

Data protection and cyber security

Checklist for new providers

Version 1 – September 2024

**New care services can use this checklist to plan their approach to digital technology, data protection and cyber security. It’s a quick summary of the key issues to consider, with links to related guidance and templates.**

Access free support from Digital Care Hub and the Better Security, Better Care programme - including free tailored support from 28 local support partners across the country and free template policies and resources for you to download and adapt for your organisation. [www.digitalcarehub.co.uk](http://www.digitalcarehub.co.uk).new-care-services

# The basics

* [Register with the Information Commissioners Office (ICO](https://ico.org.uk/for-organisations/data-protection-fee/register/)): You process personal data, so you must be registered with the ICO. [www.ico.org.uk](http://www.ico.org.uk)
* Complete the free, official Data Security and Protection Toolkit (DSPT). This will guide you through the data protection and cyber security arrangements you need to have in place. [www.digitalcarehub.co.uk/dspt](http://www.digitalcarehub.co.uk/dspt)

# Plan your use of data

* Document what data you need to store and/or share about: people using your services (including potential clients); families and visitors; staff (including applicants); trustees; funders etc.
* Consider what data is personal (i.e. identifies an individual – this includes an email address with a name in it), and what is sensitive (e.g. gender, health, union membership, religion etc.).
* Map out what data will be shared and with whom (e.g. roles within the organisation and external contacts such as GPs, pharmacists, hospital staff).
* Document how you will store, process and dispose of that data.

# Tell people how you manage their data

* Tell people using your services, their family and carers how you use their data. Ensure it is easy to understand. Consider easy read, large print, audio and translations of information to help people to understand how their information is used.
* Tell people who are considering using your services how you keep data safe. Make your Privacy Policy easy to find and understand on your website.
* Complete the Data Security and Protection Toolkit and add the certificate to your website and/or offices. It demonstrates you are taking steps to keep information safe.

# Plan your tech and paper systems

* Plan, prioritise and budget for what technology and software you may need such as:
	+ care records and planning
	+ medication management
	+ staff management including recruitment, references, appraisals, rostering, payroll
	+ quality and audit
	+ eLearning and training
	+ secure email (e.g. NHSmail)
	+ telecare (e.g. remote monitoring, personal alarms, circadian lighting etc)
	+ mobile devices for staff (and residents) (e.g. tablets, work mobile phones etc.).
* Plan how you will manage information stored and shared in basic software systems including:
	+ email
	+ Excel
	+ Word
	+ shared drives.
* Consider what data will be stored and shared on all tech systems: how will this data be protected by the software company, your staff and anyone else who may have access? What cyber security protection such as firewalls, privacy settings, anti-malware are installed?

# Consider Wi-Fi and mobile data

* Check Wi-Fi access throughout your building(s), including addition of boosters.
* Consider separate Wi-Fi for staff and residents/visitors and develop a clear policy on Wi-Fi access.
* Agree policy for logging in to clients’ or other Wi-Fi sources (e.g. during homecare visits).
* Consider mobile data contracts and payments including for staff who use their own devices for work purposes (e.g. homecare staff).

# Manage your IT suppliers

* Create a list of your suppliers who process personal information
* Check suppliers’ data protection and cyber security arrangements – including responsibilities in the event of a data breach or cyber attack.
* Check if they have cyber security certification, and the Data Security and Protection Toolkit in place.
* Rank them in terms of how crucial they are to your business. Include a back-up plan in your business continuity plan.

# Manage paper records

* Plan what paper records you will keep, how they will be stored and accessed – including any paper backups of digitally stored information.
* Plan how paper records will be kept physically secure (e.g. lockable, windows and cupboards, clear desk procedure, security badges for access, key coded locks to access secure areas etc.).
* Agree how paper records can be transported securely by staff.
* Agree how paper records are stored in a clients’ home (e.g. homecare).
* Agree how information will be sent with a client to an appointment (e.g. a medical appt / hospital).

# Implement secure email

* Email systems used for sending sensitive and confidential emails meet‘secure email standard’ (called DCB1596). For example, NHSmail is a secure email system.
* Agree when secure email should be used, and when it is optional.
* Train staff on use of secure email.

# Allocate responsibilities

* Identify a Data Security and Protection Lead who was overall senior responsibility for data security and protection issues.
* Consider what other roles you may require:
	+ Data Protection Officer
	+ Caldicott Guardian
	+ Senior Information Risk Officer
* Provide training for these roles if required.

# Train and support staff

* Include data protection and cyber security training in induction.
* Ensure all staff are aware of policies and procedures, including any updates.
* Conduct annual refresher training for all staff.
* Include data protection responsibilities in all staff, volunteer, trustee contracts or agreements.
* Keep staff records safe and up to date – including contact details, rostering and payroll systems.

# Create process for managing data breaches and cyber attacks

* Have a clear, robust system for reporting data breaches.
* Create a business continuity plan including data and cyber security (e.g.  what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire).
* Test the business continuity plan based on different scenarios.
* Train staff on the processes for reporting data breaches, and implementing the business continuity plan.
* Consider purchasing cyber insurance. Check what is included.

