



Using the Data Security and Protection Toolkit for the first time

12 May 2022

DSPT

Better security.
Better care.

Ann Garvey and Mikaela Williams-Brown
Liverpool Social Care Partnership (LSCP)

The technical issues



DSPT
Better security.
Better care.

- This webinar is being recorded
- **This is for** care providers who have never published DSPT in the past
- Attendees are on mute and can't be seen
- Please use the **Q&A** function to ask questions.
- On a phone, tap the screen to see the controls – choose More and then **Q&A**
- Questions that we can't answer: we will come back to you. Add your email to Q&A
- This webinar will last no longer than one hour
- You will get access to the recording and the presentation (inc links)

Today – our agenda



DSPT
Better security.
Better care.

- Welcome and introductions
- The Data Security and Protection Toolkit (DSPT)
- Registering
- Completing
- Publishing
- Support from the Better Security, Better Care Programme
- Please use Q&A (not Chat) for your questions

Poll



DSPT
Better security.
Better care.

Care providers:

- Has your service registered on the DSPT?
- If registered, have you started to complete the DSPT?
- Are you a single or multi site organisation?

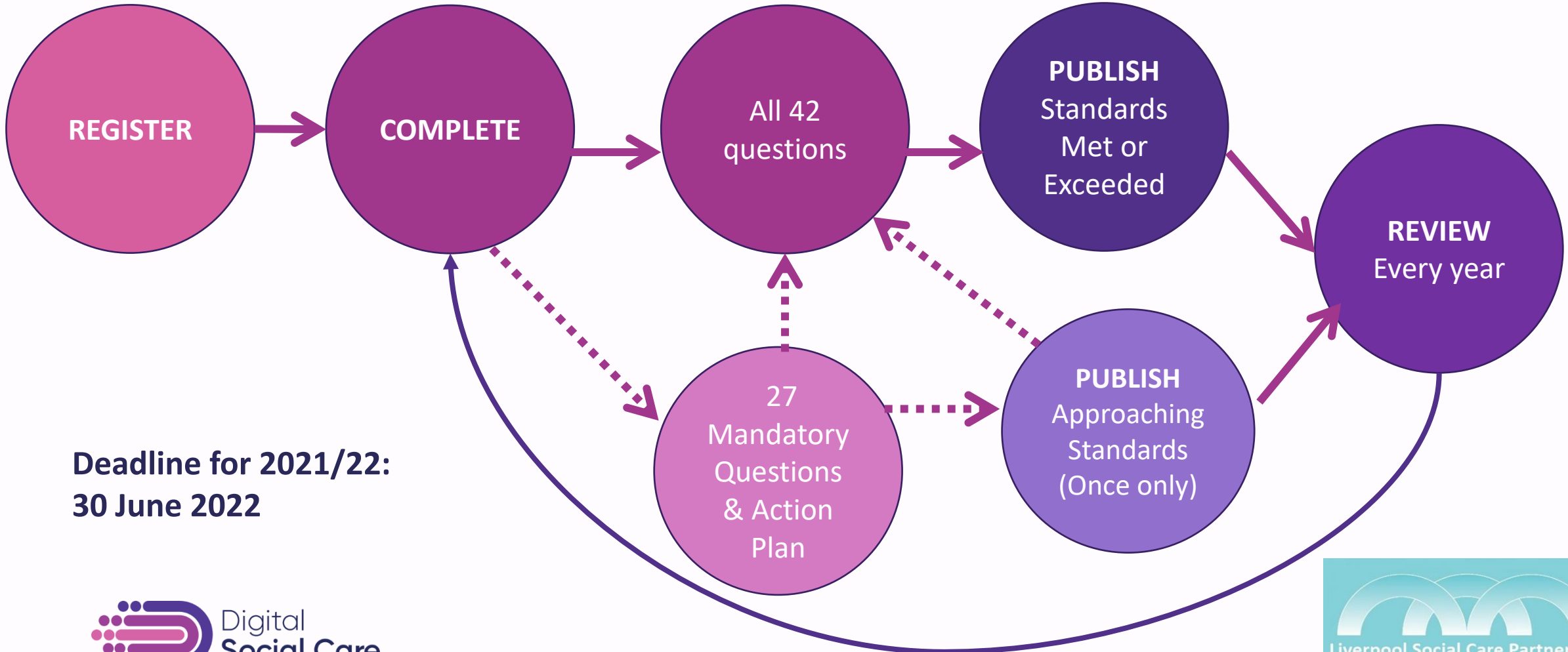


DSPT
Better security.
Better care.

