DSPT
Better Security.
Better Care.

Digital
Care Hub

Review and Republish your Data Security and Protection Toolkit

Alan Wilmott
Sussex Digital In Reach Team
On behalf of the Better Security,
Better Care Programme

The technical issues

- **This is for** care providers who have already published their 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 presentation (inc links)

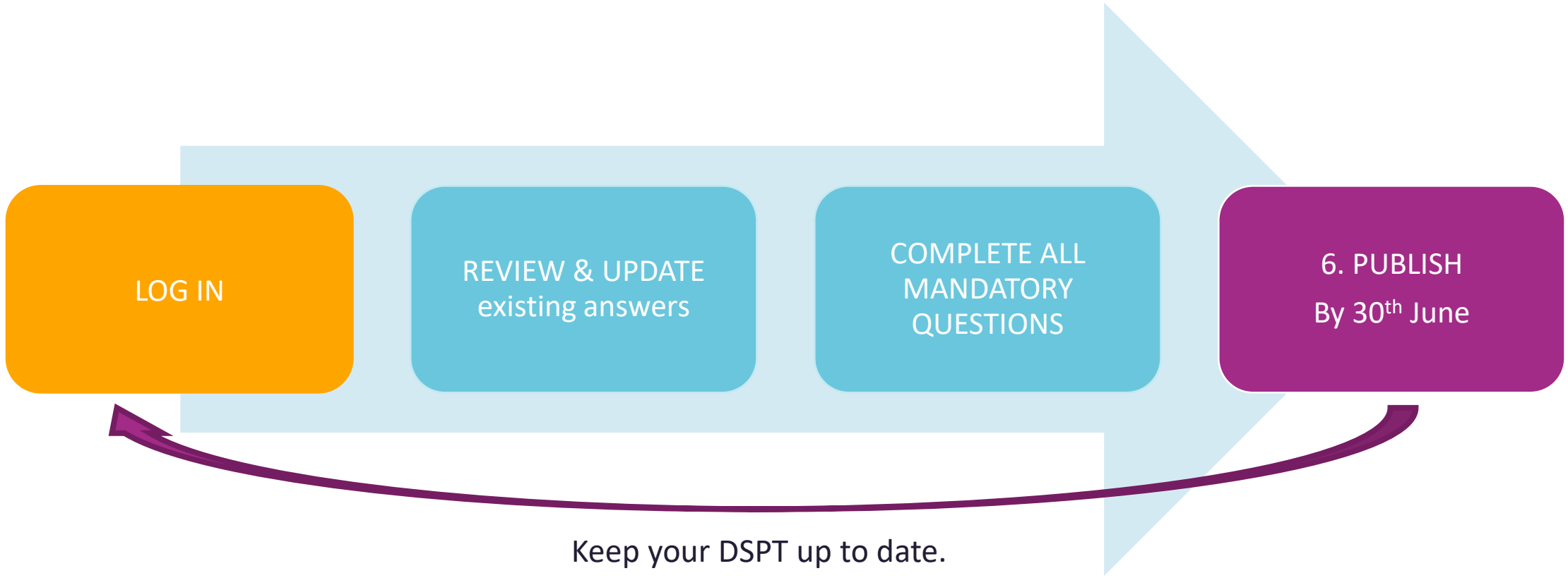
Poll for care providers only

- What level is your organisation currently at on the DSPT?
- Have you personally used the DSPT before?
- Are you a single-site or a multi-site organisation?
- Where did you hear about this DSPT webinar?

Today – our agenda

- Logging in to your DSPT
- Reviewing your DSPT
- What's changed
- Republishing your DSPT
- Tips
- Support available
- Your questions
- Next steps

Your DSPT journey: You're more than halfway there!



