Digital Care Hub

DSPT

Better Security.
Better Care.

LONDON CARE AND SUPPORT FORUM

social care, personal support and health services across the Capital

South London Partner

What is the Data Security and Protection Toolkit?

An online self assessment of your organisation's data security

Demonstrates compliance with data protection legislation

Reviewed annually

Gives advice and is a checklist of good practice

Why do providers need to pay attention to this?

- Data and cyber security is important for **safe sharing of records** – especially with increased use of digital technology during the pandemic
- It will help you **keep people's confidential information safe**
- It will help **protect your business** from the risk of being fined for a data breach and from the disruption of a cyberattack
- The DSPT will **demonstrate compliance with legal and CQC requirements**
- It's often a **contractual requirement** from councils and the NHS
- The DSPT will be your passport to **shared care records** and other digital innovations with health

  services,enablingyoutobepartofatrulyjoinedupcarenetworkwiththeinterestsofthepeople you support and care for at the centre

Why DSPT is Essential

Legal Compliance: Demonstrates adherence to Data Protection Legislation and Data Security Standards, vital for avoiding fines.

Builds Trust: Reassures service users, families, and staff that their sensitive information is secure, enhancing reputation.

Access to NHS Systems: Required for accessing NHSmail and shared care records, enabling integrated care.

CQC Compliance: Helps answer CQC questions about data governance, impacting quality ratings.
Cyber Resilience: Helps providers implement security measures against increasing cyber threats.
Contractual Requirement: Often a prerequisite for NHS contracts, tenders, and partnerships.

Consequences of Not Having or Getting it Wrong

- Data Breaches & Fines: Increased risk of breaches, leading to ICO investigations and significant fines.
- Regulatory Issues: Fails CQC inspections, especially regarding well-led and governance criteria.
- Loss of Services: Inability to use NHS digital tools like NHSmail.
- Reputational Damage: Loss of public and partner trust, damaging brand and business.
- Business Disruption: Difficulty securing contracts and maintaining partnerships.
- Legal Action: Potential breaches of GDPR and other laws.

In essence, the DSPT isn't just a formality; it's a core requirement for safe, legal, and effective digital operation in modern social care, with serious repercussions for non-compliance

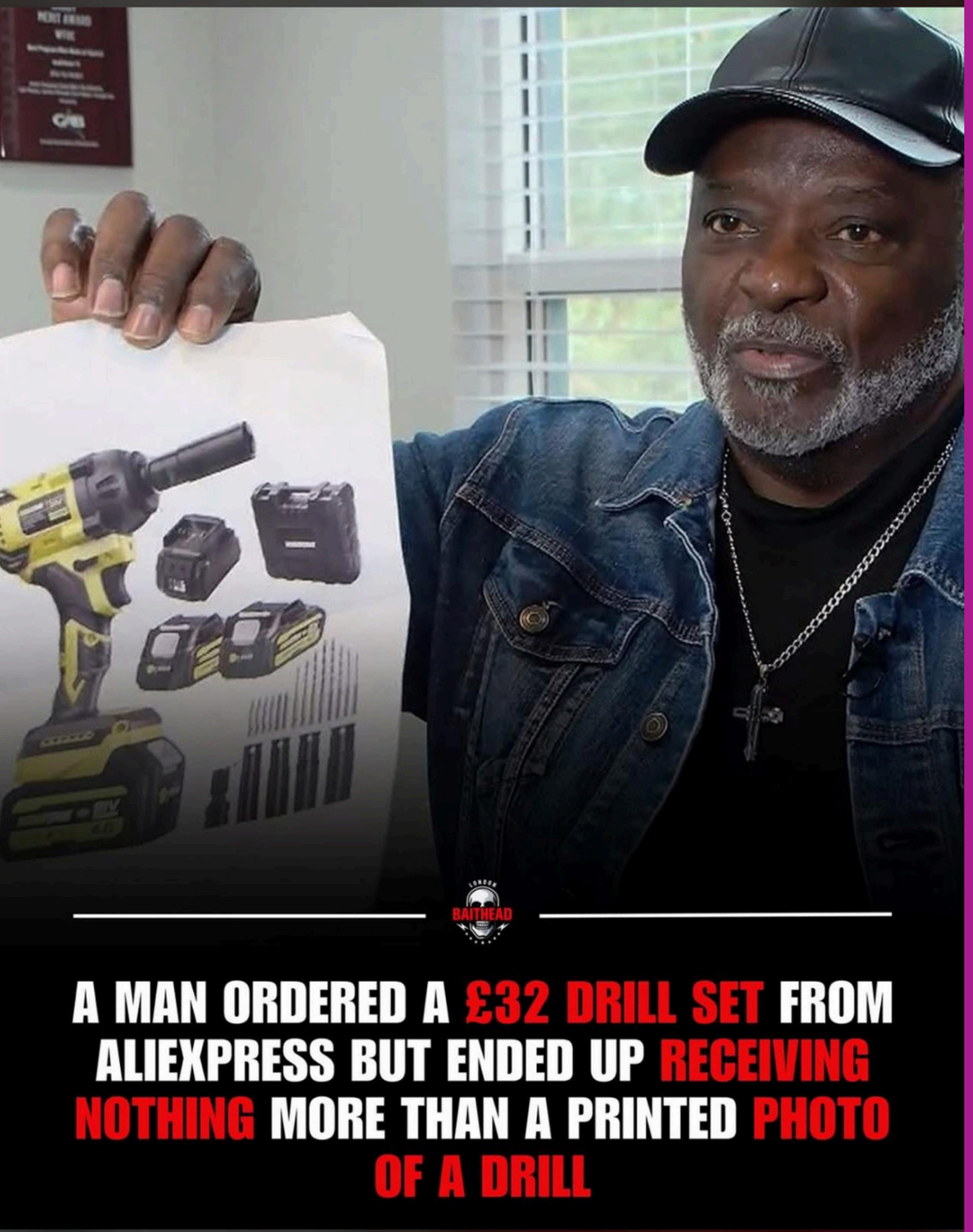
CQC's Chief Digital & Data Officer said:

