COMPLIANCE WORKING RECORD

UK AI cyber-security code self-assessment report

Customer support response assistant. Assessment NFS-AI-CYB-006 dated 7 August 2026.

Document control

Field	Value
Organisation	Northfield Services Ltd
Document type	UK AI cyber-security code self-assessment report
Document reference	NFS-AI-CYB-006
Jurisdiction	United Kingdom
Version	1.0
Status	Ready for accountable review
Classification	Fictional sample
Prepared by	Morgan Hale, Director of Operations
Prepared on	7 August 2026
Rule pack	uk-ai-cyber-code-2026-08-07.1
Sources reviewed	7 August 2026
Generated	7 August 2026

Assessment record

Field	Value
Organisation	Northfield Services Ltd
Reference	NFS-AI-CYB-006
Subject	Customer support response assistant
Jurisdiction	United Kingdom
Accountable owner	Morgan Hale, Director of Operations

Field	Value
Assessment date	7 August 2026
Next review	5 February 2027
Status	Record complete for accountable review

Subject and operating context

A live supplier-hosted retrieval assistant connected to the support platform through a private API. It processes customer ticket text and approved knowledge extracts. The manual support route remains available during an incident or supplier outage.

Field	Recorded position
Stakeholder role	System operator
Deployment route	live
Lifecycle phase	maintenance
Criticality	medium
Data sensitivity	personal
Hosting model	Supplier-hosted model through a private API, with an application proxy in the Northfield cloud environment
External components	Northstar AI service, managed vector store, support platform connector, approved knowledge repository and cloud secrets manager
Security owner	Security Lead through incident queue SEC-IR and the on-call escalation route

Assessment outcome

14 supported items were assessed from the status and evidence records entered by the user.

Field	Value
Review position	Record complete for accountable review
Evidence found	14
Missing	0

Field	Value
Uncertain	0
Not applicable	0
Not assessable	0

Secure design: AI security awareness and role training

DSIT AI Cyber Code principle 1. Include AI-specific threats and mitigations in regularly reviewed training, tailored to relevant roles and responsibilities.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 1.

Evidence: NFS-AI-CYB-006-01: Training plan, attendance record, briefing or competence assessment. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure design: Security objectives and risk assessment

DSIT AI Cyber Code principles 2 and 3. Document the business requirement, security risks, risk owners, mitigations and acceptance criteria before deployment or material change.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 2.

Evidence: NFS-AI-CYB-006-02: Security risk assessment, design review or approval record. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure design: Adversarial, unexpected-input and failure resilience

DSIT AI Cyber Code principle 2. Design and test the system for relevant adversarial attacks, unexpected inputs, misuse and system failure.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 3.

Evidence: NFS-AI-CYB-006-03: Threat model, red-team report, abuse test or failure-mode test. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure design: Human responsibility and escalation

DSIT AI Cyber Code principle 4. Assign human responsibility for security decisions, exceptions, monitoring, incident handling and material changes.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 4.

Evidence: NFS-AI-CYB-006-04: RACI, named owner, escalation procedure or approval minute. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Assets and infrastructure: AI asset inventory and provenance

DSIT AI Cyber Code principle 5. Identify and track models, datasets, prompts, code, libraries, infrastructure, credentials and external components with ownership and version information.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 5.

Evidence: NFS-AI-CYB-006-05: Asset register, model inventory, bill of materials or version record. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: Security Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Assets and infrastructure: Secure infrastructure and least privilege

DSIT AI Cyber Code principle 6. Protect infrastructure, interfaces, credentials and environments using risk-based access, separation and least-privilege controls.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 6.

Evidence: NFS-AI-CYB-006-06: Architecture diagram, access review, secrets control or configuration evidence. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: Security Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Assets and infrastructure: Supply-chain security

DSIT AI Cyber Code principle 7. Assess AI-specific supplier and component risks, record dependencies and require relevant security information and commitments.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 7.

Evidence: NFS-AI-CYB-006-07: Supplier assessment, component register, contract clause or assurance report. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: Security Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Data, models and prompts: Data, model and prompt documentation

DSIT AI Cyber Code principle 8. Document material data, models and prompts, including origin, handling, changes, access and limitations needed for security operations.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 8.

Evidence: NFS-AI-CYB-006-08: Data sheet, model card, prompt register or change history. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Testing and communication: Security testing and evaluation

DSIT AI Cyber Code principle 9. Run appropriate security testing before release and after material change, with defined acceptance, remediation and retest evidence.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 9.

Evidence: NFS-AI-CYB-006-09: Security test plan, evaluation report, defect log or retest evidence. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Testing and communication: End-user and affected-entity communication

DSIT AI Cyber Code principle 10. Provide relevant security information, limitations, safe-use instructions, reporting routes and material change notices to users and affected parties.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 10.

Evidence: NFS-AI-CYB-006-10: User notice, safety instruction, reporting route or release communication. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure operation: Security updates, patches and mitigations

DSIT AI Cyber Code principle 11. Maintain a process to identify, prioritise, communicate, test and deploy security updates, patches and mitigations.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 11.

Evidence: NFS-AI-CYB-006-11: Patch procedure, vulnerability queue, release record or customer notice. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure operation: Behaviour monitoring and anomaly response

DSIT AI Cyber Code principle 12. Monitor relevant system behaviour, security events, misuse and performance changes with thresholds, owners and response routes.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 12.

Evidence: NFS-AI-CYB-006-12: Monitoring plan, alert configuration, log review or response record. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Secure operation: Incident response and recovery

DSIT AI Cyber Code principles 3, 10 and 12. Connect AI-specific incidents to tested containment, investigation, recovery, communication and learning processes.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 13.

Evidence: NFS-AI-CYB-006-13: Incident plan, exercise, recovery test or post-incident review. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

End of life: Secure data and model disposal

DSIT AI Cyber Code principle 13. Define and evidence secure disposal of models, data, prompts, credentials, infrastructure and retained copies at end of life.

Result: Evidence identified. The organisation recorded implementation evidence, its type, the control owner and a review date that is not later than the assessment date.

Applicability: Applies. Basis: The recorded ai system or service facts place this item within the review scope. Confirmed in NFS-AI-CYB-006-SCOPE, section 14.

Evidence: NFS-AI-CYB-006-14: Retirement plan, deletion record, access revocation or supplier certificate. Owner-confirmed copy held in the controlled governance folder. Type: Controlled document and review record.

Owner: AI Governance Lead. Last tested or reviewed: 5 August 2026.

Action: None recorded. Due: Not set.

Open actions and unresolved facts

- No unresolved record gaps were produced by the supported checks.

Limitations

- The DSIT AI Cyber Security Code of Practice is voluntary. This tool does not certify security or conformity with a standard.

- A recorded control does not prove operational effectiveness. Review the underlying evidence and test results.

- The result is based only on the facts, status choices and evidence references entered by the user.

- Official materials, systems and operating facts can change. Re-run the assessment after material change and review the cited sources before approval.

Official sources

Source	Provision	Date	Link
Department for Science, Innovation and Technology: Code of Practice for the Cyber Security of AI	Principles 1 to 13	7 August 2026	https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice/code-of-practice-for-the-cyber-security-of-ai
Department for Science, Innovation and Technology: Implementation Guide for the AI Cyber Security Code of Practice	Implementation measures and evidence examples	7 August 2026	https://assets.publishing.service.gov.uk/media/679cae441d14e76535afb630/Implementation_Guide_for_the_AI_Cyber_Security_Code_of_Practice.pdf
National Cyber Security Centre: Guidelines for secure AI system development	Secure design, development, deployment and operation	7 August 2026	https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development