Your fellow travellers: Better Security, Better Care

- ✓ 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/bettersecuritybettercare

Log in to your DSPT

LOG IN

Go to www.dsptoolkit.nhs.uk Login with your email & password

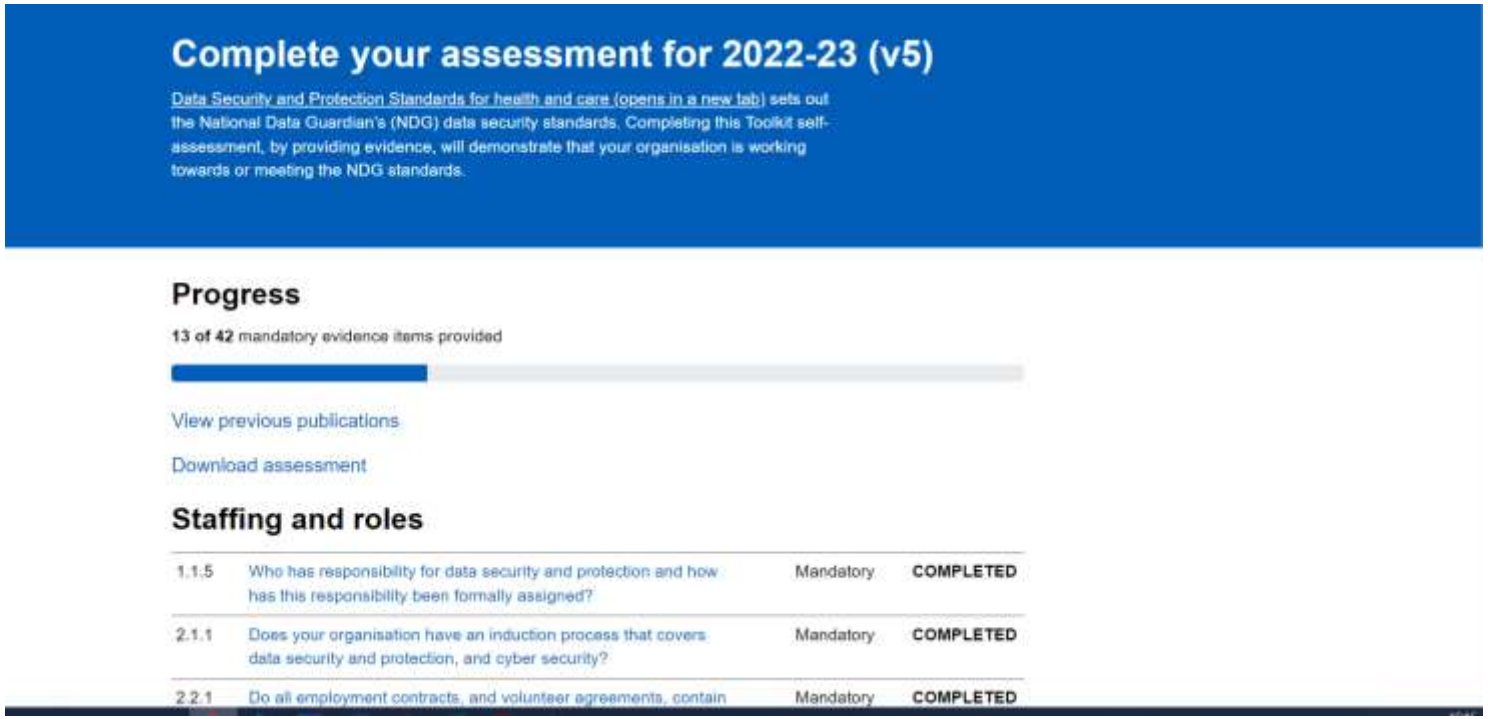
Any log in problems:

Contact DSPT helpdesk 0300 303 5035 ssd.nationalservicedesk@nhs.net

Log in

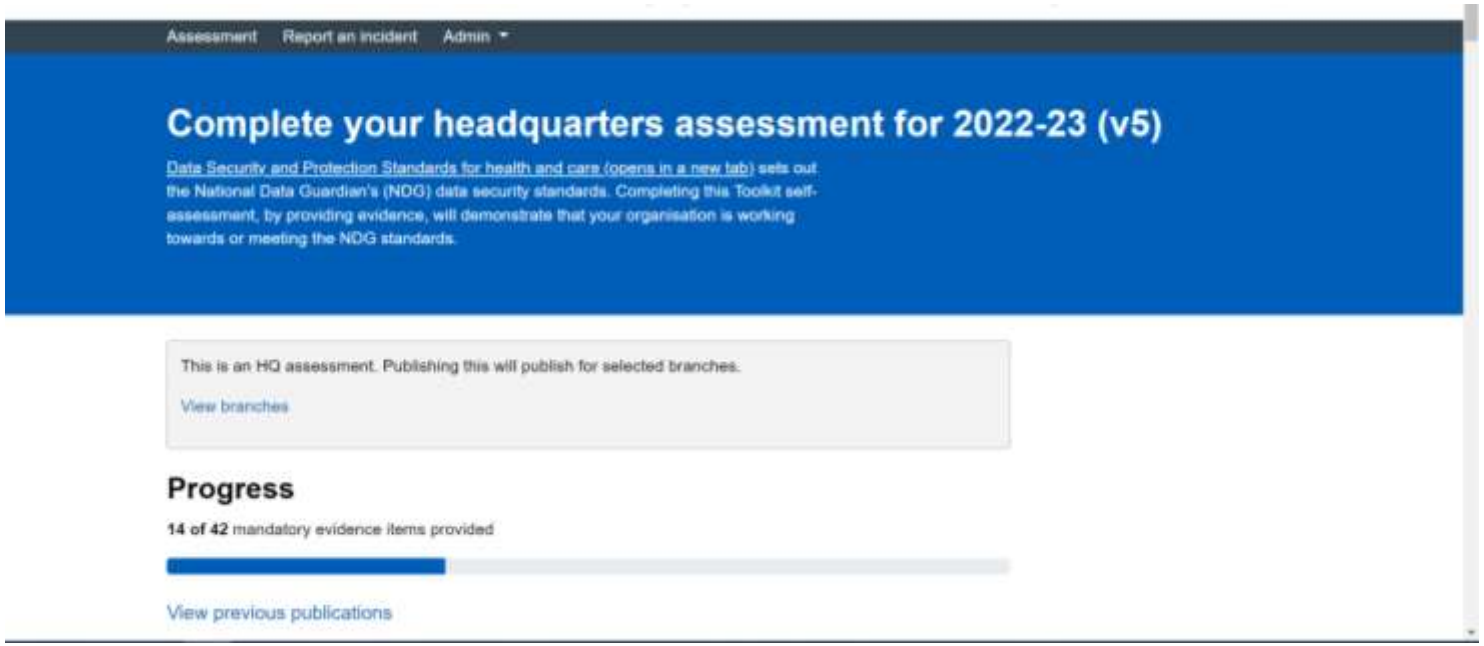
dsptoolkit.nhs.uk

What you will see



- 45 mandatory questions
- Questions grouped into 4 sections
- This is what a single site assessment view looks like for those using an ODS Code V Code

Headquarters Assessment view – for those using an HQ Code



- For those using an HQ code, the screen has a different heading
- You can view your branches here
- When you publish you can choose which of your sites you are publishing for as multisite providers can publish one DSPT that covers all their locations/branches

What you need to do will depend on what you did before

Previously published level	Action
Approaching Standards	Review and update existing answers Complete all remaining Mandatory questions to reach Standards Met. You cannot publish at Approaching Standards again
Standards Met	Review and update existing answers
Standards Exceeded	Review and update existing answers

