



DSPT
Better Security.
Better Care.



Digital
Care Hub

Completing the DSPT for the first time 2025/26

Funded by



Department
of Health &
Social Care

8/6/26



The technical issues

- 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

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



Poll

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?

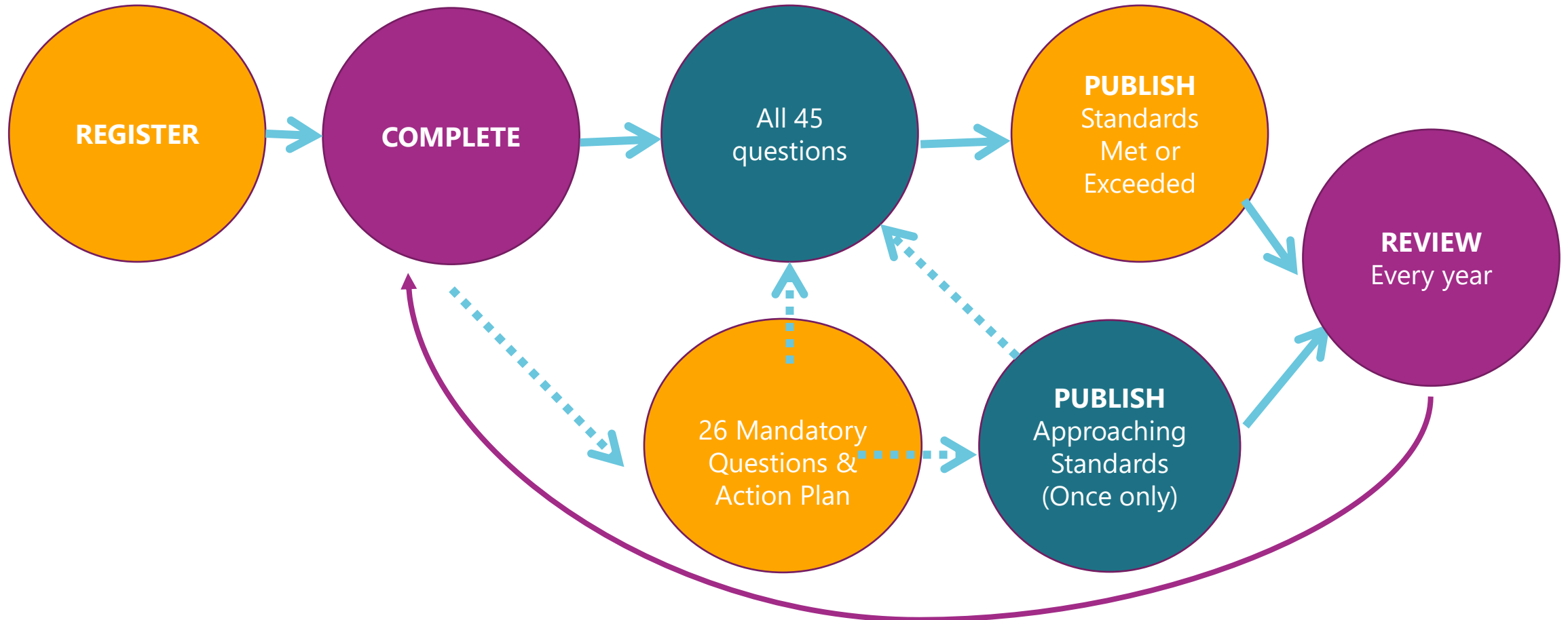


View a short video about [the DSPT on YouTube](#)

(In order to reduce the size of this file, we have removed the embedded video)



Your 'Toolkit Journey' – start now!



Detailed guidance and support

About the DSPT

Benefits and support

About

Check DSPT status

What level are you at and what does it mean?

Check status

Before you start

What to have in place the first time

Start

Review and update

What to consider and update when republishing

Review

- Free and official
- Online guidance, step by step films
- Webinars
- FAQs
- Template policies
- Helpline
- Tailored support from 32 Local Support partners across England

digitalcarehub.co.uk/dspt



CQC and DSPT

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

DSPT (or an equivalent) is now a requirement under the new Single Assessment Framework under “Well Led” Governance, management and sustainability.

