy:** Personal data must be kept accurate and up to date. Any inaccuracies should be corrected promptly.
- **Data security:** Personal data should be stored securely using password protection and encryption. Devices should be locked when not in use, and paper documents should be stored in secure locations.

Data Storage and Security

1. **Electronic storage:** Personal data must be stored on secure, password-protected systems. Data must be regularly backed up, and backup data should be stored securely.

2. **Paper records:** Any paper-based personal data should be stored securely in locked filing cabinets or rooms. When no longer required, paper records should be shredded and disposed of in confidential waste bags and certificate of secure disposal obtained.
3. **Portable media:** Removable media (e.g., USB drives, DVDs) containing personal data must be stored securely and encrypted when in use or at rest.

Data Usage

- Personal data should only be used for its intended purpose and should not be shared or disclosed to unauthorised individuals.
- Any data transfers outside the European Economic Area (EEA) must be conducted in compliance with GDPR, ensuring adequate protection for the data.
- Email is not a secure medium for sharing personal data, and alternative secure methods should be used when necessary.

Subject Access Requests (SARs) Individuals have the right to request access to personal data held about them by NWAA. A request must be made in writing to the Data Protection Officer (DPO) at the following contact:

Email: membership@aerospace.co.uk

Phone: 01772 648800

NWAA will respond to a subject access request within 30 days, as required by GDPR. To ensure security, the identity of the requester will be verified before any information is released.

Data Retention and Disposal

- Personal data should not be kept for longer than necessary and should be securely deleted or destroyed when no longer needed.
- Data retention periods will be reviewed regularly, and records will be kept only for as long as legally required or necessary for the purpose for which they were collected.

Data Transfers to Third Parties

- Data sharing with third parties will only occur when necessary and with appropriate safeguards in place.
- Contracts with third-party service providers handling personal data must include clauses that ensure compliance with data protection regulations.

Compliance and Review

- This policy will be reviewed annually to ensure it remains compliant with evolving data protection laws.
- NWAA will take prompt corrective actions in response to any data protection concerns, breaches, or non-compliance issues.

Contact Information For any questions or concerns regarding this policy or data protection practices, please contact:

Data Protection Officer (DPO)

Email: membership@aerospace.co.uk

Phone: 01772 648800

By adhering to this policy, the North West Aerospace Alliance ensures that personal data is managed safely, legally, and responsibly, upholding the privacy rights of all individuals, and maintaining trust within the aerospace community.