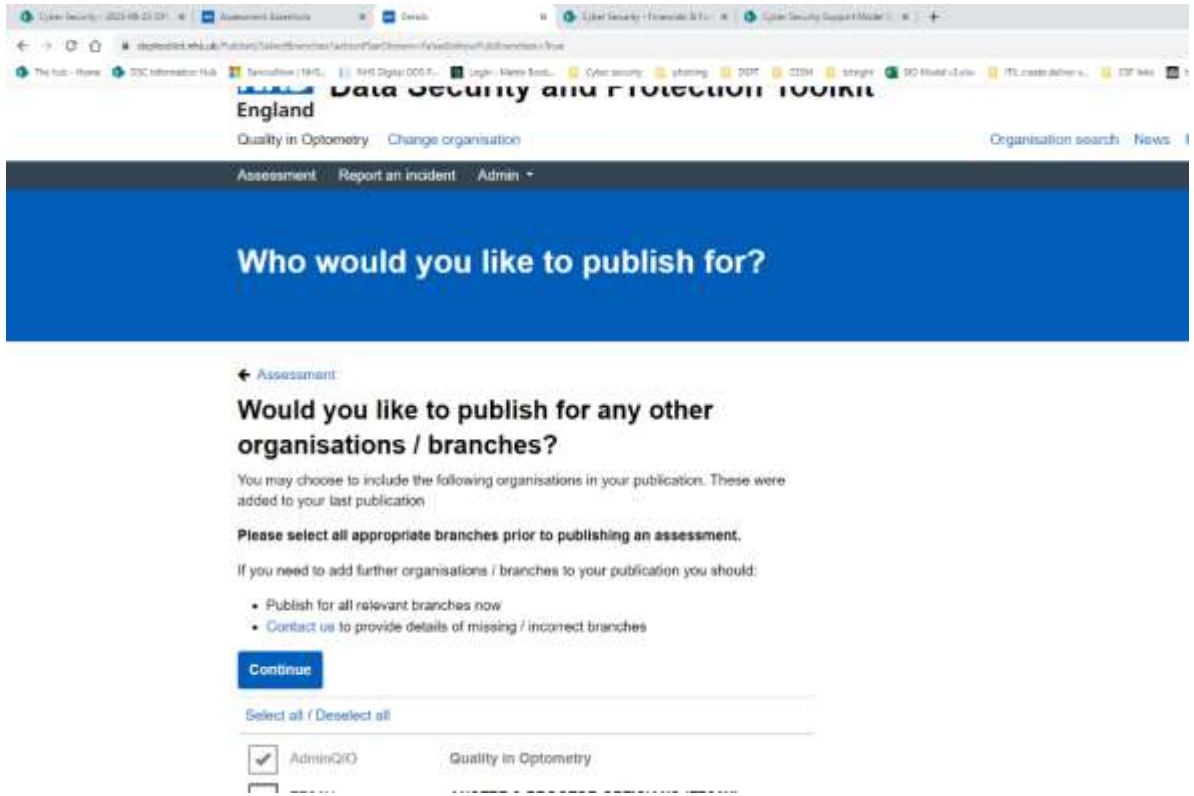
Review, update and answer questions

- Your previous answers are still there
- It may look different to what you have seen before. **DON'T PANIC!**
- The assessment view includes ALL DSPT questions
- **ONLY NEED TO ANSWER THE MANDATORY ONES**

Changes to the DSPT

Multi-site publishing (23-24 Changes)

- Addition of a screen when publishing; displayed to organisations not flagged as a HQ but previously published on behalf of other sites in their last publication.
- The existing functionality with HQ and sites is unchanged.
- When a non HQ organisation, that had sites added to their last publication selects “publish assessment” the additional screen below will be displayed.



New mandatory question: Multi-factor Authentication (MFA)

- 4.5.3:

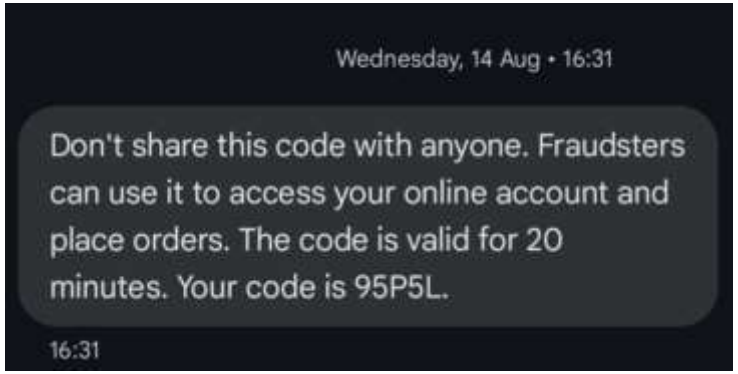
“Multi-factor authentication (MFA) is one of the most effective ways to protect data and accounts from unauthorised access.

