CONNECTBATCH LIMITED

Terms of Use

For Solutions Built Using Microsoft M365 Copilot and Related AI Services
Version 1.0 — 14-02-2026

1. Introduction

These Terms of Use govern access to and use of the **AI DOCUMENT PROCESSOR** ("the Solution"), provided by **CONNECTBATCH LIMITED** ("the ISV"), and used by **[NHS Organisation]** ("the Customer").
The Solution integrates with Microsoft technologies, including M365 Copilot and related AI capabilities, to support operational, administrative, and analytical workflows within a regulated NHS environment.

The purpose of this document is to clearly define:

- Each party's responsibilities
- Data protection and governance requirements
- Security expectations
- Appropriate use of AI features
- The limits of liability and functionality

2. Scope

This agreement applies to all NHS staff, contractors, and authorised users who interact with the ISV's solution within the Customer's Microsoft 365 tenant or approved environment.

The Terms cover:

- The ISV application logic
- Integration with Microsoft AI services
- Handling of data provided by NHS users
- System behaviour inside the NHS tenant

3. Roles and Responsibilities

3.1 The NHS Customer (Data Controller)

The Customer determines:

- The purpose and lawful basis for processing data
- What information users may input into the Solution
- Access permissions and user identity controls
- Retention, export, or deletion of data

3.2 The ISV (Solution Provider)

The ISV is responsible for:

- Application logic, functionality, and configuration
- Ensuring the Solution complies with NHS IG and DSPT standards
- Not storing or transferring NHS data outside agreed locations
- Ensuring any subprocessors are disclosed and compliant
- Providing documentation, onboarding guidance, and support
- Ensuring no disallowed data is collected or stored

3.3 Microsoft (Sub-Processor)

As the underlying cloud and AI platform provider, Microsoft is responsible for:

- Hosting the data inside the Customer's Microsoft 365 environment
- Processing data solely to deliver M365 Copilot and platform services
- Maintaining compliance with UK GDPR, NHS Cloud Security Principles, and DSPT-aligned commitments
- Ensuring customer data is **not used to train foundation models**
- Meeting all requirements of the NHS Enterprise Agreement terms

The ISV does *not* control Microsoft's processing but relies on NHS-approved contractual protections between Microsoft and the NHS.

4. Data Handling and Privacy

4.1 Categories of Data Processed

The Solution may process:

- Operational NHS data
- Technical/administrative documentation
- Application-specific configuration data
- De-identified or anonymised datasets
- User prompts and instructions

The Solution must NOT process:

- Patient Identifiable Data (PID) unless explicitly stated in a DPIA approved by the NHS Customer
- Special category personal data unless authorised
- Sensitive incident or security information outside agreed boundaries

4.2 Data Location

All data is processed:

- Within the Customer's Microsoft 365 tenant
- Using Microsoft-approved UK or region-specific environments compliant with NHS standards
- Without transfer to external systems unless contractually agreed

4.3 Data Ownership

The NHS Customer retains full ownership of:

- All inputs, outputs, and derived artifacts
- Any organisational data, content, or configuration

The ISV does not acquire ownership or usage rights except strictly for delivering the Solution.

5. AI-Specific Terms

5.1 Use of Microsoft AI Models

The Solution may rely on Microsoft foundation models for:

- Reasoning and natural language assistance
- Document summarisation and transformation
- Automation support
- Code or configuration generation

Microsoft does not use NHS data to train or improve these models.

5.2 Model Limitations

AI outputs:

- May contain inaccuracies
- Must be reviewed by NHS staff before making decisions
- Should not be used as the sole basis for clinical, legal, or safety-critical decisions
- Cannot override organisational policies or professional judgement

5.3 User Prompt Safety

Users must not input:

- PID unless authorised
- Live incidents or confidential security vulnerabilities
- Personal, financial, or sensitive staff information
- External copyrighted material beyond fair use

6. Security Requirements

The ISV Solution must:

- Follow NHS Data Security & Protection Toolkit (DSPT) expectations
- Apply secure coding practices
- Support MFA and Microsoft Entra protections
- Not reduce or bypass Microsoft 365 tenant security
- Undergo appropriate testing before deployment
- Ensure logs do not expose sensitive data

The NHS Customer must:

- Maintain secure identity and access management
- Ensure staff receive IG and cyber training
- Report incidents through local NHS processes

7. Logging, Monitoring, and Audit

The ISV may collect telemetry for:

- Performance monitoring
- Error diagnostics
- Usage analytics

…but:

- Telemetry must not include personal data unless contractually permitted
- Diagnostic data must not leave agreed regions
- The NHS Customer may request logs for audit or incident response

The NHS Customer may monitor use under its organisational policies.

8. Support and Maintenance

The ISV will:

- Provide support channels
- Deliver updates, security patches, and improvements
- Notify the Customer of material changes to functionality or data flows
- Provide documentation suitable for NHS onboarding and compliance reviews

9. Liability and Indemnity

The ISV:

- Is responsible for errors, defects, or breaches in its own code or configuration
- Is not liable for failures caused by Microsoft platform availability or behaviour
- Is not responsible for misuse by NHS users
- Shall maintain appropriate insurance for delivering digital services to the NHS

The NHS Customer:

- Is responsible for lawful processing decisions
- Is responsible for user behaviour and data entry
- Must ensure proper governance and review of outputs

10. Termination

On termination:

- Access to the Solution will be removed
- Any ISV-held data must be deleted within an agreed timeframe
- The NHS Customer may request an extraction or deletion certificate
- Documentation and audit trails must be maintained for regulatory purposes

11. Acceptance

By using the Solution, the NHS Customer and its users confirm that:

- They understand and accept these Terms of Use
- They will comply with organisational, regulatory, and contractual obligations
- They will use the Solution responsibly within the NHS governance framework

12. Third-Party Integrations

The Service may integrate with third-party systems or tools. Connectbatch is not responsible for the security, availability, or performance of any third-party services.

13. Governing Law

These Terms are governed by the laws of the United Kingdom unless otherwise specified in your organisation’s contract with Connectbatch.

14. Contact Information

For questions about these Terms or the Service, please contact: [Insert appropriate email or support contact]