# CYBER SECURITY CHECKLIST FOR DOMICILIARY CARE PROVIDERS

BLACK SWAN
CYBER SECURITY SOLUTIONS

Protect your service users' data. Stay compliant with DSPT. Maintain trust in your care.

You handle confidential care plans, medical details and staff records every day - often while working remotely across phones, tablets and laptops. Strong cyber security is essential to protect the people you care for and to maintain compliance with the DSPT, GDPR, and CQC standards.

This checklist helps you assess your current security measures and demonstrate "appropriate technical and organisational controls" under the UK GDPR and DSPT.

## 1 Access & Authentication

- [ ] Enable multi-factor authentication (MFA) for email and all care management and communication systems
- [ ] Apply role-based access control for coordinators, 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 Mobile & Remote Working Security

- [ ] Encrypt all mobile devices and ensure they can be remotely wiped
- [ ] Use Mobile Device Management (MDM) for work phones and tablets
- [ ] Require PINs or biometrics to unlock devices
- [ ] Set clear policies for connecting to Wi-Fi in clients' homes
- [ ] Ensure lost or stolen devices can be reported and locked immediately

## 3 Email & Communication Security

- [ ] Use NHS Mail or another secure, encrypted platform for client and staff data
- [ ] Configure DMARC, SPF, and DKIM for your email domains
- [ ] Enable external email banners to warn about outside messages
- [ ] Never send care or staff information in plain email or consumer messaging apps
- [ ] Train all staff to identify phishing and social engineering attempts

## 4 Data Protection & Backup

- [ ] Back up your data daily with immutable copies
- [ ] Test backups quarterly to ensure recovery and integrity
- [ ] Use UK-based or DSPT-compliant cloud storage
- [ ] Encrypt data both at rest and in transit
- [ ] Limit care plan access to authorised, active staff only
- [ ] Store backup copies securely and separately from main systems
- [ ] Include cyber incidents in your Business Continuity Plan

## 5 Device & Endpoint Protection

- [ ] Deploy Next-Gen Antivirus or Managed EDR on all laptops and tablets
- [ ] Automate patch management for devices and apps
- [ ] Maintain a current device inventory, reviewed quarterly
- [ ] Check devices for compliance before issuing them to carers
- [ ] Restrict or encrypt portable media such as USB drives
- [ ] Ensure all systems run supported operating systems

## 6 Staff Awareness & Culture

- [ ] Provide regular cyber awareness 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
- [ ] Keep training records and spot check understanding
- [ ] Supervisors should model good data handling behaviours

## 7 Governance, Compliance & Accountability

- [ ] Review your Information Security and Data Protection Policies annually
- [ ] Complete and publish your DSPT submission every year
- [ ] Maintain GDPR accountability evidence such as Records of Processing Activities
- [ ] Keep ICO registration up to date
- [ ] Hold or work towards Cyber Essentials certification
- [ ] Appoint a Caldicott Guardian or Data Protection Lead
- [ ] Ensure confidentiality clauses are included in all staff contracts
- [ ] Include data protection duties in job descriptions and onboarding
- [ ] Review information governance with senior management annually

## 8 Incident Response & Business Continuity

- [ ] Have Managed Detection & Response (MDR) or 24/7 alerting in place
- [ ] Test your incident response plan at least once a year
- [ ] Define clear steps for password resets and MFA re-enrolment
- [ ] Retain audit logs for at least 12 months
- [ ] Record, investigate, and report data breaches within 72 hours
- [ ] Share lessons learned from any incidents with your team
- [ ] Review your cyber insurance policy to ensure it aligns with your controls

BLACK SWAN
CYBER SECURITY SOLUTIONS

# Next Steps

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

We'll review your DSPT compliance, mobile device safety and backup strategy - without the jargon.


blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142