Your 'Toolkit Journey' – start now!



DSPT
Better security.
Better care.



**Deadline for 2021/22:
30 June 2022**

Your fellow travellers



DSPT
Better security.
Better care.

Better Security,
Better Care -
National support
and resources



Better Security,
Better Care -
Local support



Template Policies
and Resources for
DSPT



Check your DSPT
status



Use the DSPT for
the First Time



Published Before:
Review and
Republish your
DSPT



Free and official
Online guidance, step by step films
Webinars
FAQs
Template policies
Helpline
Tailored support from 28 Local
Support Partners across England

digitalsocialcare.co.uk/bettersecurity
[bettercare](https://digitalsocialcare.co.uk/bettercare)

CQC and DSPT



DSPT
Better security.
Better care.

Better record keeping and accountability assist with CQC regulatory compliance.

In November 2021 CQC introduced KLOE's that included information governance/use of technology, they include;

- **Effective – E1.3** How is technology and equipment used to enhance the delivery of effective care & treatment and to support people's independence?
- **Responsive – R1.6** How is technology used to support people to receive care and support quickly? Is the technology easy to use?
- **Well Led – W4.6** Are information technology systems used effectively to monitor and improve quality of care?
- **Well Led – W5.2** Does the service share appropriate information and assessments with other relevant agencies for the benefit of people who use the service?

Registering on the DSPT for the first time



DSPT

Better security.
Better care.

How to register for the Toolkit



DSPT
Better security.
Better care.



Find your ODS codes – what codes are there?



DSPT
Better security.
Better care.

- For **single sites**, for example:
 - a single care home
 - a home care agency with one CQC registered office



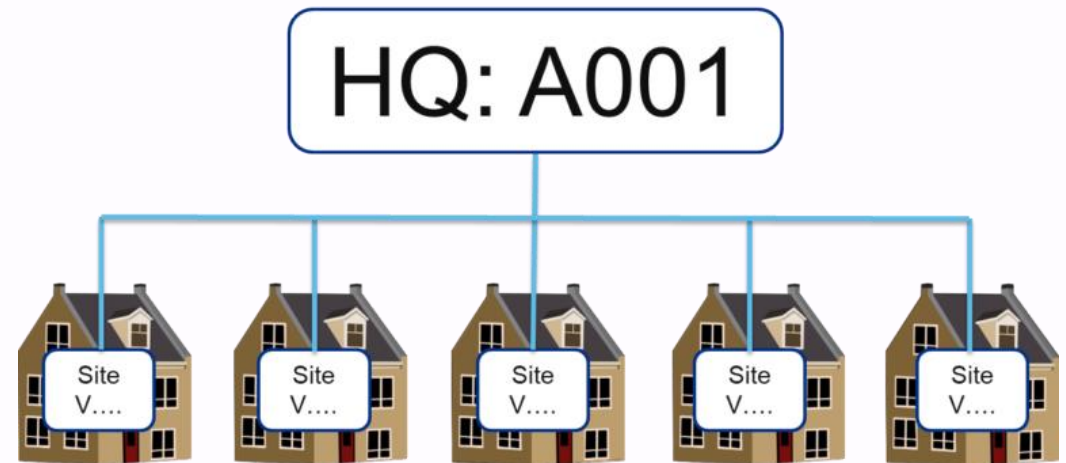
Register with your V code



DSPT
Better security.
Better care.

Find your ODS codes – what codes are there?

- For **multi sites**, for example:
 - a group of care services that share the same policies and procedures



Register with your A code
Your registration will cover all sites



DSPT
Better security.
Better care.

Find your ODS codes – what codes are there?

- For more complex **multi sites**, for example:
 - Several branches
 - And/or
 - More than one type of service provided e.g. care homes and home care



Seek advice from the helpdesk

0300 303 4034 or exeter.helpdesk@nhs.net

Find your ODS codes



DSPT
Better security.
Better care.

