



DSPT
Better Security.
Better Care.



Digital
Care Hub

New Changes to the DSPT

Sally Willcox

29th September 2026





DSPT

Better Security.
Better Care.



Digital
Care Hub

House Keeping

- This webinar is being recorded
- Attendees are on mute and can't be seen
- Please use the **Q&A** function to ask questions, not the chat.
- You will get access to the recording and the presentation



Photo by [Valeriia Svitlini](#) on [Unsplash](#)



DSPT

Better Security.
Better Care.



Digital
Care Hub

Agenda

- New DSPT Questions (mandatory)
- Wording changes
- New resources and guidance
- Support options
- Q&A



No extra questions in V9

AT A GLANCE

"No new questions have been added to the DSPT — the total is still 45 mandatory questions."

Still 45 mandatory

What this means

- Version 9 adds no additional questions to the Toolkit.
- The number of mandatory questions is unchanged at 45.
- What has changed is the wording of some questions and their tool tips.



1.1.2 Information asset register and ROPA

NEW WORDING (V9)

*“Does your organisation **maintain** an up to date **information asset register (IAR)** and a **record of processing activities (ROPA)**, and **review this regularly?**”*

Mandatory: Yes

What this means

- The question now names the IAR and ROPA directly, instead of describing “the ways in which it holds and shares information”.
- The IAR details where and how information is held and how you keep it safe.
- The ROPA lists the types of personal data shared with others – for example needs assessments, prescriptions, payslips, care plans – and how it is shared and kept safe.
- You can combine these into one register, or keep two separate documents.
- The register must have been reviewed and approved by the management team within the last twelve months.
- Example IAR and ROPA templates are available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/how-to-document-your-data-processing/>



1.1.3 Privacy notice

NEW WORDING (V9)

*“Does your organisation **maintain an up-to-date** privacy notice **that clearly explains how information is used**?”*

Mandatory: Yes

What this means

- Expanded from “have a privacy notice” to “maintain an up-to-date privacy notice”
- Added “that clearly explains how information is used”
- The tool tip now states plainly: if you use and share personal data, you must tell people what you are doing with it.
- Tell them what is collected and why, how long it is kept, who it is shared with, how it is kept secure, and their rights – such as the right to access their information.
- Set this out in writing in a privacy notice, in clear, open and honest language that is easy to read, and in a range of formats suited to different audiences.
- Cover all the data you process – people you support and their relatives, staff, volunteers, members of the public. You may have more than one notice.
- An example privacy notice is available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/resource/privacy-notice-template/>



1.3.1 Policies

NEW WORDING (V9)

*"Does your organisation **maintain** up-to-date **data protection and cyber security** policies aligned with best practice and national guidance.?"*

Mandatory: Yes

What this means

- Last year the question was "Does your organisation have up to date policies in place for data protection and for data and cyber security, aligned with good practice guidance and (where applicable) national policies?"
- The key change happened a year ago: in v7 this question said "Does your organisation have up to date policies in place for data protection and for data and cyber security?"
- The difference between v8 and 9 is in the tooltip as it now states what policies you should have as a minimum.

<https://www.digitalcarehub.co.uk/dspt/templates-and-policies/>



1.3.14 Mobile devices

NEW WORDING (V9)

*"What does your organisation have in place to minimise the risks if **laptops**, mobile phones **and other devices** are lost, stolen, hacked or used inappropriately? .?"*

Mandatory: Yes

What this means

- Emphasis on mobile devices more widely not just phones.

<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/cyber-security/reduce-the-risk-and-impact-of-a-cyber-incident/protect-mobile-devices-and-tablets/>



1.4.2 Third-party destruction contracts

NEW WORDING (V9)

*"If your organisation uses third parties to destroy records or equipment that hold personal data **or other data important to the delivery of care**, is there a written contract in place that has been reviewed in the last twelve months? This contract should meet the requirements set out in data protection regulations."*