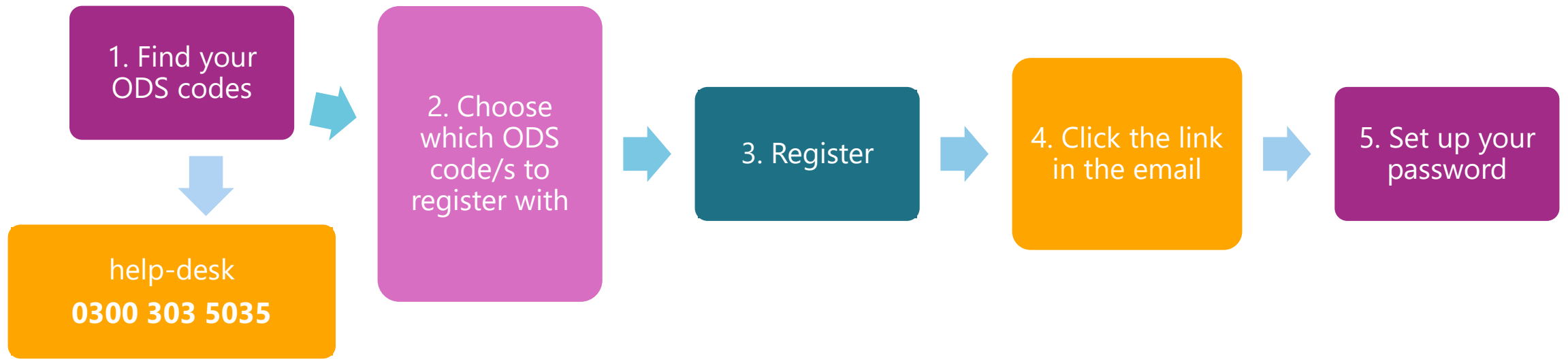
<https://www.cqc.org.uk/guidance-regulation/providers/assessment/single-assessment-framework/well-led/governance-management-sustainability>





Registering on the DSPT for the first time

How to register for the Toolkit



Find your ODS codes – what codes are there?