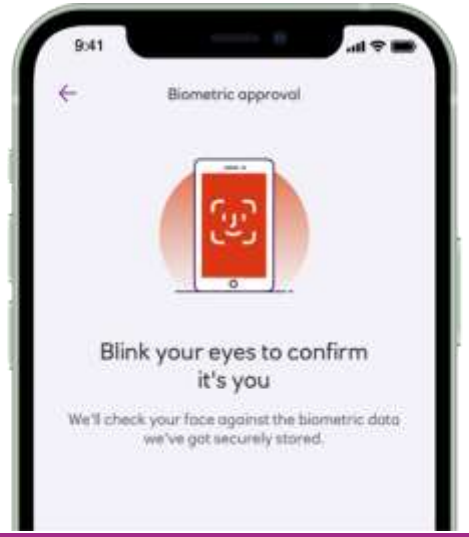
You should consider all systems that can be accessed from the internet – such as email, your digital social care record, and any cloud-based or online systems – and either ensure that all user accounts are protected with MFA, or detail any exceptions in the text box response.

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

New mandatory question: 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

New Mandatory Question 2025-26

- **4.3.1**

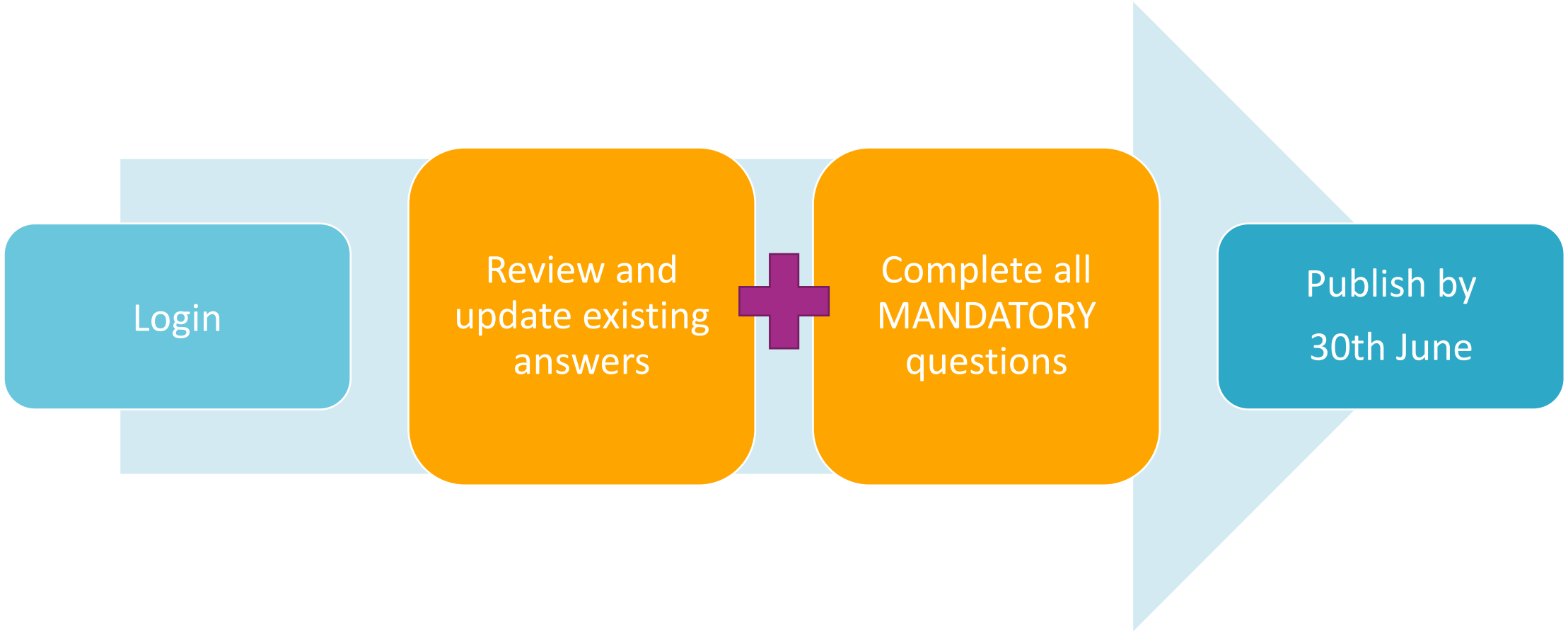
Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?