- Find your ODS code <https://odsportal.digital.nhs.uk/Organisation/Search>
- Or, search for 'ODS Portal' and choose Organisation/Practitioner search
- If you cannot find your code, or aren't sure which one/s to use, contact the DSPT Exeter helpdesk on 0300 303 4034, or email exeter.helpdesk@nhs.net

DSPT – so where do I start?



DSPT
Better security.
Better care.

- The toolkit is here: www.dsptoolkit.nhs.uk

BETA This is a new service

NHS Data Security and Protection Toolkit
Digital

Register Log in

Organisation search News Help

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

This system is subject to ongoing development.

To find out if your organisation is already registered or has published the Toolkit

If not, register here

Register and complete your organisation profile



DSPT
Better security.
Better care.

NHS Digital Data Security and Protection Toolkit
Beta This is a new service - your feedback will help us to improve it.

Assessment News Report an Incident Help Admin

Kim Hobday - ABC Surgery Change Organisation Log Out

Organisation Profile

Before starting your assessment we need to ask you some questions.

The answers you give will:

- tailor your assessment to your organisation's sector
- pre-populate elements of your assessment
- help us to produce national reports

Continue to questions

BETA This is a new service - your feedback will help us to improve it.

NHS Digital Data Security and Protection Toolkit My account Logout

Oxford Brookes University - Institute of Public Care Change organisation Organisation search News Help

Assessment Report an Incident Admin

Back to View your Profile Details Screen

Oxford Brookes University - Institute of Public Care Profile Details

Which of these categories best describes your organisation?

Choose one from the list below. Read about sectors (opens in a new tab)

<input type="radio"/> Acute	<input type="radio"/> GP
<input type="radio"/> Ambulance Trust	<input type="radio"/> Local Authority
<input type="radio"/> AQP Clinical Services	<input type="radio"/> Mental Health Trust
<input type="radio"/> AQP Non-Clinical Services	<input type="radio"/> NHS Business Partner
<input type="radio"/> Arms Length Body	<input type="radio"/> NHS Digital
<input type="radio"/> CCG	<input type="radio"/> Optician
<input type="radio"/> Charity / Hospice	<input type="radio"/> Pharmacy
<input type="radio"/> Community Services Provider	<input type="radio"/> Prison
<input type="radio"/> Company	<input type="radio"/> Researcher / Department
<input type="radio"/> CSU	<input type="radio"/> Secondary Use Organisation
<input type="radio"/> Dentist (NHS)	<input checked="" type="radio"/> Social Care
<input type="radio"/> Dentist (Private)	<input type="radio"/> University

Save

Choose Social Care

USEFUL LINKS

[Guidance on Registering](#)

[Contact your Local Support Organisation](#)

Setting up other users



DSPT
Better security.
Better care.

Auditor

- View only

Member

- Add/edit evidence

Administrator

- Manage users
- Add/edit evidence
- Confirm evidence (“confirm assertions”)
- Publish

Support on registering



DSPT
Better security.
Better care.

Guidance and support

Follow the appropriate guidance for your service below. You can also watch this webinar recording on how to register. And get free support to register and complete your DSPT from the Better Security, Better Care programme.



Register: Multisite
Social Care
Organisations



Register: Single
Site Organisations



Better Security,
Better Care.



USEFUL LINKS

[Guidance and webinar recordings on Digital Social Care website](#)

[Contact your Local Support Partner](#)

Any questions?



DSPT
Better security.
Better care.



Completing the DSPT questions



DSPT

Better security.
Better care.

Answers are NOT public



DSPT
Better security.
Better care.

- This is a self-assessment
- Your answers are NOT published – just the DSPT status that you achieve based on your self-assessment
- Not a tick box exercise – use it to work through what you need to do
- Use the answers and comments sections to record valuable information. Helps with future DSPT publications

The social care view



DSPT
Better security.
Better care.

TEST This is a new service - your [feedback](#) will help us to improve it.

NHS Digital **Data Security and Protection Toolkit** [My account](#) [Logout](#)

This is a test site and is not intended for live use.

Liverpool 3 [Change organisation](#) [Organisation search](#) [News](#) [Help](#)

[Assessment](#) [Report an Incident](#) [Admin](#) ▾

Social Care Assessment

Key data security requirements for social care organisations are listed below. Please respond to the following requirements and publish your assessment.

