Cyber Security & Data Protection Policy

1. Purpose and Scope

This policy sets out how Novi (Forward Ladies Limited) protects information, systems and personal data used in the course of business, including data belonging to clients and their staff or programme participants. Novi (Forward Ladies Limited) is a small limited company, without a formal internal governance structure such as a board or dedicated security team; accordingly, responsibility for security and data protection is held by the director, who ensures this policy is understood and followed by all employees.

This policy applies to all information, whether held electronically or on paper, and to all devices used to access or store business or client data (laptop, mobile phone, cloud accounts).

2. Roles and Responsibility

Novi (Forward Ladies Limited) holds overall responsibility for:

- Implementing and maintaining the controls described in this policy
- Making day-to-day decisions on data protection and information security
- Responding to any security incident or personal data breach
- Reviewing and updating this policy at least annually

Any employee is expected to follow this policy in their handling of business and client information, and to report any suspected security incident without delay.

Building a genuine security culture, proportionate to our size, means:

- Security and data protection are factored into real business decisions as they're made — for example, which platform or tool to use, or how a new associate is briefed — rather than treated as a separate exercise.
- Every new employee or associate is introduced to this policy and our expectations as part of onboarding, rather than left to discover them.
- This is reinforced consistently over time, not communicated once, through our Organisational Learning and Continuous Improvement process (Section 8).
- Anyone raising a concern is supported, not penalised — the goal is fixing the issue, not finding fault.

3. Data Protection and GDPR Compliance

The business processes personal data in accordance with the UK GDPR and the Data Protection Act 2018. In particular:

- Personal data is collected and processed only for specified, legitimate business purposes (e.g. client and participant contact management, programme delivery, invoicing).
- Personal data is kept accurate, limited to what is necessary, and retained only as long as needed for the purpose it was collected.
- Data subjects' rights (access, rectification, erasure, objection) are respected and can be exercised by contacting the business directly.
- Personal data is not shared with third parties except where necessary to deliver a service (e.g. a booking or payment platform) and where an appropriate data processing arrangement is in place.

- Novi (Forward Ladies Limited) is registered with the Information Commissioner's Office (ICO) as a data controller, registration reference ICO:00013516573.
- Where personal data is transferred outside the United Kingdom — including to associates, facilitators or speakers engaged internationally — such transfer is treated as a restricted transfer under Chapter V of the UK GDPR and is made only where the destination is subject to UK adequacy regulations, or where appropriate safeguards (such as the UK International Data Transfer Agreement or an equivalent addendum to the EU Standard Contractual Clauses) have been put in place, or another lawful transfer mechanism applies.

4. Device and Access Security

- All laptops and mobile devices used for business purposes are protected by a password / PIN / biometric lock.
- Device storage is encrypted (e.g. BitLocker on Windows, FileVault on Mac).
- Operating systems, applications and antivirus/anti-malware software are kept up to date with security patches applied promptly.
- Multi-factor authentication (MFA) is enabled on email, cloud storage and other business-critical accounts where available.
- Strong, unique passwords are used for business accounts, managed via a password manager.

5. Data Storage and Backup

- Business and client data is stored in reputable cloud services with encryption in transit and at rest (e.g. Microsoft 365 / Google Workspace).
- Data is backed up regularly, either automatically via cloud sync or through scheduled manual backups.
- Physical documents containing personal or confidential data are stored securely and disposed of by secure shredding when no longer required.

6. Removable Media and Remote Working

- Removable media (USB drives, external hard drives) is used only when necessary, is encrypted where it holds business or client data, and is scanned for malware before use.
- When working remotely (including from home or while travelling), the same device security controls in Section 4 apply. Public Wi-Fi is avoided for accessing sensitive data, or a VPN is used where this is unavoidable.

7. Incident Response

In the event of a suspected cyber security incident or personal data breach, Novi (Forward Ladies Limited) will:

- Take immediate steps to contain the incident (e.g. disconnect the affected device, revoke compromised credentials).
- Assess the scope and impact of the incident, including whether personal data has been compromised.
- Notify affected clients without undue delay where the incident affects their data or systems.
- Where personal data is affected and the breach is likely to result in a risk to individuals, report to the ICO within 72 hours of becoming aware, in line with UK GDPR requirements.
- Record the incident, actions taken and lessons learned, and update this policy or working practices as needed.

8. Organisational Learning and Continuous Improvement

Anyone working with us — the director, employees, or associates — who notices a security concern, near-miss, or improvement opportunity is expected to raise it as soon as possible, directly with the director. This includes anything from a suspicious email or a lost device to a suggestion for doing something more securely. There is no

blame attached to raising a concern, including where the person raising it was involved in causing it — the goal is fixing the issue, not finding fault.

- What was reported, when, and what was done about it is recorded in a dated log.
- At least once a year, alongside the annual policy review, we look back over anything logged that year to check it has been addressed and to spot any wider pattern worth acting on.
- Relevant lessons or good practice picked up from clients, sponsors, partners, or industry sources are considered for adoption, and reflected in this policy at the next review, or sooner if urgent.
- Associates and employees are made aware of any security-relevant change directly — for example, when a new engagement begins, or when this policy is updated.

9. Third Parties and Subcontractors

Where the business engages any third party or subcontractor who may access client data (for example, a bookkeeper, VA, or associate speaker/facilitator), reasonable steps are taken to ensure they handle that data securely and in line with this policy, including a written confidentiality or data processing agreement where appropriate.

10. Review

This policy is reviewed at least annually by Griselda Togobo, and following any significant security incident or change in how the business operates.

11. Risk Management

Novi maintains a lightweight risk log identifying the main information and cyber risks relevant to the business — for example, device loss or theft, phishing or account compromise, associate mishandling of data, or a third-party platform outage.

- As a small business, the director owns all identified risks; there is no wider group of risk owners, so competing objectives between multiple risk owners do not arise.
- Risk from third parties — associates, subcontractors, and software or platform providers — is considered when engaging them, including through our Associate Data Processing Agreement and by choosing established, reputable platforms (e.g. Microsoft 365).
- The risk log is reviewed at least annually, alongside this policy, and after any significant incident or regulatory change (for example, the addition of the UK GDPR restricted-transfer provisions in Section 3).
- Where a review identifies a new or changed risk, this policy or our working practices are updated accordingly.

Proportionate to the size of the business, we do not operate a formal, independently audited risk framework, a dedicated threat intelligence service, or a suitably qualified and experienced person (SQEP) function to approve risk decisions; risk decisions are made and reviewed directly by the director.

Approved by: Griselda Togobo Date: 12 August 2026