**AI GOVERNANCE POLICY TEMPLATE FOR MANAGED SERVICE PROVIDERS**

**Version:** 1.0  
**Effective Date:** [INSERT DATE]  
**Last Updated:** [INSERT DATE]  
**Next Review:** [INSERT DATE + 12 MONTHS]  
**Document Owner:** [Chief Technology Officer / Chief Information Security Officer]  
**Approved By:** [Chief Executive Officer]

**EXECUTIVE SUMMARY**

This AI Governance Policy establishes comprehensive guidelines for the responsible development, procurement, deployment, and use of Artificial Intelligence (AI) systems within [MSP COMPANY NAME] and across client environments. As a Managed Service Provider, we recognise that AI technologies present both transformational opportunities and significant risks that require careful governance to protect our business, our clients, and the individuals whose data we process.

This policy is designed to ensure compliance with UK data protection laws, industry regulations, and emerging AI governance standards while enabling innovation and competitive advantage through secure AI adoption.

**1. PURPOSE AND SCOPE**

**1.1 Purpose**

This policy aims to:

* Establish clear governance frameworks for AI systems throughout their lifecycle
* Ensure compliance with UK GDPR, data protection laws, and sector-specific regulations
* Mitigate risks associated with AI development, deployment, and operation
* Promote responsible and ethical AI practices aligned with our company values
* Protect client data, intellectual property, and competitive advantages
* Enable safe innovation and competitive differentiation through AI technologies
* Provide clear guidance for employees, contractors, and third-party vendors

**1.2 Scope**

This policy applies to:

**Personnel:**

* All [MSP COMPANY NAME] employees, contractors, consultants, and temporary staff
* Third-party vendors and suppliers providing AI-related services
* Client personnel accessing AI systems deployed in their environments

**AI Systems and Technologies:**

* Generative AI tools (e.g., ChatGPT, Claude, Gemini, Microsoft Copilot)
* Machine learning models and algorithms
* AI-powered automation and orchestration tools
* Predictive analytics and business intelligence systems
* AI-enabled cybersecurity and monitoring solutions
* Natural language processing and computer vision systems
* Any software or service that incorporates AI capabilities

**Data and Information:**

* Client data and personal information
* Company proprietary information and trade secrets
* System configurations and security intelligence
* Business strategies and competitive information
* Employee personal data and HR information

**1.3 Regulatory Context**

This policy addresses requirements under:

* UK General Data Protection Regulation (UK GDPR)
* Data Protection Act 2018
* Computer Misuse Act 1990
* Equality Act 2010
* Sector-specific regulations (where applicable)
* Client contractual obligations and service level agreements

**2. DEFINITIONS**

**Artificial Intelligence (AI):** Systems that can perform tasks typically requiring human intelligence, including machine learning, natural language processing, computer vision, and automated decision-making.

**AI System:** Any software, hardware, or service that incorporates AI technologies to process data, make predictions, or automate decisions.

**AI Model:** The mathematical representation or algorithm trained on data to perform specific AI tasks.

**Algorithmic Decision-Making:** Automated processing of personal data that produces legal effects or significantly affects individuals.

**Bias:** Systematic errors or prejudices in AI systems that result in unfair treatment of individuals or groups.

**Data Controller:** The entity that determines the purposes and means of processing personal data.

**Data Processor:** The entity that processes personal data on behalf of a data controller.

**Data Subject:** An identified or identifiable natural person whose personal data is processed.

**High-Risk AI:** AI systems that pose significant risks to health, safety, fundamental rights, or have substantial societal impact.

**Personal Data:** Any information relating to an identified or identifiable natural person.

**Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious beliefs, health data, biometric data, or data concerning sex life or sexual orientation.

**3. AI GOVERNANCE FRAMEWORK**

**3.1 AI Governance Structure**

**AI Governance Board**

* **Chair:** Chief Technology Officer
* **Members:** Chief Information Security Officer, Head of Compliance, Data Protection Officer, Head of Client Services, Senior Technical Architect
* **Responsibilities:** Strategic AI oversight, policy approval, risk assessment, incident response
* **Meeting Frequency:** Monthly, with emergency sessions as required

**AI Risk Committee**

* **Chair:** Chief Information Security Officer
* **Members:** Security Analysts, Senior Engineers, Compliance Specialists
* **Responsibilities:** Technical risk assessment, security evaluation, monitoring implementation
* **Meeting Frequency:** Bi-weekly

**AI Implementation Teams**

* **Leads:** Department Heads and Senior Technical Staff
* **Members:** Engineers, Analysts, Project Managers assigned to specific AI initiatives
* **Responsibilities:** Day-to-day implementation, testing, documentation, user training

**3.2 Roles and Responsibilities**

**Chief Executive Officer**

* Ultimate accountability for AI governance and compliance
* Approval of high-risk AI deployments
* Resource allocation for AI governance activities

**Chief Technology Officer**

* AI strategy development and implementation oversight
* Technical architecture and standards approval
* Cross-functional coordination of AI initiatives

**Chief Information Security Officer**

* AI security risk assessment and mitigation
* Security architecture and control implementation
* Incident response and breach management

**Data Protection Officer**

* Privacy impact assessment for AI systems
* Data protection compliance monitoring
* Data subject rights management in AI contexts

**Department Managers**

* Team training and awareness programs
* Local AI governance implementation
* Escalation of AI-related concerns

**All Employees**

* Compliance with AI usage policies and procedures
* Reporting of AI-related security incidents or concerns
* Participation in mandatory AI training programs

**4. AI PRINCIPLES AND ETHICS**

**4.1 Core Principles**

**Transparency and Explainability**

* AI decisions affecting clients or individuals must be explainable
* Clear documentation of AI system capabilities and limitations
* Open communication about AI usage in client services

**Fairness and Non-discrimination**

* AI systems must not unfairly discriminate against individuals or groups
* Regular bias testing and mitigation measures required
* Equal treatment regardless of protected characteristics

