Document Title	Creation Date	Review Date	Version
IASF Data Privacy & Confidentiality Policy	30/10/2025	30/10/2026	1

IASF Data Privacy & Confidentiality Policy

1. Purpose

This policy protects the privacy and confidentiality of all members, clients, and partners by ensuring compliance with data protection laws (including GDPR) and ethical data management across all IASF operations.

2. Scope

This policy applies to all personal data held by the IASF, including that of members, clients, suppliers, and partners. It covers all IASF staff, contractors, and volunteers handling data, and all systems and platforms used for storing or processing data, including the IASF Member Portal, databases, and third-party applications.

3. Policy Statement

IASF is committed to maintaining the highest standards of data protection and confidentiality. All information collected or shared by the organisation will be used solely for legitimate purposes in line with its mission to support members and uphold welfare and professional standards.

4. Key Principles (Aligned with GDPR)

• Lawfulness, Fairness & Transparency – Data will be collected and processed only for clear, lawful purposes.

• Purpose Limitation – Data will be used solely for the purpose for which it was collected.

• Data Minimisation – Only the minimum necessary data will be collected.

• Accuracy – Data will be kept accurate and up to date.

• Storage Limitation – Data will be retained only as long as necessary.

• Integrity & Confidentiality – All data will be processed securely and protected from unauthorised access.

• Accountability – IASF will maintain documentation and procedures to demonstrate compliance.

Document Title	Creation Date	Review Date	Version
IASF Data Privacy & Confidentiality Policy	30/10/2025	30/10/2026	1

5. Categories of Data Collected

IASF may collect the following categories of data:
• Contact details (name, email, phone, address)
• Professional details (qualifications, membership level, CPD records)
• Payment information (membership fees, invoices)
• Communications (emails, forms, correspondence)
• Event participation records or feedback
Sensitive data (e.g. health or welfare information) will only be collected when necessary and with explicit consent.

6. Data Storage & Security

All personal data is stored securely using password-protected systems and encrypted databases. Access is restricted to authorised personnel only. Data is not shared externally unless legally required or necessary for membership services. Backups are maintained securely and updated regularly.

7. Data Sharing & Third Parties

IASF may use trusted third-party service providers such as website hosts, payment processors, or event platforms. All third parties must comply with GDPR and sign data protection agreements. IASF does not sell or share data for commercial purposes.

8. Confidentiality Obligations

• All directors, staff, contractors, and volunteers must keep member and client information strictly confidential.

• Confidential matters must not be discussed in public or online spaces.

• Personal or professional details must not be shared without written consent.

9. Member Rights

Under data protection law, members have the right to:
• Access their personal data
• Request correction or deletion of data
• Withdraw consent at any time
• Request data portability or restriction of processing
Requests should be made in writing to the IASF Data Protection Lead.

Document Title	Creation Date	Review Date	Version
IASF Data Privacy & Confidentiality Policy	30/10/2025	30/10/2026	1

10. Data Breach Procedure

In the event of a suspected data breach:

- The IASF Data Protection Lead must be notified immediately.
- The breach will be investigated within 72 hours.
- Affected parties and regulators (where required) will be informed promptly.
- Actions will be taken to mitigate risk and prevent recurrence.

11. Retention & Disposal

Data will be retained only for as long as required by law or membership necessity. Expired or unnecessary data will be securely deleted or anonymised in accordance with data retention schedules.

12. Responsibility & Review

The IASF Board is responsible for ensuring compliance with this policy. The Data Protection Lead oversees implementation, training, and monitoring. This policy is reviewed annually or whenever relevant legislation or regulations change.