Mandatory: Yes

What this means

- Expanded from only personal data
- When there is no longer a valid reason to keep data, it must be disposed of securely – paper documents, electronic records and equipment such as old computers, mobile phones, CDs and memory sticks.
- If you use a contractor – for example a shredding company or IT recycler – the contract or other written confirmation must require appropriate security measures and allow your organisation to audit them.
- The contract must have been reviewed within the last twelve months.
- If you do not use third parties to destroy records or equipment, write "Not applicable" in the text box.
- Advice on contracts for secure disposal of personal data is available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/records-management-abbreviated-code-of-practice-and-guidance-for-adult-social-care-providers/>



1.4.3 Destroying records securely in-house

NEW WORDING (V9)

*"If your organisation destroys any records or equipment that hold personal data **or other data important to the delivery of care**, how does it make sure that this is done securely?"*

Mandatory: Yes

What this means

- Expanded from only personal data
- When there is no longer a valid reason to keep data, it must be disposed of securely – paper documents, electronic records and equipment such as old computers, mobile phones, CDs and memory sticks.
- If anyone in your organisation destroys records or equipment themselves, such as shredding documents, briefly describe how you make sure this is done securely.
- If you only use third parties and do not destroy records yourselves, write "Not applicable" in the text box.
- Advice on the safe destruction of personal data is available from Digital Care Hub (Records Management Code of Practice, Section 5).

<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/records-management-abbreviated-code-of-practice-and-guidance-for-adult-social-care-providers/>



5.1.1 Reviewing processes after a breach or near miss

NEW WORDING (V9)

*"If your organisation has had a data **or a cyber security breach** or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?"*

Mandatory: Yes

What this means

- Expanded from just data breaches to include cyber security breaches
- Confirm you have reviewed any process that caused a breach or near miss, or that forces people into unauthorised workarounds which could compromise data and cyber security.
- Workarounds include using unauthorised devices such as home computers or personal memory sticks, or forwarding emails to personal email addresses.
- It is good practice to review processes annually even if no breach or near miss has taken place.
- If there were no breaches or near misses in the last twelve months, tick the box and write "Not applicable" in the comments box.



6.1.3 Informing individuals after a high-risk breach

NEW WORDING (V9)

*"If your organisation has had a data breach, **did you consider the risk to affected individuals** and were all individuals who were affected informed where the risk was high?"*

Mandatory: Yes

What this means

- Minor wording change
- If a breach is likely to result in a high risk to individuals' rights and freedoms, you must inform those affected without undue delay.
- High risk examples include damage to reputation, financial loss, unfair discrimination, information that could allow identity fraud, or individuals being targeted by people with malicious intent.
- If there have been no such breaches in the last twelve months, tick and write "Not applicable" in the comments box.
- More information is available from the Information Commissioner's Office.

<https://ico.org.uk/for-organisations/report-a-breach>



6.2.1 Antivirus and antimalware software

NEW WORDING (V9)

"Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?"

Mandatory: Yes

What this means

- No change to the question, minor change to the tooltip
- This applies to all servers, desktop computers, laptops and tablets.
- Antivirus and antimalware software are the same thing – they perform the same functions.
- You may need to ask your IT support company to help answer this question.
- If your organisation does not use any computers or other devices, tick and write "Not applicable" in the comments box.
- Further information is available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/cyber-security/reduce-the-risk-and-impact-of-a-cyber-incident/have-up-to-date-antivirus-software/>



7.1.1 Digital asset register

NEW WORDING (V9)

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

Mandatory: Yes

What this means

- No change to wording – new links in the tooltip
- The digital asset register lists the digital devices (hardware) and computer software your organisation uses.
- It should have been reviewed at least once in the last twelve months.
- You can keep it as a separate list or combine it with your Information Asset Register (see 1.1.2).
- A digital asset register template and guidance on managing assets – IAR, DAR and ROPA – are available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/resource/digital-asset-register-template/>



7.1.2 Business continuity plan

NEW WORDING (V9)

*“Does your organisation **ensure its business continuity plan covers data and cyber security, and that is regularly reviewed and tested?**”*

Mandatory: Yes

What this means

- Addition of the requirement to regularly test it.
- The plan should cover data and cyber security – for example how you would continue delivering care during a power cut, loss of phone or internet, a hack, a broken computer, or loss of the office through fire.
- It should include communications with other organisations and your data protection obligations.
- It should be understood by relevant staff and other stakeholders, and be reviewed and tested regularly.
- An example business continuity plan is available from Digital Care Hub.