**Privacy and Data Protection**

* Privacy by design in all AI implementations
* Strict data minimisation and purpose limitation
* Strong security controls for personal data processing

**Human Oversight and Control**

* Meaningful human review of AI decisions
* Clear escalation procedures for AI system failures
* Human intervention capabilities in all automated processes

**Accountability and Responsibility**

* Clear ownership and responsibility for AI system outcomes
* Comprehensive audit trails and logging
* Regular assessment and improvement of AI systems

**Security and Robustness**

* Strong cybersecurity controls throughout AI lifecycle
* Resilience against adversarial attacks and manipulation
* Comprehensive testing and validation procedures

**4.2 Prohibited AI Practices**

The following AI applications are strictly prohibited:

* **Surveillance and Monitoring:** AI systems for employee surveillance beyond legitimate security monitoring
* **Social Credit Systems:** AI used to score or rank individuals based on social behaviour
* **Emotion Recognition:** AI systems claiming to infer emotions, intentions, or psychological states from biometric data
* **Predictive Policing:** AI systems predicting individual criminal behaviour
* **Mass Personal Data Profiling:** Automated profiling for marketing without explicit consent
* **Discrimination:** AI systems designed to discriminate based on protected characteristics

**5. AI RISK MANAGEMENT FRAMEWORK**

**5.1 Risk Assessment Methodology**

We adopt a risk-based approach based on the NIST AI Risk Management Framework, incorporating the four core functions:

**GOVERN**

* Establish AI governance culture and accountability
* Integrate AI considerations into organisational risk management
* Maintain awareness of AI developments and regulatory changes

**MAP**

* Identify and categorise AI systems and their contexts
* Map AI risks to business objectives and stakeholder impacts
* Document AI system capabilities, limitations, and dependencies

**MEASURE**

* Implement monitoring and testing of AI system performance
* Track key performance indicators and risk metrics
* Conduct regular audits and assessments

**MANAGE**

* Implement controls to mitigate identified risks
* Respond to incidents and emerging risks
* Continuously improve AI governance processes

**5.2 Risk Categories**

**Technical Risks**

* Model performance degradation or failure
* Adversarial attacks and data poisoning
* System integration and compatibility issues
* Scalability and resource constraints

**Operational Risks**

* Dependency on AI vendors and third parties
* Skills gaps and training requirements
* Process disruption during AI implementation
* Service availability and business continuity

**Legal and Compliance Risks**

* Data protection violations and privacy breaches
* Discrimination and bias in AI decisions
* Intellectual property infringement
* Regulatory non-compliance and enforcement action

**Reputational Risks**

* Client trust and confidence erosion
* Public relations and media scrutiny
* Competitive disadvantage from AI failures
* Brand damage from ethical concerns

**Financial Risks**

* Implementation costs and budget overruns
* Liability for AI system failures or errors
* Regulatory fines and legal costs
* Revenue loss from service disruptions

**5.3 Risk Classification Matrix**

| **Risk Level** | **Likelihood** | **Impact** | **Examples** |
| --- | --- | --- | --- |
| **Critical** | High | High | AI system processing special category data with bias issues |
| **High** | High | Medium | Generative AI tools exposing client confidential information |
| **Medium** | Medium | Medium | Automated monitoring tools with false positive rates |
| **Low** | Low | Low | AI-powered documentation tools for internal use only |

**5.4 Risk Mitigation Strategies**

**Technical Controls**

* Multi-factor authentication for AI system access
* Encryption of data at rest and in transit
* Regular security testing and vulnerability assessments
* Automated monitoring and alerting systems

**Administrative Controls**

* Clear policies and procedures for AI usage
* Regular training and awareness programs
* Access controls and segregation of duties
* Incident response and business continuity plans

**Physical Controls**

* Secure data centres and computing infrastructure
* Environmental monitoring and protection
* Physical access controls and surveillance
* Secure disposal of AI-related hardware and media

**6. APPROVED AI TOOLS AND SERVICES**

**6.1 Enterprise-Approved AI Platforms**

**Tier 1 - Approved for Client Data Processing**

*Microsoft 365 Copilot (Business/Enterprise)*

* **Use Cases:** Document creation, email assistance, data analysis
* **Data Handling:** Zero retention, EU data residency available
* **Security Controls:** Enterprise DLP, audit logging, admin controls
* **Approval Level:** Department Manager
* **Review Date:** [INSERT DATE + 6 MONTHS]

*Azure AI Foundry*

* **Use Cases:** Custom AI application development, ML model hosting
* **Data Handling:** Customer-controlled data residency and retention
* **Security Controls:** Full enterprise security stack, compliance certifications
* **Approval Level:** AI Governance Board
* **Review Date:** [INSERT DATE + 6 MONTHS]

*Anthropic Claude Enterprise*

* **Use Cases:** Complex analysis, research, strategy development
* **Data Handling:** Zero retention, configurable privacy controls
* **Security Controls:** Enterprise SSO, audit logs, admin dashboard
* **Approval Level:** CISO Approval Required
* **Review Date:** [INSERT DATE + 6 MONTHS]

**Tier 2 - Approved for Internal Use Only**

*GitHub Copilot Enterprise*

* **Use Cases:** Code development, documentation, automation scripts
* **Data Handling:** Enterprise data protections, audit capabilities
* **Security Controls:** Code scanning, security policies, admin controls
* **Approval Level:** CTO Approval Required
* **Review Date:** [INSERT DATE + 6 MONTHS]

*Microsoft Security Copilot*

* **Use Cases:** Security analysis, threat detection, incident response
* **Data Handling:** Microsoft security infrastructure protections
* **Security Controls:** Integrated security policies, audit logging
* **Approval Level:** CISO Approval Required
* **Review Date:** [INSERT DATE + 6 MONTHS]

