CYBER SECURITY CHECKLIST FOR CARE HOMES

BLACK SWAN
CYBER SECURITY SOLUTIONS

Protect your residents' data. Stay compliant with DSPT. Build trust in your care.

You handle some of the most sensitive personal data there is – medical records, care plans, ID documents, payroll and visitor information. A single breach could mean a CQC notification, DSPT compliance failure, and serious reputational harm.

This checklist helps you benchmark your current cyber security measures and demonstrate "appropriate technical and organisational controls" under the UK GDPR, DSPT, and Data Protection Act 2018.

1 Access & Authentication

- [ ] Enable multi-factor authentication (MFA) for all key systems (email, NHS Mail, care planning, HR, payroll)
- [ ] Apply role-based access control (RBAC) for staff, carers and managers
- [ ] Keep admin accounts separate from daily-use logins
- [ ] Store passwords securely in a password manager
- [ ] Revoke access promptly when staff leave or change roles
- [ ] Review user accounts and permissions at least quarterly
- [ ] Each staff member has their own unique login - no shared or generic accounts
- [ ] Your email password is unique and not reused elsewhere
- [ ] All passwords are strong (at least 12 characters) or use three random words
- [ ] Apply account lockout after several failed login attempts
- [ ] Follow a secure password reset process - no resets by email or text without ID checks
- [ ] Review and update passwords immediately if compromise is suspected

2 Email & Communication Security

- [ ] Use NHS Mail or another secure, encrypted platform for resident data
- [ ] Configure DMARC, SPF, and DKIM to protect against spoofing
- [ ] Enable an external email banner to highlight outside messages
- [ ] Never send resident or staff personal data in plain email
- [ ] Provide phishing awareness training for all staff

3 Data Protection & Backup

- [ ] Back up your data daily with immutable copies
- [ ] Test backups quarterly for speed and reliability
- [ ] Use UK-based or NHS DSPT-compliant storage
- [ ] Encrypt data at rest and in transit
- [ ] Restrict access to care records by role
- [ ] Store backup copies securely and separately
- [ ] Include cyber incidents in your Business Continuity Plan

4 Device & Endpoint Protection

- [ ] Deploy Next-Gen Antivirus / Managed EDR
- [ ] Enable disk encryption (BitLocker / FileVault)
- [ ] Use individual logins on shared devices – no generic usernames
- [ ] Automate patch management and keep logs
- [ ] Maintain an inventory of assets
- [ ] Restrict or encrypt portable media (USB drives)
- [ ] Ensure all systems run supported operating systems

5 Network & Building Systems

- [ ] Use secure Wi-Fi (WPA3) and separate staff and guest networks
- [ ] Configure and review your firewall quarterly
- [ ] Enable DNS filtering and web threat protection
- [ ] Keep CCTV, nurse call, and IoT systems separate from admin networks
- [ ] Restrict cloud sharing to named users – no public links

6 Staff Awareness & Training

- [ ] Provide regular cyber and data protection training
- [ ] Run phishing simulations to build awareness
- [ ] Cover GDPR, DSPT and confidentiality during induction
- [ ] Encourage a no-blame culture for incident reporting
- [ ] Display visual reminders in staff areas
- [ ] Keep training records and conduct spot checks
- [ ] Supervisors model good data handling behaviours

7 Governance, Compliance & Accountability

- [ ] Review your Information Security and Data Protection Policies annually
- [ ] Complete and publish your DSPT submission each year
- [ ] Maintain GDPR accountability records
- [ ] Keep ICO registration up to date
- [ ] Hold or work towards Cyber Essentials certification
- [ ] Appoint a Caldicott Guardian or Data Protection Lead
- [ ] Include confidentiality clauses in all staff contracts
- [ ] Add data protection duties to job descriptions and onboarding
- [ ] Review information governance annually with management

8 Incident Response & Business Continuity

- [ ] Use Managed Detection & Response (MDR) or 24/7 alerting
- [ ] Test your incident response plan every year
- [ ] Have clear steps for password resets, MFA re-enrolment, and notifying residents or families
- [ ] Retain Microsoft 365 audit and sign-in logs for 12 months
- [ ] Record, investigate and report data breaches within 72 hours
- [ ] Share lessons learned from incidents to prevent recurrence
- [ ] Review your cyber insurance to ensure it matches your security controls

BLACK SWAN
CYBER SECURITY SOLUTIONS

Next Steps

Book your Care Sector Security Review with Black Swan Cyber Security Solutions.

We'll assess your DSPT compliance, security and data protection controls -without the jargon.

blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142