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



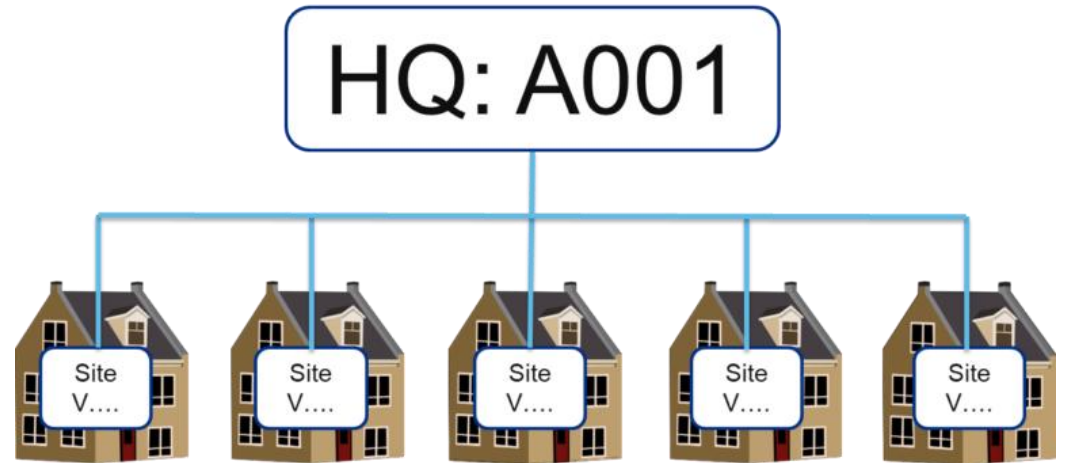
Register with your V code



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**



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

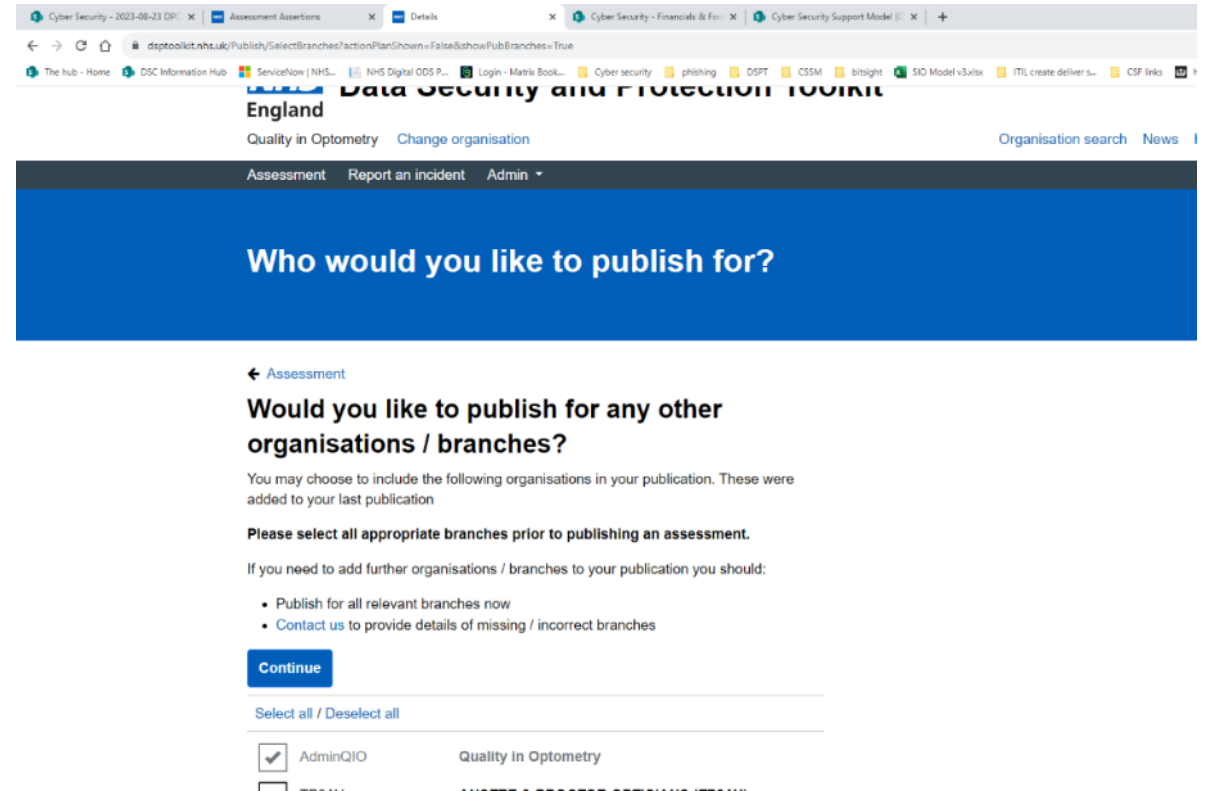


Seek advice from the helpdesk
0300 303 5035 or ssd.nationalservicedesk@nhs.net



Multi-sites

- Tick all sites you would like to publish on behalf of.
- Add your Registered Managers as viewers/auditors of your DSPT
- Revisit & republish each year & ensure all sites are ticked



The screenshot shows a web browser window with multiple tabs. The active tab is titled 'Assessment Assertions' and shows the URL 'dsptoolkit.nhs.uk/Publish/SelectBranches?actionPlanShown=False&showPubBranches=True'. The page header includes 'Data Security and Protection Toolkit England' and navigation links like 'Quality in Optometry', 'Change organisation', 'Assessment', 'Report an incident', and 'Admin'. A large blue banner asks 'Who would you like to publish for?'. Below this, a section titled 'Would you like to publish for any other organisations / branches?' provides instructions and a list of selected organisations: 'AdminQIO' and 'Quality in Optometry', both with checked checkboxes.



Find your ODS codes

- 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 helpdesk on 0300 303 5035, or email ssd.nationalservicedesk@nhs.net



DSPT – so where do I start?

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

The screenshot shows the NHS Digital Data Security and Protection Toolkit homepage. At the top left, there is a 'BETA' badge and the text 'This is a new service'. The main header features the NHS Digital logo and the title 'Data Security and Protection Toolkit'. In the top right corner, there are links for 'Register' and 'Log in', both of which are circled in red. Below the header, there are links for 'Organisation search', 'News', and 'Help', with 'Organisation search' also circled in red. A red arrow points from a text box below to the 'Organisation search' link. Another red arrow points from a text box below to the 'Register' link. The main content area has a blue background and contains the following text:

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.

Below the screenshot, there are two text boxes with arrows pointing to the website elements:

- A box on the left: 'To find out if your organisation is already registered or has published the Toolkit' with an arrow pointing to the 'Organisation search' link.
- A box on the right: 'If not, register here' with an arrow pointing to the 'Register' link.



Register and complete your organisation profile

The screenshot shows the 'Organisation Profile' page. At the top left is the NHS Digital logo with a 'Beta' badge and the text 'This is a new service - your feedback will help us to improve it.' The page title is 'Data Security and Protection Toolkit'. Below the title are navigation links: 'Assessment', 'News', 'Report an Incident', 'Help', and 'Admin'. The user's name 'Kim Hobday - ABC Surgery' is displayed, along with 'Change Organisation' and 'Log Out' buttons. The main heading is 'Organisation Profile', followed by the text 'Before starting your assessment we need to ask you some questions.' Below this, it says 'The answers you give will:' and lists three bullet points: 'tailor your assessment to your organisation's sector', 'pre-populate elements of your assessment', and 'help us to produce national reports'. A 'Continue to questions' button is at the bottom.