<https://www.digitalcarehub.co.uk/resource/creating-and-testing-a-business-continuity-plan-for-data-and-cyber-security/>



7.3.1 Secure, tested backups

NEW WORDING (V9)

*"How does your organisation make sure that there are working, **appropriately secure** backups of all important data and information?"*

Mandatory: Yes

What this means

- Addition of "appropriately secure"
- New links added to tooltip
- Back up your most important data somewhere separate from your computer – a secure external hard drive or cloud-based storage.
- Test your backups regularly so you know they work.
- Briefly explain how your backup systems work and how you have tested them; your IT support company may need to help.
- The National Cyber Security Centre has a small business guide and advice on offline backups. <https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security/backing-up-your-data>
- If your organisation does not use computers or IT systems at all, write "Not applicable" in the text box.

<https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world>



7.3.2 Emergency contacts kept securely

NEW WORDING (V9)

*"Are all emergency contacts kept securely, **separate from your computer**, in hardcopy and are they up to date?"*

Mandatory: Yes

What this means

- Change of emphasis from hardcopy to separate from your computer
- Contacts are those needed to enact the business continuity plan covering data and cyber security, including phone numbers as well as email addresses.
- Store the list separately from your computer or IT system – for example a hardcopy – so you can reach it when systems are down.
- Contacts should include your IT support company, IT systems suppliers, your ICB or local authority commissioner(s), the NCSC reporting line, and your DPO or Data Security and Protection Lead.
- Check that all contacts are up to date.



10.2.1 Assuring IT supplier cyber security

NEW WORDING (V9)

“How does your organisation assure that your IT system suppliers have robust cyber security arrangements?”

Mandatory: Yes

What this means

- Check that any supplier of IT systems – and your IT support company – holds a cyber security certification. IT systems include rostering, care planning and electronic MAR charts.
- Suitable certifications: Cyber Essentials (ideally Plus, verifiable on the IASME certificate search); ISO 27001 (ask to see the certificate); or DSPT “Standards Met” – ideally “Standards Exceeded”, which also means Cyber Essentials Plus.
<https://iasme.co.uk/cyber-essentials/ncsc-certificate-search>
- External assurance also counts – for example a digital social care record supplier on the Assured Solutions List has been assured by NHS England.
- Briefly explain what certification your suppliers hold and what checks you carried out.
- If suppliers have no certification, outline what you do to assure they prioritise data protection and cyber security – for example recognised cyber security training, or cyber security requirements written into contracts.
- If you use no IT systems and have no external IT support, tick and write “Not applicable” in the comments box.
- Guidance is available from Digital Care Hub.
<https://www.digitalcarehub.co.uk/data-protection-and-cyber-security/cyber-security/reduce-the-risk-and-impact-of-a-cyber-incident/manage-your-suppliers/>



The most significant change is to 10.2.1

2025/26 v8

Do your organisation's IT system suppliers have cyber security certification?

2026/27 v9

How does your organisation assure that your IT system suppliers have robust cyber security arrangements?

- This question has changed from a yes/no tick box to a text one.
- The focus has changed from verifying that all your IT suppliers have cyber certification to explaining what due diligence you undertake.
- The tool tip gives some examples of how to do this and links to a revised DCH page on managing your suppliers



Full programme of support

Data Security and
Protection Toolkit



Better Security, Better
Care.



Cyber Resilient Care:
Support to small
providers



New Care Services



Cyber Security Guidance



Adult Social Care
Caldicott Guardian
Learning Network



- ✓ Free and official
- ✓ Online guidance, step by step films
- ✓ Webinars
- ✓ FAQs
- ✓ Template policies
- ✓ Helpline
- ✓ Tailored support from Local Support Partners across England

[digitalcarehub.co.uk/
bettersecuritybettercare](https://digitalcarehub.co.uk/bettersecuritybettercare)





DSPT

Better Security.
Better Care.



Digital
Care Hub

Any questions?





Thank you.