**6.2 Prohibited AI Tools**

**Consumer AI Services** (Prohibited for Business Use)

* ChatGPT Free/Plus (OpenAI)
* Google Bard/Gemini (Consumer)
* xAI Grok (All Tiers)
* DeepSeek AI (All Tiers)
* Any AI service without enterprise data protections

**High-Risk AI Categories**

* Facial recognition and biometric analysis tools
* Emotion detection and psychological profiling systems
* Social media monitoring and sentiment analysis tools (without explicit consent)
* Automated decision-making tools affecting employment or financial decisions

**6.3 AI Tool Approval Process**

**Step 1: Initial Assessment**

* Business justification and use case documentation
* Vendor security and privacy assessment
* Data flow mapping and classification
* Initial risk assessment

**Step 2: Technical Evaluation**

* Security architecture review
* Integration testing and validation
* Performance and scalability assessment
* Documentation and training requirements

**Step 3: Legal and Compliance Review**

* Data protection impact assessment (DPIA)
* Contract and terms of service review
* Regulatory compliance verification
* Client notification requirements

**Step 4: Approval and Implementation**

* AI Governance Board review and approval
* Implementation planning and testing
* User training and documentation
* Monitoring and review procedures

**7. DATA GOVERNANCE FOR AI SYSTEMS**

**7.1 Data Classification and Handling**

**Client Data**

* **Definition:** Any data owned by or relating to our clients
* **AI Usage:** Only with explicit client consent and approved tools
* **Protection Level:** Highest security controls and monitoring
* **Retention:** Client-specified retention periods only

**Company Confidential Data**

* **Definition:** Proprietary information, trade secrets, business strategies
* **AI Usage:** Internal tools only, with executive approval
* **Protection Level:** Strong access controls and encryption
* **Retention:** Business requirement-based retention

**Personal Data**

* **Definition:** Data relating to identified or identifiable individuals
* **AI Usage:** Strict purpose limitation and lawful basis required
* **Protection Level:** UK GDPR compliance mandatory
* **Retention:** Legal and business requirement minimums

**Public Data**

* **Definition:** Information available in the public domain
* **AI Usage:** Permitted with appropriate attribution
* **Protection Level:** Standard security controls
* **Retention:** Standard business retention policies

**7.2 Data Processing Principles**

**Lawfulness, Fairness, and Transparency**

* Clear lawful basis for all AI data processing
* Fair and transparent AI system operation
* Comprehensive privacy notices and documentation

**Purpose Limitation**

* AI systems used only for specified, legitimate purposes
* No secondary use without additional lawful basis
* Clear boundaries on AI model training and improvement

**Data Minimisation**

* Process only data necessary for AI system objectives
* Regular review and reduction of data sets
* Automated data lifecycle management

**Accuracy**

* Ensure data quality and accuracy for AI training
* Regular validation and correction procedures
* Clear processes for handling inaccurate AI outputs

**Storage Limitation**

* Time-limited retention of AI training and processing data
* Automated deletion and anonymisation procedures
* Regular review of data retention requirements

**Integrity and Confidentiality**

* Strong security controls throughout AI data lifecycle
* Protection against unauthorised access and processing
* Comprehensive backup and recovery procedures

**7.3 Special Category Data**

Processing of special category data (health, biometric, genetic, etc.) in AI systems requires:

* **Explicit Consent:** Clear, informed consent from data subjects
* **Legal Basis:** Additional lawful basis under UK GDPR Article 9
* **Enhanced Security:** Additional technical and organisational measures
* **Impact Assessment:** Mandatory DPIA with expert review
* **Regular Review:** Quarterly assessment of necessity and proportionality

**8. CLIENT AI SERVICES FRAMEWORK**

**8.1 AI Service Delivery Models**

**AI-Enhanced Managed Services**

* Integration of approved AI tools into existing service delivery
* Enhanced monitoring, automation, and predictive analytics
* Client notification and consent for AI-powered services
* Transparent reporting of AI involvement in service delivery

**AI Advisory and Consulting**

* Strategic AI adoption planning and roadmap development
* AI vendor evaluation and selection support
* AI governance and policy development assistance
* Training and change management for AI implementations

**Custom AI Solutions**

* Development of bespoke AI applications for client needs
* Integration with client systems and data sources
* Ongoing maintenance and optimisation services
* Full documentation and knowledge transfer

**8.2 Client Consent and Communication**

**Pre-Implementation Requirements**

* Written client consent for AI system deployment
* Clear explanation of AI capabilities and limitations
* Documentation of data processing implications
* Agreement on monitoring and oversight procedures

**Ongoing Communication**

* Regular reporting on AI system performance and outcomes
* Notification of any AI-related incidents or issues
* Updates on AI system changes or improvements
* Annual review of AI service agreements

**Transparency Obligations**

* Clear labelling of AI-generated content or decisions
* Explanation of AI system logic and decision factors
* Documentation of human oversight and intervention points
* Open communication about AI limitations and risks

**8.3 Client Data Protection**

**Data Processing Agreements**

* Comprehensive DPAs covering all AI data processing
* Clear specification of data controller/processor roles
* Detailed security and privacy requirements
* Incident notification and response procedures

**Technical Safeguards**

* Encryption of client data at rest and in transit
* Logical separation of client data in multi-tenant systems
* Regular security testing and vulnerability assessments
* Comprehensive access logging and monitoring

**Organisational Measures**

* Staff training on client data protection requirements
* Clear procedures for handling client data in AI systems
* Regular audits and compliance assessments
* Incident response and breach notification procedures

**9. IMPLEMENTATION GUIDELINES**

**9.1 AI System Development Lifecycle**

**Phase 1: Planning and Design**

* Business case development and approval
* Risk assessment and mitigation planning
* Data requirements analysis and sourcing
* Technical architecture and design documentation

**Phase 2: Development and Testing**

* Secure development practices and code review
* Comprehensive testing including bias and fairness assessment
* Security testing and vulnerability assessment
* User acceptance testing and validation