USEFUL LINKS

- [Guidance on Registering](#)
- [Contact your Local Support Organisation](#)

The screenshot shows the 'Which of these categories best describes your organisation?' page. At the top left is the NHS Digital logo with a 'Beta' badge and the text 'This is a new service - your feedback will help us to improve it.' The page title is 'Data Security and Protection Toolkit'. Below the title are navigation links: 'My account', 'Logout', 'Oxford Brookes University - Institute of Public Care', 'Change organisation', 'Organisation search', 'News', and 'Help'. The user's name 'Kim Hobday - ABC Surgery' is displayed, along with 'Change Organisation' and 'Log Out' buttons. The main heading is 'Which of these categories best describes your organisation?'. Below this, it says 'Choose one from the list below. Read about sectors (opens in a new tab)'. There are two columns of radio button options: 'Acute', 'Ambulance Trust', 'AQP Clinical Services', 'AQP Non-Clinical Services', 'Arms Length Body', 'CCG', 'Charity / Hospice', 'Community Services Provider', 'Company', 'CSU', 'Dentist (NHS)', 'Dentist (Private)', 'GP', 'Local Authority', 'Mental Health Trust', 'NHS Business Partner', 'NHS Digital', 'Optician', 'Pharmacy', 'Prison', 'Researcher / Department', 'Secondary Use Organisation', and 'Social Care'. The 'Social Care' option is selected, indicated by a yellow dot and a purple arrow pointing to it. A 'Save' button is at the bottom.

Choose Social Care



Setting up other users

Viewer

- View only

Member

- Add/edit evidence

Administrator

- Manage users
- Add/edit evidence
- Publish



Support on registering

Register or log in

Single or multi-site
registration - Changes to
registration

Register

USEFUL LINKS

- [Register or log in – Digital Care Hub](#)
- [Completing the DSPT - Webinar recordings - Digital Care Hub](#)
- [Local Support Organisations | Digital Care Hub](#)



Any questions?





Completing the DSPT questions

Answers are NOT public

- 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



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

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 protection, and cyber security?	Mandatory



The social care view

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



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
2.2.1	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 in the last twelve months?	
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 2022?	
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

Policies and procedures



Questions are grouped under 4 headings

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



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



What the question asks 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?



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
2.2.1	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 in the last twelve months?	
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 2022?	
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	COMPLETED
-------	--	-----------	-----------



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

Staff

1.1.5

2.1.1

2.2.1

3.1.1

3.2.1

3.4.1

4.1.1

Evidence item 4.1.1

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

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.

Comments (optional)

Save

or Cancel

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

Mandatory

Policies and procedures

1.1.1

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

Mandatory **COMPLETED**



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

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 data protection is everybody's business, there must be a named person within your organisation who takes overall senior responsibility for data security and protection issues. Their responsibility is to provide senior level leadership and guidance.

In the text box, name the person or people within your organisation with overall responsibility for data security and protection, along with their roles. 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](#) or a [Caldicott Guardian](#).

You can read more about data security and protection responsibilities and specialised roles on the [Digital Social Care Website](#).

Comments (optional)

[Save](#) or [Cancel](#)

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



Awareness training

- 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, in the last 12 months?



Free e-learning course for all staff working in adult social care services in England

- Easily accessible
- 15-20 min per module
- Relatable case scenario-based
- learning for all staff.
- Free
- Compliant with question 3.2.1 on data protection training of staff.
- [eLearning Courses - Digital Care Hub](#)

Module 1: Data protection rights and responsibilities

My responsibilities • People's rights

[View resource](#)

Module 2: Keeping data secure

Sharing confidential data • Recording and disposing of data

[View resource](#)

Module 3: Threats to data security

Fraud and scams • Safe use of digital devices • Safe keeping of paper records

[View resource](#)

Module 4: Data breaches

What is a data breach? • Data confidentiality • Availability of data • Data integrity • Receiving data in error

[View resource](#)



e-learning course for data leads working in adult social care services in England

- Easily accessible
- 15-20 min per module
- Relatable case scenario-based
- Tailored learning for those leading on data protection and cyber security
- Free
- [Complete the training here](#)

Guide to completing the course

How to navigate the course

User guide

Content and learning outcomes

Overview of all the modules

Overview

Copyright

Copyright and background

Background

Videos

Summary videos from all modules

Summary videos



Managers' Discussion Tool & Quiz for Staff

Better Security, Better Care Managers' discussion tool

Version 3 – September 2023

This discussion tool is designed to help you have discussions with your frontline staff to check their knowledge and provide evidence of their competence in data security and protection to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#).