- **7.1.1**

You have an asset register detailing your organisation's hardware, software and data, which is kept up to date.

Republishing your DSPT

Review, update and complete MANDATORY QUESTIONS



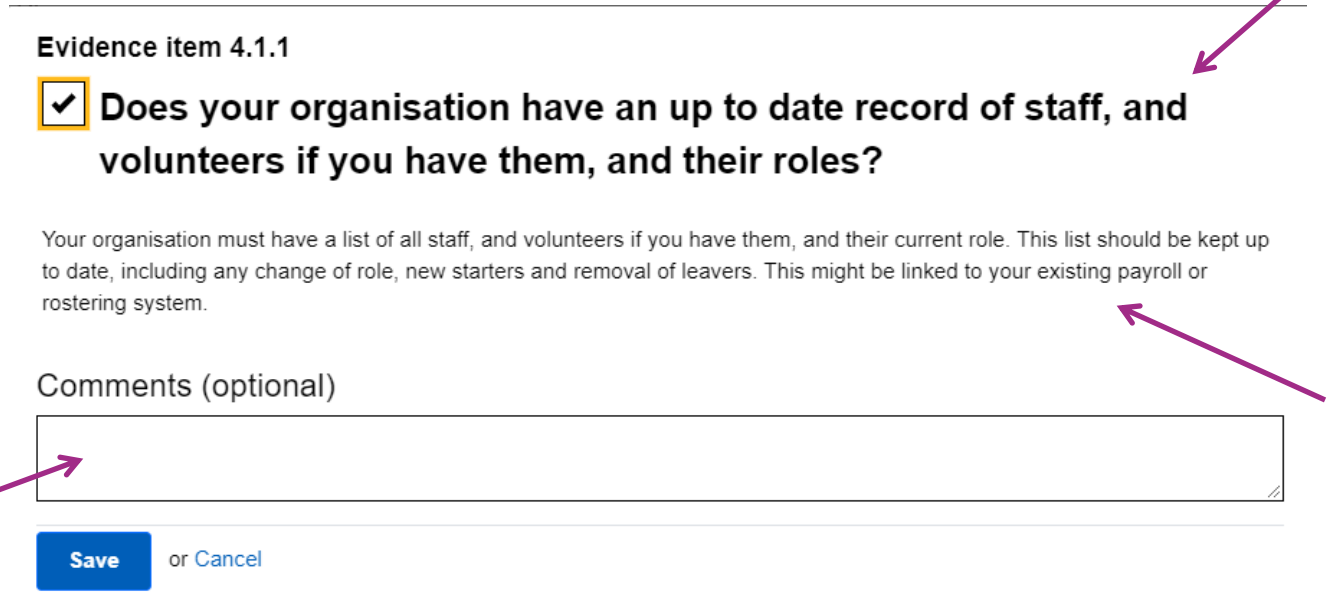
Review and update existing answers

- Only answer questions marked **MANDATORY**
- You may leave all other questions blank
- Click on an evidence item (in blue) to answer the question and see the tool tip
- Review and update existing answers

2.2.1	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory	COMPLETED
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed in the last twelve months?	Mandatory	COMPLETED
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 twelve months?	Mandatory	COMPLETED
3.3.1	Provide details of any specialist data security and protection training undertaken.		
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?	Mandatory	COMPLETED
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory	COMPLETED