**Phase 3: Deployment and Integration**

* Phased deployment with monitoring and feedback
* Integration testing with existing systems
* User training and documentation
* Monitoring and alerting configuration

**Phase 4: Operation and Maintenance**

* Ongoing monitoring and performance assessment
* Regular security and compliance reviews
* Model retraining and improvement processes
* Incident response and issue resolution

**Phase 5: Decommission and Disposal**

* Secure data deletion and system shutdown
* Documentation and knowledge preservation
* Asset disposal and vendor contract termination
* Lessons learned and process improvement

**9.2 Security Requirements**

**Access Control**

* Multi-factor authentication for all AI system access
* Role-based access control with principle of least privilege
* Regular access reviews and recertification
* Automated provisioning and deprovisioning processes

**Data Protection**

* Encryption of data at rest using AES-256 or equivalent
* Encryption of data in transit using TLS 1.3 or equivalent
* Key management using hardware security modules (HSMs)
* Regular encryption key rotation and management

**Network Security**

* Network segmentation and micro-segmentation for AI systems
* Intrusion detection and prevention systems (IDS/IPS)
* Web application firewalls (WAF) for AI web services
* Regular network security assessments and penetration testing

**Monitoring and Logging**

* Comprehensive logging of all AI system activities
* Real-time monitoring and alerting for security events
* Log retention and analysis for forensic investigations
* Integration with security information and event management (SIEM)

**9.3 Training and Awareness**

**Mandatory Training Programs**

* AI fundamentals and business applications
* Data protection and privacy in AI contexts
* Security best practices for AI systems
* Ethical considerations and bias awareness

**Role-Specific Training**

* Technical staff: AI development and deployment security
* Management: AI governance and risk management
* Sales and client services: AI capability and limitation communication
* Compliance: AI regulatory requirements and assessment

**Ongoing Education**

* Monthly AI governance and security updates
* Quarterly workshops on emerging AI technologies
* Annual comprehensive AI policy training
* External conference and certification support

**10. MONITORING AND COMPLIANCE**

**10.1 Performance Monitoring**

**AI System Performance Metrics**

* Model accuracy, precision, recall, and F1 scores
* Response time and throughput measurements
* Error rates and failure analysis
* User satisfaction and feedback scores

**Business Impact Metrics**

* Service delivery improvement measurements
* Cost reduction and efficiency gains
* Client satisfaction and retention rates
* Revenue impact and ROI analysis

**Security and Compliance Metrics**

* Security incident frequency and severity
* Data protection compliance scores
* Audit finding resolution rates
* Training completion and assessment scores

**10.2 Audit and Assessment**

**Internal Audits**

* Quarterly AI system security assessments
* Annual comprehensive AI governance reviews
* Ongoing compliance monitoring and testing
* Regular risk assessment updates

**External Audits**

* Annual third-party security assessments
* Compliance audits for regulatory requirements
* Client-requested AI system reviews
* Certification and accreditation maintenance

**Continuous Monitoring**

* Automated compliance checking and reporting
* Real-time security monitoring and alerting
* Performance dashboard and metrics tracking
* Incident detection and response procedures

**10.3 Reporting and Documentation**

**Governance Reporting**

* Monthly AI Governance Board reports
* Quarterly business impact and ROI analysis
* Annual AI strategy and policy reviews
* Ad-hoc incident and issue reports

**Compliance Documentation**

* Data protection impact assessments (DPIAs)
* AI system design and architecture documentation
* Security control implementation evidence
* Training records and competency assessments

**Client Reporting**

* Regular AI service performance reports
* Incident notification and resolution updates
* Annual AI governance and compliance summaries
* On-demand transparency and explainability reports

**11. INCIDENT RESPONSE AND BUSINESS CONTINUITY**

**11.1 AI Incident Classification**

**Severity 1 - Critical**

* AI system complete failure affecting client services
* Confirmed data breach involving AI systems
* Discriminatory AI decisions affecting individuals
* Regulatory investigation or enforcement action

**Severity 2 - High**

* AI system performance degradation affecting service quality
* Suspected security incident involving AI systems
* Client complaint about AI system behaviour
* Significant bias or fairness concerns identified

**Severity 3 - Medium**

* AI system minor performance issues
* Policy violation or non-compliance incident
* Training data quality concerns
* Vendor service disruption affecting AI capabilities

**Severity 4 - Low**

* AI system maintenance or planned downtime
* Minor configuration or performance adjustments
* User error or training needs identified
* Documentation or process improvement opportunities

**11.2 Incident Response Procedures**

**Immediate Response (0-4 hours)**

* Incident detection and initial assessment
* Stakeholder notification and communication
* Immediate containment and stabilisation actions
* Evidence preservation and investigation initiation

**Investigation Phase (4-24 hours)**

* Detailed forensic analysis and root cause investigation
* Impact assessment and risk evaluation
* Client and regulatory notification as required
* Corrective action planning and implementation

**Recovery Phase (24-72 hours)**

* System restoration and service recovery
* Ongoing monitoring and stability verification
* Communication updates to stakeholders
* Documentation and lessons learned capture

**Post-Incident Phase (72+ hours)**

* Comprehensive incident analysis and reporting
* Process improvement and policy updates
* Training and awareness program updates
* Follow-up monitoring and validation

**11.3 Business Continuity Planning**

**AI System Dependencies**

* Identification of critical AI systems and dependencies
* Alternative service delivery procedures
* Vendor contingency and backup arrangements
* Client communication and expectation management

**Disaster Recovery**

* AI system backup and recovery procedures
* Data backup and restoration processes
* Alternative infrastructure and service arrangements
* Testing and validation of recovery capabilities

**Communication Plans**

* Internal communication procedures and escalation
* Client notification and update procedures
* Regulatory reporting and compliance requirements
* Media and public relations management