The tool is broken down into four colour coded sections covering the four learning outcomes for frontline social care staff:

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle data safely
2. Be able to apply relevant data security and protection legislation and principles
3. Be aware of physical and digital threats to data security and know how to avoid them, including:
 - i. being alert to social engineering
 - ii. safe use of digital devices
 - iii. safe keeping of physical records
4. Be able to identify data breaches and incidents and know what to do if one happens

Better Security, Better Care Multiple choice quiz for frontline staff

Version 3 – September 2023

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the [Data Security and Protection Toolkit](#). Circle or tick the correct answers.

Name: _____ Date: _____ Score: _____

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle personal data safely

Question	Answer options
1a True or False: We have a legal duty to respect the privacy of the people who use our care services?	True False
1b True or False: Sharing information with the right people can be just as important as not disclosing to the wrong person?	True False
1c Can someone you support ask to see and have a copy of the personal data that is held about them?	Yes No
1d When you collect someone's personal details, should you tell them what will happen to that information and who it will be shared with?	Yes No



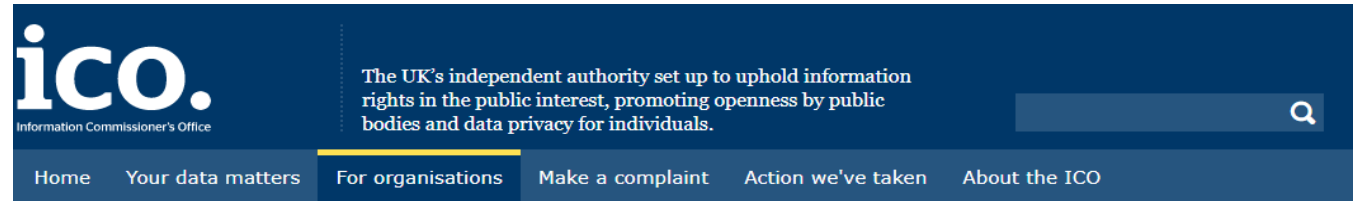
2. Policies and procedures

What the questions cover

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



ICO registration



The header of the ICO website features the logo on the left, a mission statement in the center, and a search bar on the right. Below this is a navigation menu with several options.

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.

Every organisation or sole trader who processes personal information needs to pay a data protection fee to the ICO, unless they are exempt.

Further reading

 [Search the register](#)
About the ICO

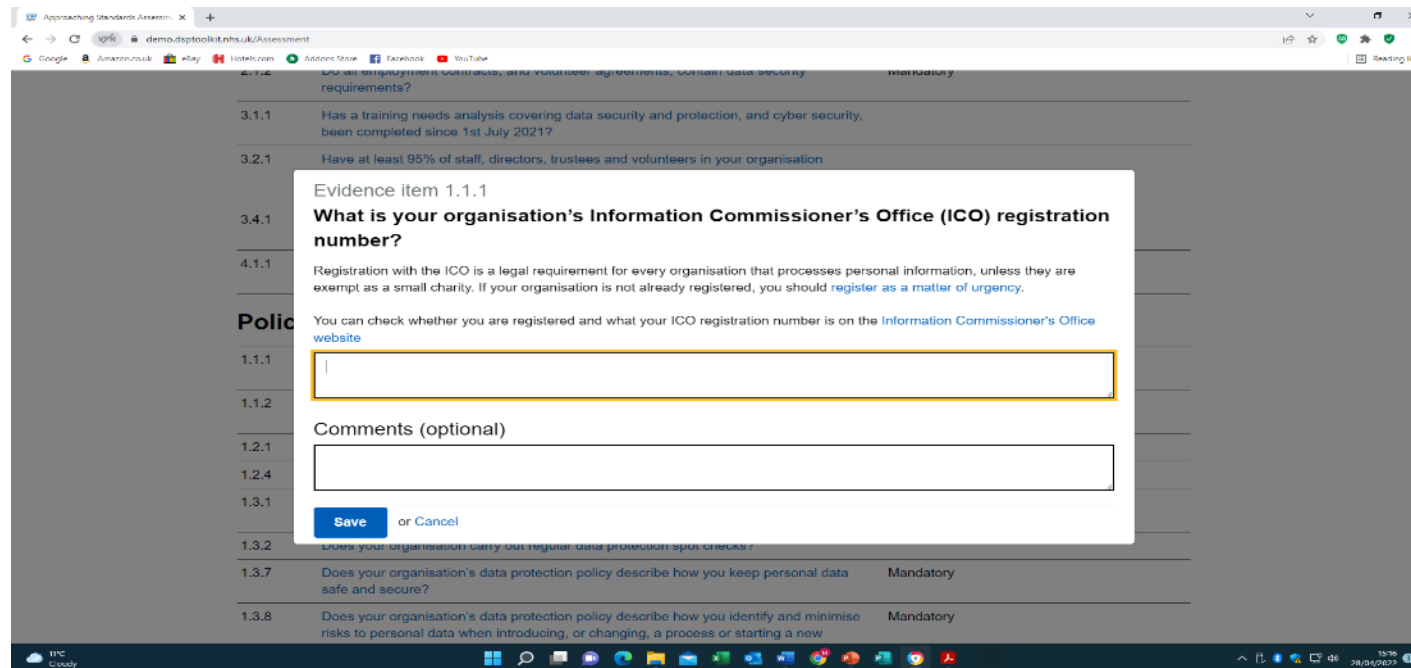
 [Legal definitions](#)
For organisations