Important
If you only respond to the MANDATORY requirements, you will be asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.1.1	Does your organisation have an induction process that covers data security and	Mandatory



The social care view



DSPT
Better security.
Better care.

Hotels.com Addons Store Facebook YouTube

Important

If you only respond to the MANDATORY requirements, you will be asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.1.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	
3.2.1	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?	
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?	
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory

Click on an evidence item (in blue) to answer the question and see the detailed guidance

Policies and procedures



Questions are grouped under 4 headings



DSPT
Better security.
Better care.

Question group	Number of questions to achieve status of Standards Met
Staffing and roles	7
Policies and procedures	11
Data security	8
IT systems and devices	16



DSPT
Better security.
Better care.

1. Staffing and roles - What the questions cover

- Who has responsibility for this area of work?
- Staff records and contracts
- Data protection and cyber security induction and training for all staff

Staff records



DSPT
Better security.
Better care.



What the question asks 4.1.1



DSPT
Better security.
Better care.

- 4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?

action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.1.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	
3.2.1	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?	
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?	
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory

Question 4.1.1



Policies and procedures

1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory
1.1.2	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Mandatory
1.2.1	Does your organisation have a privacy notice?	Mandatory

action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5 Who has responsibility for data security and protection and how has this responsibility been formally assigned? Mandatory

2.1.1 Evidence item 4.1.1

2.1.2 **Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?**

3.1.1 Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.

3.2.1

3.4.1 Comments (optional) Evidence item 4.1.1

4.1.1

Save or Cancel

Policy

1.1.1 What is your organisation's Information Commissioner's Office (ICO) registration number? Mandatory

1.1.2 Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information? Mandatory

1.2.1 Does your organisation have a privacy notice? Mandatory



Example Response to Question 4.1.1

4.1.1

Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?

Yes

Comments:

Staff and volunteer registered are contained in HR files, both hard copies and electronic versions which are saved on both the Google Drive and portable D drive in the Operations Director's office. The hard copies are kept in a locked drawer

Example question 1.1.5



DSPT
Better security.
Better care.

Evidence item 1.1.5

Who has responsibility for data security and protection and how has this responsibility been formally assigned?

Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level.

In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO).

[Read more about data security and protection responsibilities and specialised roles.](#)

Write your answer here

Comments (optional)

Save or Cancel

different types of personal and sensitive information?

Question

Tooltip gives best practice advice: it's what you need to do

Tooltip may include links (in blue) to further help

Write your answer here

Comments very useful for colleagues and future

Further information from Digital Social Care



DSPT
Better security.
Better care.

- [Data Security and Protection Responsibilities](#)
- [Staff Guidance](#)
- [Guidance on finding training for staff](#)

2. Policies and procedures

What the questions cover



DSPT
Better security.
Better care.

- Information Commissioner's Office registration
- Policies:
 - Up to date data protection policies
 - Audits and spot checks
- Holding and sharing information
- Retaining records
- Disposing of records and equipment
- List of suppliers

ICO registration



DSPT
Better security.
Better care.

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home Your data matters **For organisations** Make a complaint Action we've taken About the ICO

[For organisations](#) / [Data protection fee](#)

Data protection fee

Share

If you've recently received a letter from the ICO about paying your data protection fee, we hope you'll find our website useful in helping you comply with your other UK GDPR obligations. If you've paid in the last 14 days, please ignore the letter you've received from us. If you need to pay, your fee will need to be renewed every 12 months.

When you complete an application form online or make a payment, we endeavour to send your confirmation early the following working day. However, due to the large volume of work we are currently receiving, your confirmation may arrive later on that following day. We apologise for any inconvenience this may cause.

Further reading

- [Search the register](#)
About the ICO
- [Legal definitions](#)
For organisations
- [Guide to the data protection fee](#)
For organisations



What the question asks – 1.1.1



DSPT
Better security.
Better care.

- 1.1.1 What is your organisation's Information Commissioner's Office (ICO) registration number?

The screenshot shows a web browser window with the URL `demo.dsptoolkit.nhs.uk/Assessment`. The page displays a list of assessment questions. A modal dialog is open over question 1.1.1, titled "Evidence item 1.1.1". The dialog contains the following text:

What is your organisation's Information Commissioner's Office (ICO) registration number?

Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should [register as a matter of urgency](#).

You can check whether you are registered and what your ICO registration number is on the [Information Commissioner's Office website](#)

Below the text is a text input field with a yellow border, currently empty. Underneath the input field is a "Comments (optional)" section with another empty text input field. At the bottom of the modal, there are "Save" and "Cancel" buttons.

The background page shows a list of questions with their IDs and descriptions:

- 3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?
- 3.2.1 Have at least 95% of staff, directors, trustees and volunteers in your organisation
- 3.4.1
- 4.1.1
- 1.1.1
- 1.1.2
- 1.2.1
- 1.2.4
- 1.3.1
- 1.3.2 Does your organisation carry out regular data protection spot checks?
- 1.3.7 Does your organisation's data protection policy describe how you keep personal data safe and secure? Mandatory
- 1.3.8 Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new Mandatory

Response to the Question 1.1.1



DSPT
Better security.
Better care.

1.1.1

What is your organisation's Information Commissioner's Office (ICO) registration number?

We have an ICO certificate on our wall with our ICO registration number: ZA046070.

Comments:

The Organisation was registered on the 18th of March 2014. This certificate is displayed in the main office.



DSPT
Better security.
Better care.

Further support: template policies

Approaching Standards: required policies

- [How to document your data processing, including template information asset register \(IAR\) and Record of Processing Activities \(ROPA\)](#)
- [Privacy Notice Template](#)
- [Data Protection Policy](#)
- [Data Quality Policy – Template](#)
- [Record Keeping Policy – Template \(Also known as a Data or Document Retention Policy\)](#)
- [Data Security Policy – Template](#)
- [Network Security Policy – Template](#)
- [Smart Phone Policy Template – BYOD](#)
- [Contracts: what contracts you must have in place](#)

Standards Met: Additional required policies

- [Training Needs Analysis](#)
- [Data Security Audit Checklist](#)
- [Creating and Testing a Business Continuity Plan for Data and Cyber Security](#)

Recommended documentation

- [Data Security Breach Incident Reporting Form – Template](#)
- [Mobile Devices Assignment Form – Template](#)
- [Smart Phone Policy Template – Organisation Provided Phones](#)
- [Template Suppliers List](#)

[Find template policies to download and reuse on Digital Social Care website](#)

3. Data security - What the questions cover



DSPT
Better security.
Better care.

- Data breaches:
 - What is a data breach? What is a 'near miss'?
 - What your plans should cover
- Physical security and paper records 'on the move'
- Business continuity:
 - 'Data emergencies' – what your plans should cover
 - How to make sure your plans will work

4. IT systems and devices - What the questions cover



DSPT
Better security.
Better care.

- People and their access to information
- Passwords
- Backups
- Protecting your devices
- Technical set up and support
- What documentation should your suppliers have?

Example Question 4.1.2



DSPT
Better security.
Better care.

Approaching Standards Assessment x +

demo.dsptoolkit.nhs.uk/Assessment

Google Amazon.co.uk eBay Hotels.com Addons Store Facebook YouTube

IT Systems and devices

1.3.11	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Mandatory
1.3.14	What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	
4.1.2	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Mandatory
4.2.4	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	Mandatory
4.5.4	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	Mandatory
6.2.1	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	Mandatory
6.3.2	Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?	
7.3.1	How does your organisation make sure that there are working backups of all important data and information?	Mandatory
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory
7.3.4	Are backups routinely tested to make sure that data and information can be restored?	
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?	
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for	

Question 4.1.2

11°C Cloudy

15:31 28/04/2022

Further guidance: Digital Social Care



DSPT
Better security.
Better care.

Staff and workforce

- [Data Security and Protection Responsibilities](#)
- [Staff Guidance](#)
- [Guidance on finding training for staff](#)

IT and software suppliers

- [Guidance on managing software suppliers who process personal data](#)

Document retention and disposal

- [Guidance on document retention](#)
- [Advice on contracts with third parties for secure disposal of personal data](#)

Improving security

- [Guidance on strong passwords](#)
- [Guidance on antivirus software](#)
- [Guidance on back ups](#)
- [Guidance on software updates](#)

Mobile devices

- [Protecting Mobile Phones and Tablets](#)

National Data Opt-Out

- [Guidance on the National Data Opt-Out](#)

Actions

- Contact your [Better Security, Better Care Local Support Partner](#)
- Visit [Digital Social Care website](#) – view guidance, register for free updates

Confirm and Publish your DSPT Assessment



DSPT

Better security.
Better care.