**12. VENDOR AND THIRD-PARTY MANAGEMENT**

**12.1 AI Vendor Assessment**

**Security and Privacy Evaluation**

* Comprehensive security architecture review
* Data protection and privacy policy assessment
* Compliance certification and audit verification
* Business continuity and disaster recovery capabilities

**Technical Capabilities Assessment**

* AI model performance and accuracy evaluation
* Scalability and integration capabilities
* Support and maintenance service levels
* Documentation and training quality

**Legal and Commercial Terms**

* Contract terms and service level agreements
* Data processing and liability provisions
* Intellectual property and licensing terms
* Termination and data return procedures

**12.2 Ongoing Vendor Management**

**Performance Monitoring**

* Regular service level and performance reviews
* Security and compliance monitoring
* Financial stability and business continuity assessment
* Innovation and technology roadmap evaluation

**Risk Management**

* Vendor risk assessment and mitigation
* Regular security and compliance audits
* Incident response and communication procedures
* Business continuity and contingency planning

**Relationship Management**

* Regular business reviews and strategic planning
* Technical support and escalation procedures
* Contract renewal and renegotiation processes
* Knowledge transfer and training coordination

**13. COMPLIANCE AND REGULATORY REQUIREMENTS**

**13.1 Data Protection Compliance**

**UK GDPR Requirements**

* Lawful basis assessment for all AI data processing
* Data subject rights management and response procedures
* Data protection impact assessments (DPIAs) for high-risk AI
* Breach notification and reporting procedures

**Data Processing Documentation**

* Records of processing activities for AI systems
* Data flow mapping and classification
* Data retention and deletion procedures
* Cross-border data transfer assessments

**Individual Rights Management**

* Right of access to AI system decisions and logic
* Right to rectification of inaccurate AI training data
* Right to erasure and data portability
* Right to object to automated decision-making

**13.2 Sector-Specific Compliance**

**Financial Services**

* FCA guidance on AI governance and risk management
* Consumer Duty obligations for AI-powered services
* Operational resilience requirements for AI systems
* Model risk management and validation procedures

**Healthcare**

* MHRA guidance on AI as a medical device
* NHS data security and protection standards
* Clinical governance and safety requirements
* Research and development ethical considerations

**Public Sector**

* Government AI procurement and deployment guidance
* Public sector equality duty considerations
* Transparency and accountability requirements
* Security clearance and vetting procedures

**13.3 Emerging Regulatory Requirements**

**AI Act Compliance (Future)**

* High-risk AI system identification and classification
* Conformity assessment and CE marking requirements
* Post-market monitoring and incident reporting
* Transparency and explainability obligations

**UK AI Regulation Development**

* Monitoring of UK government AI policy development
* Engagement with regulatory consultations and guidance
* Preparation for potential AI-specific legislation
* Industry best practice and standard adoption

**14. POLICY ENFORCEMENT**

**14.1 Violation Categories**

**Minor Violations**

* Failure to complete mandatory AI training
* Use of unapproved AI tools for non-sensitive tasks
* Inadequate documentation of AI system usage
* Minor security configuration errors

**Serious Violations**

* Processing client data through prohibited AI services
* Failure to conduct required risk assessments
* Inadequate security controls for AI systems
* Non-compliance with client data processing agreements

**Critical Violations**

* Deliberate bypass of AI security controls
* Unauthorised disclosure of client data through AI systems
* Discriminatory use of AI systems affecting individuals
* Failure to report known AI security incidents

**14.2 Disciplinary Actions**

**Minor Violations**

* Verbal warning and corrective training
* Written documentation and performance monitoring
* Additional training and competency assessment
* Temporary restriction of AI system access

**Serious Violations**

* Formal written warning and performance improvement plan
* Suspension of AI system access privileges
* Mandatory additional training and certification
* Potential impact on performance reviews and advancement

**Critical Violations**

* Formal disciplinary action up to and including termination
* Legal action for breach of contract or confidentiality
* Reporting to professional bodies or regulatory authorities
* Financial liability for damages and remediation costs

**14.3 Appeals and Resolution**

**Appeals Process**

* Right to appeal disciplinary decisions
* Independent review by senior management
* External mediation or arbitration if required
* Documentation and communication of appeals decisions

**Corrective Actions**

* Additional training and competency development
* Process improvements and policy updates
* System enhancements and security controls
* Ongoing monitoring and performance management

**15. POLICY GOVERNANCE AND UPDATES**

**15.1 Review and Update Schedule**

**Regular Reviews**

* Quarterly risk assessment and control effectiveness review
* Semi-annual policy and procedure updates
* Annual comprehensive policy review and approval
* Ad-hoc reviews for significant incidents or regulatory changes

**Update Triggers**

* New AI technologies or service implementations
* Regulatory changes or enforcement actions
* Significant security incidents or vulnerabilities
* Client requirements or contractual changes
* Industry best practice developments

**15.2 Change Management**

**Policy Change Process**

* Impact assessment and stakeholder consultation
* Draft policy development and technical review
* Legal and compliance validation
* Senior management approval and communication
* Implementation planning and training delivery

**Version Control**

* Comprehensive document version management
* Change tracking and audit trail maintenance
* Communication of policy changes to all stakeholders
* Archive management and historical record keeping

**15.3 Training and Communication**

**Policy Communication**

* All-hands meetings for significant policy changes
* Department-specific training and implementation guidance
* Regular policy awareness and refresh training
* Integration with new employee onboarding programs

**Competency Assessment**

* Regular testing of AI policy knowledge and understanding
* Role-specific competency requirements and assessments
* Continuous professional development and training programs
* External certification and accreditation support

**16. IMPLEMENTATION CHECKLIST**

**Phase 1: Foundation (Months 1-2)**

**Governance Structure**

* [ ] Establish AI Governance Board and working groups
* [ ] Define roles and responsibilities for AI governance
* [ ] Appoint Data Protection Officer and AI compliance lead
* [ ] Create AI governance policies and procedures documentation

