



DSPT Readiness Checklist

What CQC and DSPT assessors actually check

Use this to see where your practice stands before your next DSPT submission or CQC inspection. Tick each item that already applies.

1. Data security basics

- ☐ All staff devices have up-to-date antivirus / endpoint protection
- ☐ Multi-factor authentication (MFA) enabled on email and care systems
- ☐ Firewall and network security reviewed in the last 12 months
- ☐ Data backups run automatically and have been test-restored

2. Access and accountability

- ☐ Staff access to patient / resident records is role-based, not open to all
- ☐ Leavers are removed from all systems on their last working day
- ☐ You can produce an access log if an inspector asks who viewed a record
- ☐ Staff have completed data protection / cyber awareness training in the last 12 months

3. Documentation and evidence

- ☐ Current DSPT submission is up to date (check expiry date)
- ☐ GDPR / data protection policy exists, is dated, and staff have read it
- ☐ You have a documented incident response plan for a data breach
- ☐ Cyber Essentials certification is current (or you have a plan to get it)

Scoring guide

10-12 checked	Strong position. Focus on maintaining evidence.
6-9 checked	Gaps exist. Worth a readiness review before your next submission.
Under 6 checked	Submission or inspection risk. Book a review now.

Scored under 10?

Book a DSPT readiness check. We'll walk through the gaps and tell you exactly what to fix first, before an assessor or inspector does.

info@guardiq.co.uk | 020 8537 8167 | guardiq.co.uk

**IT & SECURITY
MANAGED FOR YOU**