

CQC AI Statements & *how they relate to* DSPT Standards Met

CQC AI Principles for Social Care

1. AI to support, not to replace: AI can enhance, but not replace human decision making

2. Human oversight: AI outputs and processes are continuously monitored and evaluated

3. Transparency and choice: People who use services have appropriate information to make informed decisions about their care, including the role of AI in care pathways. Non-digital routes to care are offered if needed, also considering digital skills and connectivity

4. Safety and reliability: Providers ensure that introducing and using AI provides safe care and equitable outcomes for people

5. Security: The technology is resilient to cyberattacks and sensitive information is stored and processed securely to comply with the General Data Protection Regulation

6. Fairness and impartiality: Good AI accelerates equity of care in terms of access and outcomes. For example, it provides accurate results across geographies and population groups, and any potential known biases are mitigated

7. AI readiness and training: Those using AI are sufficiently trained and confident in using the technology, and they assess whether it can be integrated into existing pathways

8. Effective governance: There are effective mechanisms such as risk assessments to ensure AI contributes to high-quality, equitable care, and established systems to recognise, report and investigate when something goes wrong so that lessons are learned and solutions implemented

9. Data Protection Impact Assessment (DPIA): A DPIA assesses and documents risks to privacy and data subject rights to understand and minimise any interference with people's rights, to enable lawful use of AI

10. Accountability: There are clear mechanisms for addressing issues or harm caused by AI

11. Procurement: AI tools are procured in line with relevant regulatory standards

1. AI to support not replace Human Decision-Making

1. Policy stating *AI is decision support only*

2. Human sign-off for care decisions

3. Guidance on when *not* to rely on *AI*

DSPT Standard **5 (Risk Management)** – Risks Identified and mitigated: *Prevents unsafe reliance on AI*

DSPT standard **10 (Fit for purpose systems)** – System supports safe care: *Ensures AI supports not replaces care decisions*

2. Human Oversight

1. Monitoring logs and review processes

2. Escalation procedures for incorrect *AI* outputs

DSPT Standard 5 (Risk Management) Monitoring of risks and system outputs

DSPT Standard 8 (Incident Management) – Ability to detect and respond to *AI* failures

3. Transparency & Choice

1. Privacy notices referencing *AI* use (or AI Acceptable Use Policy)

2. Service user information (leaflets, consent discussions)

3. Alternative non-digital pathways

DSPT Standard 1 & 2 Staff communicate appropriately about data use

DSPT Standard 4 Lawful and fair processing (transparency principle)

4. Safety and Reliability

1. *AI* risk assessments and Data Processing Impact Assessments (DPIAs)

2. Testing and validation records

3. Outcome & performance monitoring

DSPT Standard **5 Risk assessment and mitigation**

DSPT Standard **10 (Fit for purpose systems) Systems safe and reliable**

5. Security

1. Access controls for *AI* systems

2. Supplier security assurance

3. Cyber security policies covering *AI* tools

DSPT Standard **6 (Access Control)** Controlled access to systems

DSPT Standard **7 (Cyber Security)** Protection against breaches

6. Fairness & Impartiality

1. Bias assessments/equality considerations

2. Evidence of fairness checks

3. EqlA (if applicable)

DSPT Standard **5 Risk Management (Bias Risks)**

DSPT Standard **10 Systems deliver equitable outcomes**

7. AI Readiness & Training

1. Training records (*AI* awareness, safe use)

2. Staff Guidance on generative *AI* risks

DSPT Standard **1 Staff trained and aware**

DSPT Standard **2 Staff understand secure data handling**

8. Effective Governance

1. *AI* governance framework

2. Risk register entries

3. Incident logs and review processes

DSPT Standard **5 Risk governance structures (DPIA)**

DSPT Standard **8 Incident reporting processes (Incident logs)**

DSPT Standard **3 Documentation and records (AI register)**

9. Data Protection Impact Assessment (DPIA)

1. Completed DPIAs for AI systems

2. Documentation of risks to rights and freedoms

DSPT Standard **4 Lawful processing and DPIAs**

DSPT Standard **5 Risk Assessment**

10. Accountability

1. Named AI lead / SRO

2. Clear escalation and accountability processes

DSPT Standard **1 Roles and responsibilities**

DSPT Standard **8 Accountability for incidents**

DSPT Standard **3 Documented processes**

11. Procurement

1. Supplier due diligence

2. Assurance of compliance with UK GDPR

3. Contracts with data protection clauses

DSPT Standard **6 & 7 Security and supplier assurance**

DSPT Standard **10 Systems fit for purpose**

Summary

These CQC AI expectations fit almost entirely within DSPT standards: 4, 5, 6, 7 and 10

The strongest alignment is:

- NDG 5 Risk Management
- NDG 10 Safe, effective systems

While answering Standards Met questions, you can incorporate wording like:

- “AI systems are used only as decision-support tools with full human oversight”
- “AI risks are assessed through DPIAs and managed within the organisational risk framework”
- “Staff are trained in safe and appropriate use of AI technologies”