"CQC will increasingly expect a good provider to comply with the Data Security and Protection Toolkit or equivalent, as a minimum. This also applies where you use a combination of digital and paper record systems."

Mobile devices

Including smartphones and tablets these are devices increasingly being used by care providers to access and manage care data. As they leave the safety of a fixed working environment, they often need additional protection.

‘A small Domiciliary care service in Leicester, were left stunned after a phishing attack breached their email server and gained access to carer’s personal devices, getting their hands on banking information which had devastating consequences.”

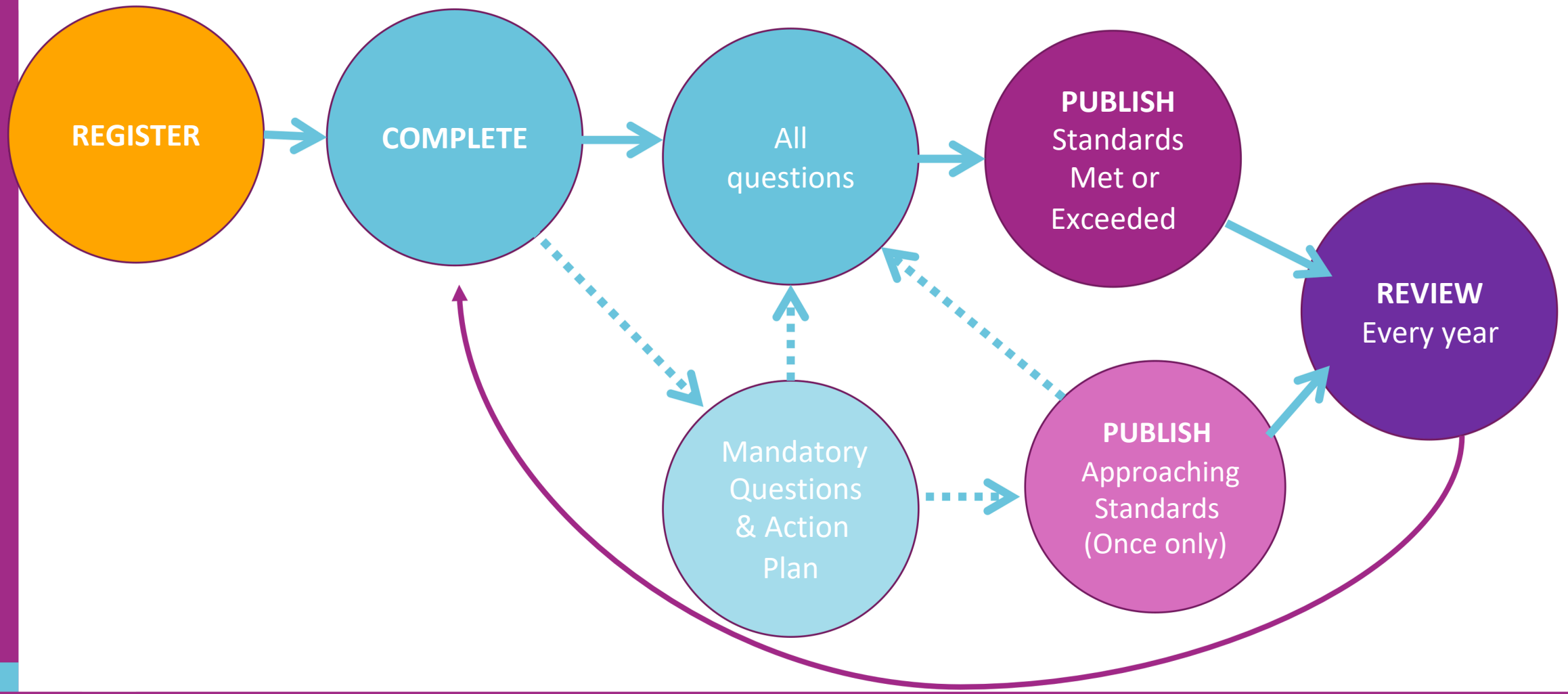


It’s not just about being Cybersecure it’s about being Cyber-Aware

The Better Security, Better Care Programme provides free support for Adult Social Care to help providers complete the DSPT. It does this through 28 Local Support Partners situated across England (with LCAS in South London) to offer specialised, tailored support to the sector.

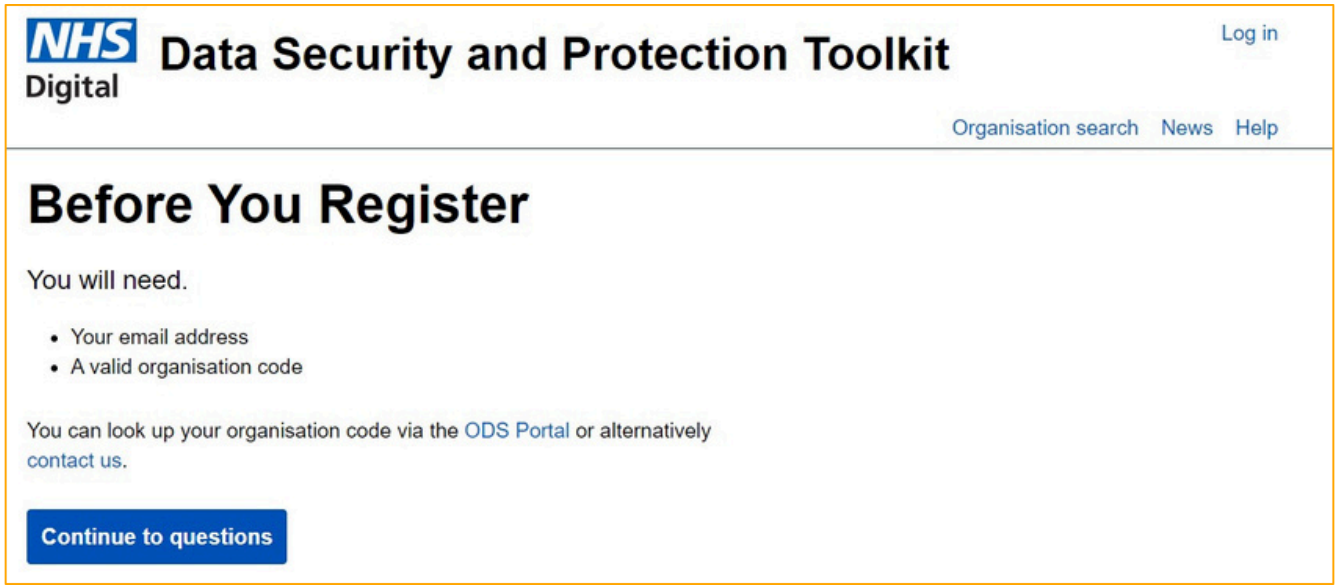
For any further information, please contact
Peter Webb peter@lcasforum.org
07956878901 Or
Dudley Sawyerr dudley@lcasforum.org
07984466130

The ‘Toolkit Journey’



Register – go to the right page

- Go to https://www.dsptoolkit.nhs.uk/Account/Register
- Or, search for ‘DSPT’ and choose the first link, then choose Register



Registration with ICO

- Every organisation must be registered with the ICO
- Link in the Action Plan to double check

InformationCommissioner'sOffice-Registerofdataprotectionfeepayers(ico.org.uk)

- If not registered , get them to do it as a priority
- Can be fined if not registered

Social Care: 42 Questions in 4 groups

Question group	Number of questions to achieve Approaching Standards	Number of questions to achieve Standards Met
Staffing and roles	4	7
Policies and procedures	10	12
Data security	5	9
IT systems and devices	7	17
Total	**26**	**45**

2 additional question for 2025/26

Evidence item 7.1.1

Do you have a digital asset register detailing your organisation's hardware and software , which is kept up to date?

This digital asset register is a list of the digital devices (hardware) and computer software your organisation uses. The register should have been reviewed at least once in the last twelve months.