Confirm Answers



DSPT
Better security.
Better care.

1.2 Individuals' rights are respected and supported

1.2.1 Does your organisation have a privacy notice? Mandatory **COMPLETED**

1.2.4 Is your organisation compliant with the national data opt-out policy? Mandatory **COMPLETED**

I confirm that the evidence entered for this assertion is correct
25/04/2022 12:22 by Mikaela Williams-Brown

Publish at Standards Met

42 Mandatory questions answered



DSPT
Better security.
Better care.

- When you have reviewed/updated and answered all 42 questions, and ticked to confirm your answers, click on publish assessment
- **Remember:** your DSPT status will be published. NOT your full report

Assessment Assertions

dsptoolkit.nhs.uk/Assessment

Assessment Report an Incident Admin

Assessment

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

- 1 Personal Confidential Data Staff Responsibilities
- 3 Training
- 4 Managing Data Access
- 5 Process Reviews
- 6 Responding to Incidents
- 7 Continuity Planning
- 8 Unsupported Systems
- 9 IT Protection
- 10 Accountable Suppliers

Progress

Go to progress dashboard and reports

43 of 43 mandatory evidence items provided

36 of 36 assertions confirmed

[Publish Assessment](#) [View previous publications](#)

Filters

Mandatory

1 Personal Confidential Data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only

Publish at Approaching Standards – 27 Mandatory questions answered



DSPT
Better security.
Better care.

demo.dsptoolkit.nhs.uk/Assessment

updates are downloaded and installed?

9.1.1 Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?

9.5.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?

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

Publish Approaching Standards Assessment

Tell us what you think of the service

There is a problem!



DSPT
Better security.
Better care.

below.
Please respond to the following requirements and publish your assessment.

There is a problem
Please complete mandatory requirement 8.3.5 in the IT Systems and devices section

Important
If you only respond to the MANDATORY requirements, you will be asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

The screenshot shows a web browser window with the URL 'demo.dsptoolkit.nhs.uk/Assessment'. The page content includes a blue box with instructions, a red-bordered box with a problem message, and a yellow box with an important note. The Windows taskbar is visible at the bottom, showing the search bar and various application icons.



DSPT
Better security.
Better care.

Headquarters Assessment Publish for all sites

NHS Digital Data Security and Protection Toolkit My account Logout

This is a test site and is not intended for live use.

2309 Test HQ Organisation [Change organisation](#) [Organisation search](#) [News](#) [Help](#)

[Assessment](#) [Report an Incident](#) [Admin](#)

Headquarters Assessment

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

- 1 Personal Confidential Data
- 2 Staff Responsibilities
- 3 Training
- 4 Managing Data Access
- 5 Process Reviews
- 6 Responding to Incidents
- 7 Continuity Planning
- 8 Unsupported Systems
- 9 IT Protection
- 10 Accountable Suppliers

Progress

[Go to progress dashboard and reports](#)

39 of 43 mandatory evidence items provided

0 of 36 assertions confirmed

This is an HQ assessment. Publishing this will publish for selected branches.

[View branches](#)

[Publish Assessment](#) [View previous publications](#)

Filters

Mandatory

- Mandatory (25)
- Not Mandatory (11)

Assertion Status

- Met (22)
- Not Met (4)
- Other (10)

Confirmed

- Not Confirmed (36)

Owner

- No Owner (36)

1 Personal Confidential Data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

[Get the big picture on the data security and protection standards \(opens in a new tab\).](#)

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency

Owner:
No Owner [Assign Owner](#)

1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory
-------	--	-----------

- Do they have the same policies & procedures?
- If yes, publish one DSPT for all

Further support on publishing



DSPT
Better security.
Better care.

- [Guidance on Publishing for the first time](#)
- [Contact your Local Support Partner](#)

What next?



DSPT

Better security.
Better care.