 [Guide to the data protection fee](#)
For organisations



What the question asks – 1.1.1

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



The screenshot shows a web browser window displaying an assessment tool. A modal window is open over the assessment content, titled "Evidence item 1.1.1". The question text is: "What is your organisation's Information Commissioner's Office (ICO) registration number?". Below the question, there is a text box for the answer, a "Comments (optional)" section with another text box, and "Save" and "Cancel" buttons. The background assessment content is partially visible, showing a list of questions with their IDs and descriptions.

Evidence item 1.1.1
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](#).

1.1.1

Comments (optional)

[Save](#) or [Cancel](#)



Response to the Question 1.1.1

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.

Further support: template policies (Be sure to tailor to your service)

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

[Find all template policies to download and reuse on the Digital Care Hub website here](#)

Standards Met: Additional required policies

- Training Needs Analysis
- Data Security Audit Checklist
- Creating and Testing a Business Continuity Plan for Data and Cyber Security
- National Data Opt Out

Recommended documentation

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



3. Data security - What the questions cover

- 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

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



Multi-factor Authentication (MFA)

4.5.3:

“Multi-factor authentication (MFA) is one of the most effective ways to protect data and accounts from unauthorised access.

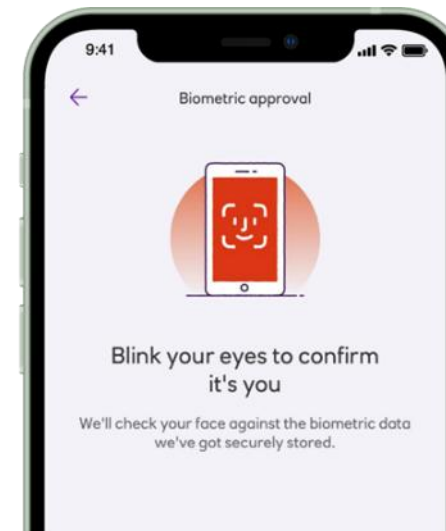
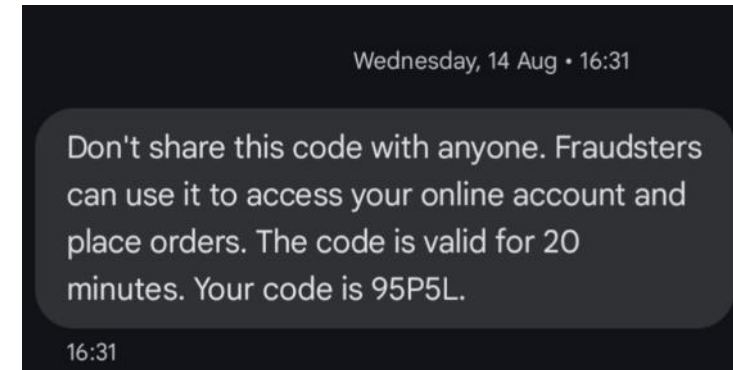
You should consider all systems that can be accessed from the internet – such as email, your digital social care record, and any cloud-based or online systems – and either ensure that all user accounts are protected with MFA, or detail any exceptions in the text box response.