# Be careful with mobile devices

* Create clear policies about the use of mobile devices – including use of personal devices for work purposes.
* Plan your approach to managing the loss, theft or hacking of mobile devices (e.g. track location, have PINs in place to prevent unauthorised access).
* Encrypt mobile devices including laptops, mobile phones, USB sticks, memory cards etc.

# Passwords and access

* Provide strong passwords or train staff on setting up strong passwords.
* Consider using multi-factor authentication (MFA).
* Set up screensavers on computers and mobile devices so that information is hidden after short periods of inactivity.
* Remove staff’s access and update passwords when they leave or change roles which affects the information they should access. Carry out a regular review.

# Ensure back-ups are in place

* Create a reliable process for backups, including frequency, location and responsibility (e.g. computer unconnected to shared systems, cloud, mobile device, USB stick, summary print records etc.).
* Test the back up process and reliability of data frequently.

# Consider internal communications

* Agree how staff can communicate information about work (e.g. use of WhatsApp, text messages, email etc.).

# Protect software

* Ensure all software is up to date and still supported by the manufacturer. If not, assess the level of risk this poses and record decisions.
* Add anti-virus software to all computers and digital devices. Create a process for regular checking and updating.

#   Agree approach to social media

* Create a social media policy covering the use of corporate social media accounts, and staff’s use of their personal accounts when referencing work. Include approach to sharing photos of staff, clients, family etc including how to gain and record consent.

# Develop your policies, procedures and contracts

* Ensure you have key policies in place. (See list below).
* Communicate these to all staff, volunteers, trustees etc (e.g. as part of induction, regular training, team meetings, read and sign).
* Monitor compliance with policies and procedures (e.g. as part of staff appraisals).

# Policies, contracts and procedures

You must have particular policies and contracts in place to comply with data protection legislation. You can download and adapt Digital Care Hub’s free templates to create these. But ensure they work for your organisation and share them with managers, staff and volunteers.

Find free templates at [www.digitalcarehub.co.uk/dspt/templates-and-policies/](http://www.digitalcarehub.co.uk/dspt/templates-and-policies/)

### Policies

Have policies in place covering the following as a minimum:

* [Privacy Notice](https://www.digitalcarehub.co.uk/resource/privacy-notice-template/)
* [Data Protection Policy](https://www.digitalcarehub.co.uk/resource/data-protection-policy-template/)
* [Data Quality Policy](https://www.digitalcarehub.co.uk/resource/data-quality-policy-template/)
* [Record Keeping Policy (Also known as a Data or Document Retention Policy)](https://www.digitalcarehub.co.uk/resource/record-keeping-policy-template/)
* [Data Security Policy](https://www.digitalcarehub.co.uk/resource/data-security-policy-template/)
* [Network Security Policy](https://www.digitalcarehub.co.uk/resource/network-security-policy-template/)
* [Smart Phone Policy BYOD](https://www.digitalcarehub.co.uk/resource/smart-phone-policy-template-byod/) OR [Smart Phone Policy Template – Organisation Provided Phones](https://www.digitalcarehub.co.uk/resource/smart-phone-policy-template-organisation-provided-phones/)

### Contracts

Have contracts in place covering:

* [Third party contracts](https://www.digitalcarehub.co.uk/resource/3rd-party-contracts-guidance/)
* [Staff confidentiality contracts – sample clause](https://www.digitalcarehub.co.uk/resource/staff-confidentiality-contract-clause-template/)

### Procedures

Have procedures and records in place covering:

* [Business Continuity Plan for Data and Cyber Security](https://www.digitalcarehub.co.uk/resource/creating-and-testing-a-business-continuity-plan-for-data-and-cyber-security/)
* [How to document your data processing, including template information asset register (IAR) and Record of Processing Activities (ROPA)](https://www.digitalcarehub.co.uk/data-security-protecting-my-information/how-to-document-your-data-processing/)
* [Secure Disposal of Personal Data](https://www.digitalcarehub.co.uk/resource/advice-on-contracts-for-secure-disposal-of-personal-data/)
* [Passwords](https://www.digitalcarehub.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/)

### Recommended documentation

In addition to the required policies, we recommend that you consider having the following in place.

* [Training Needs Analysis](https://www.digitalcarehub.co.uk/resource/training-needs-analysis/)
* [Data Security Audit Checklist](https://www.digitalcarehub.co.uk/resource/data-security-audit-checklist/)
* [Data Security Breach Incident Reporting Form](https://www.digitalcarehub.co.uk/resource/data-security-breach-incident-reporting-form-template/)
* [Mobile Devices Assignment Form](https://www.digitalcarehub.co.uk/resource/portable-devices-assignment-form-template/)
* [Template Suppliers List](https://www.digitalcarehub.co.uk/resource/template-suppliers-list/)
* [Business continuity plan audit tool](https://www.digitalcarehub.co.uk/resource/business-continuity-plan-audit-tool/)
* [Multi-factor authentication record](https://www.digitalcarehub.co.uk/data-security-protecting-my-information/cyber-security/implement-multi-factor-authentication-mfa/)