**Risk Assessment**

* [ ] Conduct comprehensive AI risk assessment
* [ ] Identify current AI usage across the organisation
* [ ] Classify AI systems by risk level and business impact
* [ ] Document risk mitigation strategies and controls

**Basic Training**

* [ ] Develop AI awareness training program
* [ ] Deliver mandatory training to all employees
* [ ] Create role-specific training materials
* [ ] Establish ongoing training and competency requirements

**Phase 2: Implementation (Months 3-6)**

**Technical Controls**

* [ ] Deploy approved AI tools and platforms
* [ ] Implement security controls and monitoring systems
* [ ] Configure access controls and user authentication
* [ ] Establish logging and audit capabilities

**Operational Procedures**

* [ ] Implement AI system approval and change management processes
* [ ] Establish incident response and escalation procedures
* [ ] Create monitoring and performance measurement systems
* [ ] Develop vendor management and oversight procedures

**Client Services**

* [ ] Update client contracts and service agreements
* [ ] Implement client consent and notification procedures
* [ ] Develop AI service delivery documentation
* [ ] Train client-facing staff on AI capabilities and limitations

**Phase 3: Optimisation (Months 6-12)**

**Advanced Capabilities**

* [ ] Implement advanced AI tools and custom solutions
* [ ] Develop automated compliance and monitoring systems
* [ ] Establish predictive analytics and intelligence capabilities
* [ ] Create AI innovation and development programs

**Continuous Improvement**

* [ ] Conduct regular policy and procedure reviews
* [ ] Implement feedback and lessons learned improvements
* [ ] Expand training and competency development programs
* [ ] Develop AI centre of excellence and expertise

**External Engagement**

* [ ] Engage with industry groups and standards bodies
* [ ] Participate in regulatory consultations and guidance development
* [ ] Share best practices and lessons learned with peers
* [ ] Pursue AI governance certifications and accreditations

**APPENDIX A: RISK ASSESSMENT TEMPLATES**

**A.1 AI System Risk Assessment Template**

**System Information**

* System Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Business Owner: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Technical Owner: \_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Implementation Date: \_\_\_\_\_\_\_\_\_\_\_
* Review Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Risk Categories Assessment**

| **Risk Category** | **Risk Level (1-5)** | **Mitigation Controls** | **Residual Risk** | **Owner** |
| --- | --- | --- | --- | --- |
| Data Privacy |  |  |  |  |
| Security |  |  |  |  |
| Bias/Fairness |  |  |  |  |
| Transparency |  |  |  |  |
| Business Impact |  |  |  |  |
| Regulatory |  |  |  |  |

**Overall Risk Assessment**

* Combined Risk Score: \_\_\_/25
* Risk Classification: Critical / High / Medium / Low
* Approval Required: Yes / No
* Approving Authority: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Implementation Conditions: \_\_\_\_\_\_\_\_\_\_\_

**A.2 Data Protection Impact Assessment Template**

**DPIA Reference:** DPIA-AI-[YEAR]-[NUMBER] **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Reviewer:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Section 1: System Description**

* AI System Purpose: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Data Types Processed: \_\_\_\_\_\_\_\_\_\_\_\_\_
* Data Sources: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Processing Activities: \_\_\_\_\_\_\_\_\_\_\_\_\_
* Automated Decision-Making: Yes / No

**Section 2: Necessity and Proportionality**

* Legal Basis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Legitimate Interests Assessment: \_\_\_\_
* Data Minimisation Measures: \_\_\_\_\_\_\_\_
* Purpose Limitation Controls: \_\_\_\_\_\_\_

**Section 3: Risk Assessment**

* Rights and Freedoms Impact: \_\_\_\_\_\_\_
* Vulnerable Groups Affected: \_\_\_\_\_\_\_\_
* Potential Harms Identified: \_\_\_\_\_\_\_\_
* Likelihood Assessment: \_\_\_\_\_\_\_\_\_\_\_\_

**Section 4: Mitigation Measures**

* Technical Safeguards: \_\_\_\_\_\_\_\_\_\_\_\_\_
* Organisational Measures: \_\_\_\_\_\_\_\_\_\_
* Privacy by Design Features: \_\_\_\_\_\_\_
* Ongoing Monitoring Plans: \_\_\_\_\_\_\_\_\_

**APPENDIX B: APPROVED AI TOOLS DETAILED SPECIFICATIONS**

**B.1 Microsoft 365 Copilot Enterprise Configuration**

**Required Configuration Settings**

* Tenant Data Residency: EU/UK regions only
* Data Loss Prevention: Enabled with custom policies
* Audit Logging: Comprehensive logging enabled
* Admin Controls: Centralized administration required

**Security Requirements**

* Multi-factor Authentication: Mandatory for all users
* Conditional Access: Risk-based access policies
* Information Protection: Sensitivity labeling required
* Compliance Center: Regular compliance reporting

**Usage Guidelines**

* Approved Data Types: Business documents, emails, presentations
* Prohibited Data Types: Client personal data, payment information
* Output Review: Human review required for client-facing content
* Training Requirements: Mandatory certification before access

**B.2 Azure AI Foundry Security Architecture**

**Infrastructure Requirements**

* Virtual Network: Dedicated VNet with NSG rules
* Private Endpoints: All services behind private endpoints
* Key Vault: Azure Key Vault for secret management
* Monitoring: Azure Monitor and Security Center integration

**Data Protection**

* Encryption at Rest: Customer-managed keys (CMK)
* Encryption in Transit: TLS 1.3 minimum
* Access Controls: Azure RBAC with custom roles
* Data Residency: UK South/West regions only

**Compliance Features**

* Audit Logging: Comprehensive activity logging
* Compliance Manager: Regular compliance assessments
* Data Governance: Purview integration for data cataloging
* Backup/Recovery: Automated backup with cross-region replication