Next steps



DSPT
Better security.
Better care.

1. Register on the DSPT
2. Contact your [Local Support Partner](#)
3. Large providers – Contact Digital Social Care help@digitalsocialcare.co.uk
4. Check out the guidance on Digital Social Care
5. Start to answer questions on DSPT now – return to it later

www.digitalsocialcare.co.uk/bettersecuritybettercare

Twitter [@DigiSocialCare](https://twitter.com/DigiSocialCare)

Useful tips



DSPT

Better security.
Better care.



DSPT
Better security.
Better care.

Tip: Export your assessment to Excel

Assessment

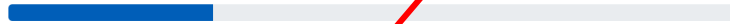
[Data Security and Protection Standards for health and care \(opens in a new tab\)](#) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

- 1 Personal confidential data
- 2 Staff responsibilities
- 3 Training
- 4 Managing data access
- 5 Process reviews
- 6 Responding to incidents
- 7 Continuity planning
- 8 Unsupported systems
- 9 IT protection
- 10 Accountable suppliers

Progress

12 of 42 mandatory evidence items provided



0 of 36 assertions confirmed



[Publish Assessment](#)

[Go to progress dashboard and reports](#)

[View previous publications](#)

Go to dashboard and reports

Assessment progress

View your organisation's progress towards meeting the National Data Guardian's 10 Data Security Standards or download a copy of your assessment.

[← Back to assessment](#)

Export assessment

You can download your assessment as a spreadsheet (.xlsx) which can then be opened in Excel. This will not include any files that have been uploaded as evidence.

[Download Assessment](#)

Tip: Save as PDF



DSPT
Better security.
Better care.

Assessment

[Data Security and Protection Standards for health and care \(opens in a new tab\)](#) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

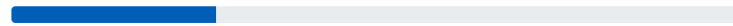
NDG Standards

- 1 Personal confidential data
- 2 Staff responsibilities
- 3 Training
- 4 Managing data access
- 5 Process reviews
- 6 Responding to incidents
- 7 Continuity planning
- 8 Unsupported systems
- 9 IT protection
- 10 Accountable suppliers

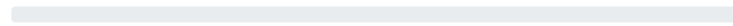
Progress

[Go to progress dashboard and reports](#)

12 of 42 mandatory evidence items provided



0 of 36 assertions confirmed



[Publish Assessment](#)

[View previous publications](#)

Go to View previous publications

Select the DSPT Assessment you want

Previous Publications

Status	Date Published	
18/19 Standards Met	14/05/2019	View Details
18/19 Entry Level	02/05/2019	View Details

Ctrl P to Print and select Save as PDF

NHS Digital [My account](#) [Logout](#)

Data Security and Protection Toolkit

This is a test site and is not intended for live use.

Care Provider Alliance
[Organisation search](#) [News](#) [Help](#)

Assessment
[Report an incident](#)
[Admin](#)

18/19 Standards Met Assessment - 14/05/2019 15:32

Destination: [Save as PDF](#)
Pages: [All](#)
Layout: [Portrait](#)
More settings: [▼](#)

Tip: Share your DSPT status



DSPT
Better security.
Better care.

- Multi sites: tell your branches
- Tell your Registered Managers
- Add your DSPT Status to your website (eg your Privacy Statement). Consider adding a link directly to the DSPT status
- Include in all your bids
- Tell your commissioners
- Tell your NHS partners
- Tell your IT suppliers

Tip: Making it real



DSPT
Better security.
Better care.

- Keep your DSPT up to date throughout the year – easier to republish
- Ensure managers and staff understand what is expected of them
- Enable managers to access the information – consider having a print out of the documents and related policies and procedures in a manual. Useful for CQC

Any final questions?



DSPT
Better security.
Better care.



Poll



DSPT
Better security.
Better care.

- What impact has this webinar had on your confidence to complete the DSPT?
- How likely is it that you will complete and publish by 30 June 2022?
- How likely is it that you will contact your Local Support Partner for help?
- Would you recommend this webinar to a colleague?

Feedback



DSPT
Better security.
Better care.

“I am glad I did attend the training. The information is both relevant and beneficial to not only me but the people we support, the staff members and our management team.”

Thank you for your support, we have just completed the toolkit. I really do appreciate your support and time.