[Guidance on implementing MFA](#) can be found on Digital Care Hub, further information and guidance is also being developed by Digital Care Hub.”



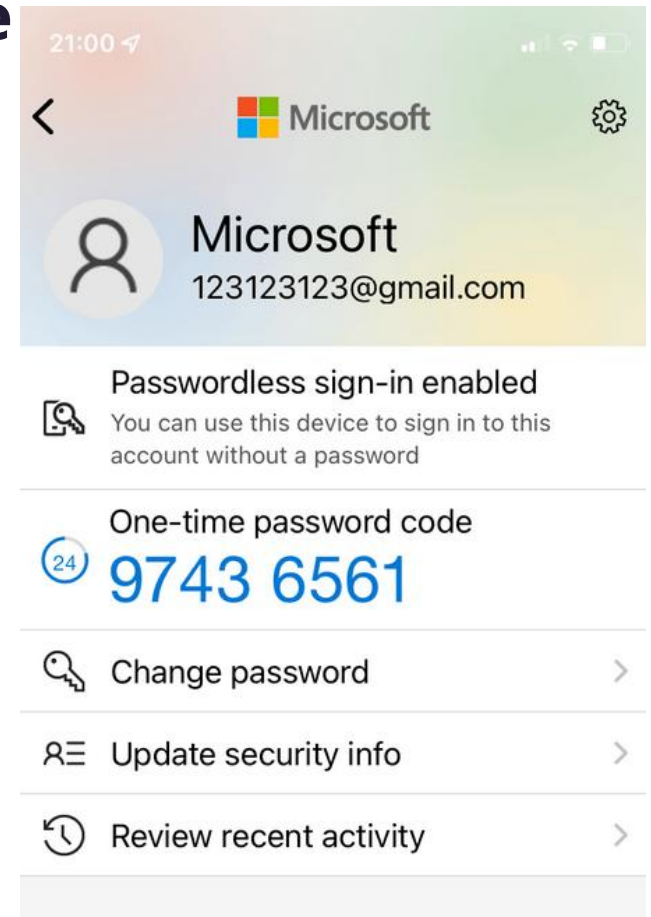
Multi-factor Authentication (MFA)

- Multi-factor authentication (MFA) is a way to make your online accounts much safer by adding extra steps to prove it's really you trying to log in.
- Usually this is a text message, email code, fingerprint or authenticator app e.g. Microsoft.
- You've probably done this when online banking or logging into social media
- Ensures we keep us all safe by only allowing people to have access who *should* have access.



Multi-factor Authentication (MFA): steps to take

- Review your current systems & speak with suppliers
- Identify any potential issues e.g. staff sharing devices or logins
- Identify where implementing MFA might not be appropriate (e.g. if there are already other significant controls in place)
- Decide on your organisations balance of security vs. useability
- Note any systems without MFA at a director or board level & why



Multi-factor Authentication (MFA): security vs usability

- Important not to go overboard – systems must be useable. Adding too many layers means people either stop using existing systems or find workarounds.
- Identify the appropriate level of security for each system you use based on the sensitivity of information, the usability and your appetite for risk as an organisation.
- Where appropriate, MFA should be implemented for all individual logins to systems.
- Use the support available: Local Support Organisations, software suppliers, IT supplier



Further guidance: Digital Care Hub

Online guidance

Answer DSPT questions

Staffing & roles - Policies &
Procedures - Data Security - IT
Systems & Devices

Questions

Actions

- Contact your [Local Support Organisations | Digital Care Hub](#)
- Visit [Digital Care Hub website](#) – view guidance, register for free updates





Publish your DSPT Assessment

Publish at Approaching Standards – 26 mandatory questions answered

- If the 26 'mandatory' questions have been completed, but other questions remain not completed, you can publish at Approaching Standards

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 doing so and a summary of the action your organisation is taking to minimise the risk.	
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory COMPLETED
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	<u>Do your organisation's IT system suppliers have cyber security certification?</u>	

Publish Approaching Standards Assessment

- You will need to complete an action plan to show how you will complete the rest of the questions

The screenshot shows the NHS Data Security and Protection Toolkit interface. At the top, there is a beta notice: "BETA This is a new version - your feedback will help us to improve it". Below this, the header includes the NHS Digital logo and navigation links for "My account" and "Logout". A secondary navigation bar contains "December Social care test", "Change organisation", "Organisation search", "News", and "Help". The main content area is titled "Assessment" and "Provide an action plan". A message reads: "Thank you for responding to all the mandatory requirements". Below this, there are three bullet points: "You should now download a blank action plan template, which lists the requirements you have not yet responded to.", "You should then complete this plan and upload a copy here, as proof you are approaching the Data Security and Protection Toolkit standard.", and "You will then be able to publish your 'Approaching Standards' assessment." There is an "Upload file" section with a dashed box for the file and a "Publish Approaching Standards Assessment" button at the bottom.