**APPENDIX C: INCIDENT RESPONSE PLAYBOOKS**

**C.1 AI Data Breach Response Playbook**

**Phase 1: Detection and Assessment (0-1 hour)**

1. **Immediate Actions**
   * Isolate affected AI systems
   * Preserve evidence and logs
   * Notify incident response team
   * Begin impact assessment
2. **Initial Assessment**
   * Determine scope of potential breach
   * Identify data types potentially affected
   * Assess number of individuals impacted
   * Evaluate need for immediate notifications

**Phase 2: Containment and Investigation (1-24 hours)**

1. **Containment**
   * Implement additional security controls
   * Restrict access to affected systems
   * Monitor for ongoing unauthorised activity
   * Document all containment actions
2. **Investigation**
   * Forensic analysis of affected systems
   * Review of AI system logs and activities
   * Interviews with relevant personnel
   * Assessment of attack vectors and methods

**Phase 3: Notification and Communication (24-72 hours)**

1. **Regulatory Notifications**
   * ICO notification within 72 hours if required
   * Client notifications per contractual obligations
   * Other regulatory bodies as applicable
   * Legal counsel consultation
2. **Stakeholder Communication**
   * Internal incident updates
   * Client and partner notifications
   * Media and public relations coordination
   * Employee communication and guidance

**Phase 4: Recovery and Lessons Learned (72+ hours)**

1. **System Recovery**
   * Secure restoration of AI services
   * Verification of system integrity
   * Enhanced monitoring implementation
   * Validation of security controls
2. **Post-Incident Analysis**
   * Comprehensive incident report
   * Root cause analysis
   * Process improvement recommendations
   * Policy and procedure updates

**C.2 AI Bias Incident Response Playbook**

**Phase 1: Bias Detection and Verification (0-4 hours)**

1. **Initial Response**
   * Document bias complaint or detection
   * Preserve AI system state and data
   * Notify AI governance team
   * Initiate bias assessment procedures
2. **Bias Verification**
   * Technical analysis of AI model outputs
   * Statistical testing for discriminatory patterns
   * Review of training data for bias sources
   * Assessment of protected characteristic impacts

**Phase 2: Impact Assessment and Mitigation (4-24 hours)**

1. **Impact Analysis**
   * Identify affected individuals or groups
   * Assess extent of discriminatory decisions
   * Evaluate legal and regulatory implications
   * Document potential harms and consequences
2. **Immediate Mitigation**
   * Suspend biased AI system if necessary
   * Implement human override procedures
   * Review and correct affected decisions
   * Notify affected individuals as appropriate

**Phase 3: Remediation and Prevention (24+ hours)**

1. **Technical Remediation**
   * Retrain AI models with bias mitigation
   * Implement fairness constraints and testing
   * Update data preprocessing procedures
   * Enhance ongoing bias monitoring
2. **Process Improvements**
   * Review bias testing procedures
   * Update training and awareness programs
   * Strengthen vendor oversight requirements
   * Implement enhanced governance controls

**APPENDIX D: TRAINING MATERIALS FRAMEWORK**

**D.1 AI Fundamentals Training (All Employees)**

**Module 1: Introduction to AI**

* Definition and types of AI technologies
* Common AI applications in business
* Benefits and risks of AI adoption
* MSP-specific AI use cases and examples

**Module 2: Data Protection and Privacy**

* UK GDPR requirements for AI systems
* Personal data identification and classification
* Consent and lawful basis for AI processing
* Individual rights in AI contexts

**Module 3: Ethics and Bias**

* Ethical principles for AI development and use
* Understanding bias in AI systems
* Fairness and non-discrimination requirements
* Reporting concerns and escalation procedures

**Module 4: Security and Risk Management**

* AI-specific security threats and vulnerabilities
* Secure AI usage best practices
* Incident reporting and response procedures
* Risk assessment and mitigation strategies

**Assessment Requirements**

* Written examination (80% pass rate required)
* Practical scenario assessments
* Annual refresher training mandatory
* Competency tracking and reporting

**D.2 Technical AI Training (Technical Staff)**

**Advanced Module 1: AI Security Architecture**

* Secure AI development lifecycle
* Threat modeling for AI systems
* Security controls and monitoring
* Vulnerability assessment and testing

**Advanced Module 2: AI Model Development**

* Responsible AI development practices
* Data quality and bias testing
* Model validation and verification
* Performance monitoring and maintenance

**Advanced Module 3: AI Integration and Deployment**

* Secure integration patterns
* API security and authentication
* Monitoring and logging implementation
* Incident response and troubleshooting

**Advanced Module 4: AI Governance Implementation**

* Risk assessment methodologies
* Compliance monitoring and reporting
* Policy implementation and enforcement
* Stakeholder communication and training

**APPENDIX E: CLIENT COMMUNICATION TEMPLATES**

**E.1 AI Service Implementation Notification**

**Subject:** Implementation of AI-Enhanced Services - [Client Name]

Dear [Client Contact],

We are writing to inform you of our planned implementation of artificial intelligence technologies to enhance our managed services delivery for your organisation. This initiative is part of our continued commitment to providing innovative, efficient, and secure IT services.

**AI Services Overview:**

* Enhanced monitoring and predictive analytics
* Automated incident detection and response
* Intelligent performance optimisation
* Improved security threat detection

**Data Protection Measures:**

* All AI processing complies with UK GDPR requirements
* Client data remains within approved geographical boundaries
* Enhanced security controls and monitoring implemented
* No client data used for AI model training without explicit consent

**Your Rights and Controls:**

* Right to object to AI processing of your data
* Right to request human review of AI-driven decisions
* Access to AI system transparency and explainability
* Regular reporting on AI service performance and outcomes

**Next Steps:** We will schedule a briefing session to discuss the implementation details and address any questions or concerns. Please contact [Contact Information] to arrange this meeting.

**Contact Information:** For questions about this AI implementation:

* Technical queries: [Technical Contact]
* Data protection matters: [DPO Contact]
* Service delivery: [Account Manager]

We look forward to delivering enhanced services through these innovative AI capabilities while maintaining our commitment to security, privacy, and service excellence.