You can have a separate list of digital assets or combine it into one document with your Information Asset Register (see 1.1.2.).

Download and adapt our digital asset register template.

View our guidance on managing assets – including information asset registers (IAR), digital assets register (DAR) and record of processing activities (ROPA).

- Upload a document
- Reference an existing uploaded document
- Specify an intranet or internet link to a document
- Enter text describing the document's location

Comments (optional)

Save or Cancel

Evidence item 4.3.1

Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?

The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others.

This requirement applies to IT system administrators working in external companies who support your organisation's IT systems. This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s.

If your organisation does not use any IT systems, then 'tick' and write ""Not applicable"" in the comments box.

Download and adapt our template: Privileged Access Agreement – Statement of Compliance.

Comments (optional)

Save or Cancel

Privacy Notices

- Does your organisation have a privacy notice?
- Allorganisationsshouldhaveoneormoretocover all types of people they hold data on (e.g. clients and staff)
- Key things to check:
  - Howvisible isit?
  - Where is it, how is it shared?
  - When was it last reviewed and up-dated?
  - Doesit coverthe nationaldataoptout?
- Template Privacy notice on DSC – get them to check theirs against it

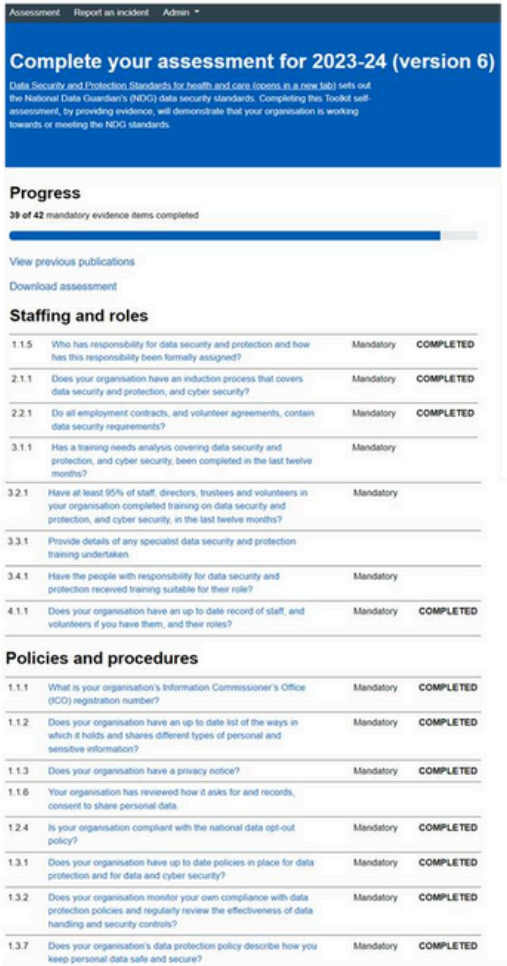
Privacy Notice - Template - Digital Care Hub

- More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital] and [National Data Opt-Out - Digital Care Hub]

Policies for data protection and data and cyber security

- Does your organisation have up-to-date policies for data protection and data and cyber security?
- Most will have them – could be one or more
- Should cover
  - Data protection
  - Data quality
  - Record keeping
  - Data security
  - Network security (if relevant)
- Ask:
  - Do they have them? (ask to see them)
  - Are they up-to-date?
  - How do they know they are beingimplementedandstaffarefollowingthem?
- Template policies on DCH Template Policies and Resources - Digital Care Hub

Republishing and sharing DSPT Assessments



Care providers must review, update and republish their toolkit assessment at least once every year, otherwise it goes out of date and it is invalid

Toolkit will look slightly different after the initial publication
78 social care questions including non-mandatory questions they don't need to answer.
Once they have completed 43 mandatory questions, they can republish
For more information on republishing see:
https://www.digitalcarehub.co.uk/dspt/publish-or-republish/republishing/

How to share proof of the DSPT Assessment:
https://www.digitalcarehub.co.uk/dspt/publish-or-republish/

Spot Checks

- Does your organisation monitor your own compliance with data protection policies and regularly review the effectiveness of data handling and security controls? (i.e. spot checks)
- There is an example audit checklist that you can download from DCH

DataSecurityAuditChecklist - DigitalCareHub

Ask:

- Do you do regular checks/audit?
- Do you have an audit checklist for this?
- Do you have a log of these and the actions that have been taken?
- What do you do to check staff are following your policies and procedures?

DSPT

Better Security.
Better Care.

Digital Care Hub

LONDON CARE AND SUPPORT FORUM

social care, personal support and health services across the Capital

South London Partner

For any further information, please contact

Peter Webb peter@lcasforum.org
07956878901 Or
Dudley Sawyerr dudley@lcasforum.org
07984466130