Publish at Standards Met - all questions answered

- If you have answered all 45 questions, click on publish assessment to publish at Standards Met
- **Remember:** your DSPT status will be published. NOT your answers



data and information		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory COMPLETED
7.3.4	Are backups routinely tested to make sure that data and information can be restored?	COMPLETED
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?	COMPLETED
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 doing so and a summary of the action your organisation is taking to minimise the risk.	COMPLETED
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory COMPLETED
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?	COMPLETED
9.5.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	COMPLETED
10.2.1	Do your organisation's IT system suppliers have cyber security certification?	COMPLETED

Publish Assessment



There is a problem!

Social Care Assessment

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

There is a problem

[Please complete mandatory requirement 7.3.2 in the IT Systems and devices section](#)

[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

Staffing and roles



Headquarters Assessment – publish for all sites

Assessment Report an incident Admin

Complete your headquarters assessment for 2022-23 (v5)

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, will demonstrate that your organisation is working towards or meeting the NDG standards.

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

[View branches](#)

Progress

14 of 42 mandatory evidence items provided

[View previous publications](#)

- For those using an HQ code, you can view your branches here
- Do they have the same policies & procedures, IT systems and data security arrangements?
- If yes, publish one DSPT for all sites



Further support on publishing

Publish or republish, and share

For the first time or republish and share

Publish

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



Tip: Once published, export your assessment to Excel

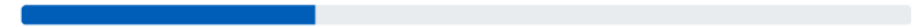
Click on download



The Excel file will download into your device straight away

Progress

14 of 42 mandatory evidence items provided



[View previous publications](#)

[Download assessment](#)

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	COMPLETED
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory	
2.2.1	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 in the last twelve months?	Mandatory	



Tip: Save your published DSPT as a PDF

Click on View Details to save as a PDF



[← Back to assessment](#)

Previous Publications

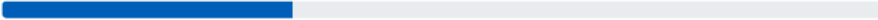
Status	Date Published	
21/22 Standards Met	10/05/2022	View Details Download Certificate



If you have published at Standards Met you can download a certificate

Progress

14 of 42 mandatory evidence items provided



[View previous publications](#)

[Download assessment](#)

Go to View previous publications

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	COMPLETED
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory	
2.2.1	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 in the last twelve months?	Mandatory	



Tip: Save your published DSPT as a PDF

Ctrl + P
to Save as PDF

The screenshot shows a web page for a 'Data Security and Protection Toolkit' assessment. The page includes a 'TEST' label, a feedback message, the NHS Digital logo, and navigation links like 'My account' and 'Logout'. The main content is a blue box with the text: '21/22 Standards Met Assessment', '10 May 2022 15:14', 'Published by: Daniel OShaughnessy', and 'Published as: Test Care Home (test123)'. A 'Back to publications' link is at the bottom. On the right, a print dialog box is open, showing options for destination (Save to PDF), orientation (Portrait/Landscape), pages (All), colour mode, paper size (A4), scale (Fit to page width), and pages per sheet (1). The 'Save' button is highlighted with a red arrow.

Click on save



Tip: Once published, share your DSPT status

- Multi sites: tell your branches, tell your Registered Managers
- Download a certificate to prove your DSPT status
- Add your DSPT Status to your website (eg your Privacy Statement)
- Include in all your bids
- Tell your commissioners
- Tell your NHS partners
- Tell your IT suppliers



Tip: Making it real

- 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



Next steps

1. Register on the DSPT
2. Contact your [Local Support Organisations](#) or the Digital Care Hub helpline help@digitalcarehub.co.uk Tel [0808 196 4848](tel:08081964848)
3. Large providers – Contact Digital Care Hub caregroups@digitalcarehub.co.uk
4. Check out the [guidance on Digital Care Hub](#)
5. Start to answer questions on DSPT now – return to it later

<http://www.digitalcarehub.co.uk/dspt>



Any questions?



Poll

- What impact has this webinar had on your confidence to complete the DSPT?
- How likely is it that you will complete and publish in the next three months?
- How likely is it that you will contact your Local Support Partner for help?
- Would you recommend this webinar to a colleague?
- Where have you heard about this webinar?





Thank you.