Best regards, [Name and Title]

**E.2 AI Incident Notification Template**

**Subject:** URGENT - AI System Incident Notification - [Client Name]

Dear [Client Contact],

We are writing to inform you of an incident involving AI systems that process your organisation's data. We take this matter very seriously and are committed to full transparency and rapid resolution.

**Incident Summary:**

* Date and Time: [Incident Details]
* Systems Affected: [System Information]
* Nature of Incident: [Brief Description]
* Current Status: [Status Update]

**Data Impact Assessment:**

* Data types potentially affected: [Data Categories]
* Number of records involved: [Quantity]
* Geographical scope: [Location Information]
* Risk to individuals: [Risk Assessment]

**Immediate Actions Taken:**

* [List of containment measures]
* [Investigation procedures initiated]
* [Security enhancements implemented]
* [Monitoring and verification activities]

**Ongoing Response:**

* Comprehensive forensic investigation in progress
* Enhanced security monitoring implemented
* Regular updates will be provided
* Independent security assessment scheduled

**Your Requirements:**

* Please review your incident response procedures
* Consider additional monitoring of affected systems
* Report any unusual activity immediately
* Coordinate with your data protection officer

**Next Communication:** We will provide a comprehensive update within [Timeframe] including:

* Detailed investigation findings
* Root cause analysis
* Remediation measures implemented
* Prevention strategies for future incidents

**Contact Information:**

* Incident Manager: [Name and Contact]
* Technical Lead: [Name and Contact]
* Account Manager: [Name and Contact]
* 24/7 Emergency Line: [Emergency Contact]

We sincerely apologise for this incident and any inconvenience caused. Our teams are working around the clock to resolve this matter and prevent future occurrences.

Best regards, [Incident Response Team]

**APPENDIX F: REGULATORY COMPLIANCE CHECKLIST**

**F.1 UK GDPR Compliance Checklist for AI Systems**

**Lawfulness of Processing**

* [ ] Lawful basis identified and documented for each AI processing activity
* [ ] Legitimate interests assessment completed where applicable
* [ ] Consent mechanisms implemented for consent-based processing
* [ ] Regular review of lawful basis validity and ongoing necessity

**Data Subject Rights**

* [ ] Procedures for handling access requests to AI-generated decisions
* [ ] Right to rectification processes for AI training data
* [ ] Right to erasure implementation for AI systems
* [ ] Right to object procedures for automated decision-making
* [ ] Data portability processes for AI-processed personal data

**Data Protection by Design and Default**

* [ ] Privacy impact assessments completed for all AI systems
* [ ] Data minimisation principles implemented in AI data processing
* [ ] Purpose limitation controls enforced in AI applications
* [ ] Technical and organisational measures documented and implemented

**Automated Decision-Making**

* [ ] Identification of solely automated decision-making processes
* [ ] Human intervention capabilities implemented where required
* [ ] Meaningful information about AI logic provided to data subjects
* [ ] Regular assessment of AI decision accuracy and fairness

**Data Protection Officer**

* [ ] DPO consultation on AI system design and implementation
* [ ] DPO involvement in AI-related data protection impact assessments
* [ ] Regular DPO reporting on AI compliance status
* [ ] DPO training on AI-specific data protection issues

**F.2 Security and Risk Management Compliance**

**Information Security Management**

* [ ] AI systems included in information security management system (ISMS)
* [ ] Risk assessments completed for all AI implementations
* [ ] Security controls implemented based on risk assessment outcomes
* [ ] Regular security testing and vulnerability assessments conducted

**Business Continuity and Disaster Recovery**

* [ ] AI systems included in business continuity planning
* [ ] Disaster recovery procedures tested for AI infrastructure
* [ ] Alternative service delivery procedures documented
* [ ] Recovery time and point objectives defined for AI services

**Vendor and Supply Chain Management**

* [ ] Due diligence completed for all AI vendors and suppliers
* [ ] Contractual security requirements defined and enforced
* [ ] Regular vendor security assessments and audits conducted
* [ ] Incident response procedures coordinated with vendors

**Monitoring and Incident Response**

* [ ] Continuous monitoring implemented for AI system security
* [ ] Incident detection and response procedures tested regularly
* [ ] Incident reporting mechanisms established and communicated
* [ ] Lessons learned processes implemented for security incidents

**DOCUMENT CONTROL**

**Version History**

| **Version** | **Date** | **Author** | **Changes** |
| --- | --- | --- | --- |
| 1.0 | [Date] | [Author] | Initial policy creation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Distribution**

| **Role** | **Name** | **Date Received** | **Acknowledgment** |
| --- | --- | --- | --- |
| CEO |  |  |  |
| CTO |  |  |  |
| CISO |  |  |  |
| DPO |  |  |  |
| Department Managers |  |  |  |

**Review and Approval**

| **Role** | **Name** | **Signature** | **Date** |
| --- | --- | --- | --- |
| Document Owner |  |  |  |
| Legal Review |  |  |  |
| DPO Review |  |  |  |
| CISO Approval |  |  |  |
| CEO Approval |  |  |  |

**Next Review Date:** [Insert Date + 12 Months]

**Document Classification:** Company Confidential **Retention Period:** 7 Years **Distribution:** All Staff, Board Members, Key Vendors

*This AI Governance Policy Template is based on current best practices, regulatory requirements, and industry standards as of 2025. It should be customised to reflect your specific business requirements, regulatory environment, and operational context. Regular review and updates are essential to maintain effectiveness and compliance.*

**For support with implementing this policy or creating industry-specific versions, contact:**

* **Email:** [governance@company.com]
* **Phone:** [Contact Number]
* **Internal Resource:** AI Governance Board

**External Resources:**

* ICO AI Guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/
* NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework
* BSI AI Standards: https://www.bsigroup.com/en-GB/standards/artificial-intelligence/

**END OF DOCUMENT**