Example question 4.1.1

Question



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

Comments are VERY useful especially for your colleagues & future publication

Example Response to Question 4.1.1

4.1.1

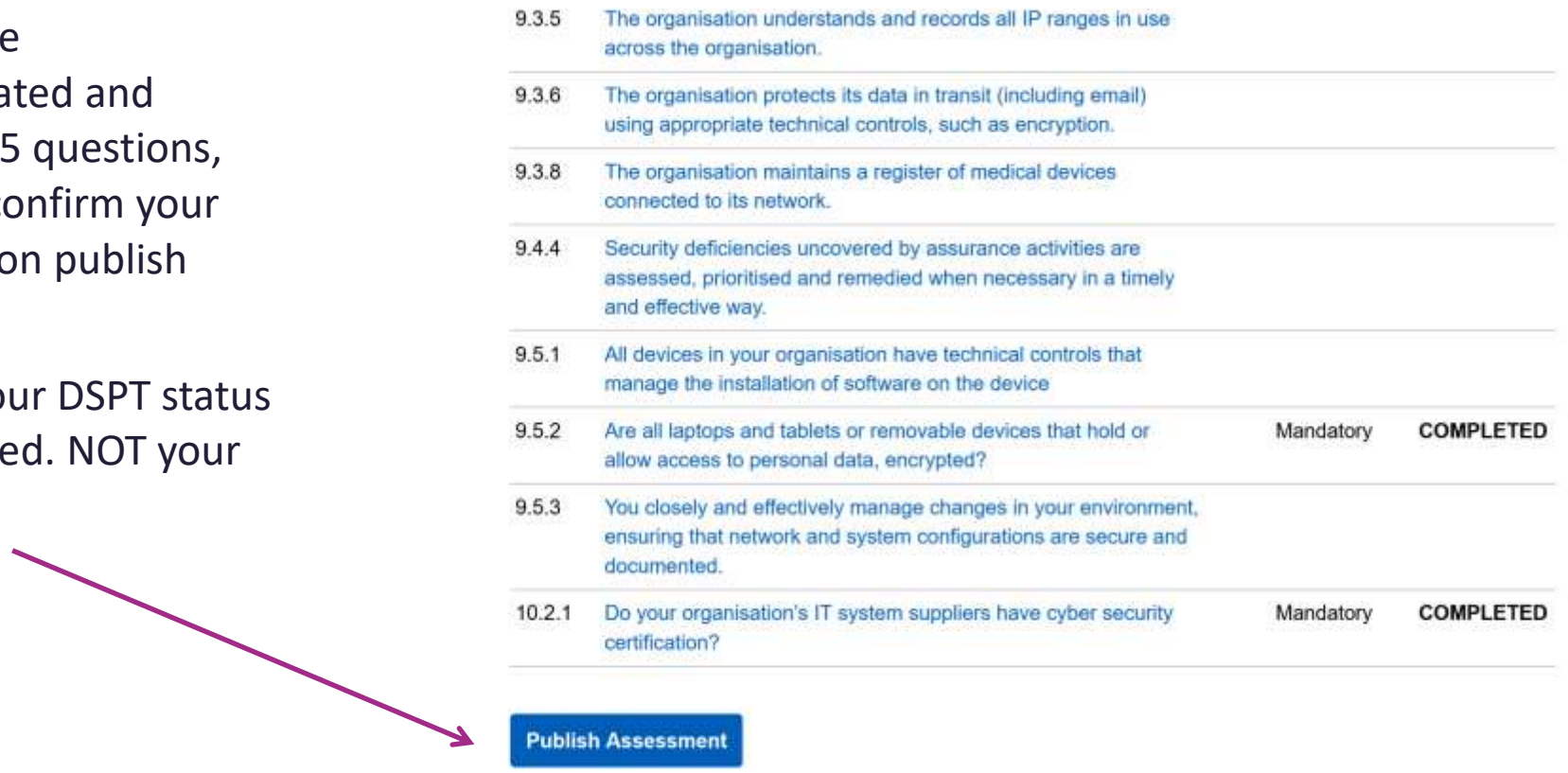
Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?

> 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.

Publish your DSPT status

Publish your updated DSPT status

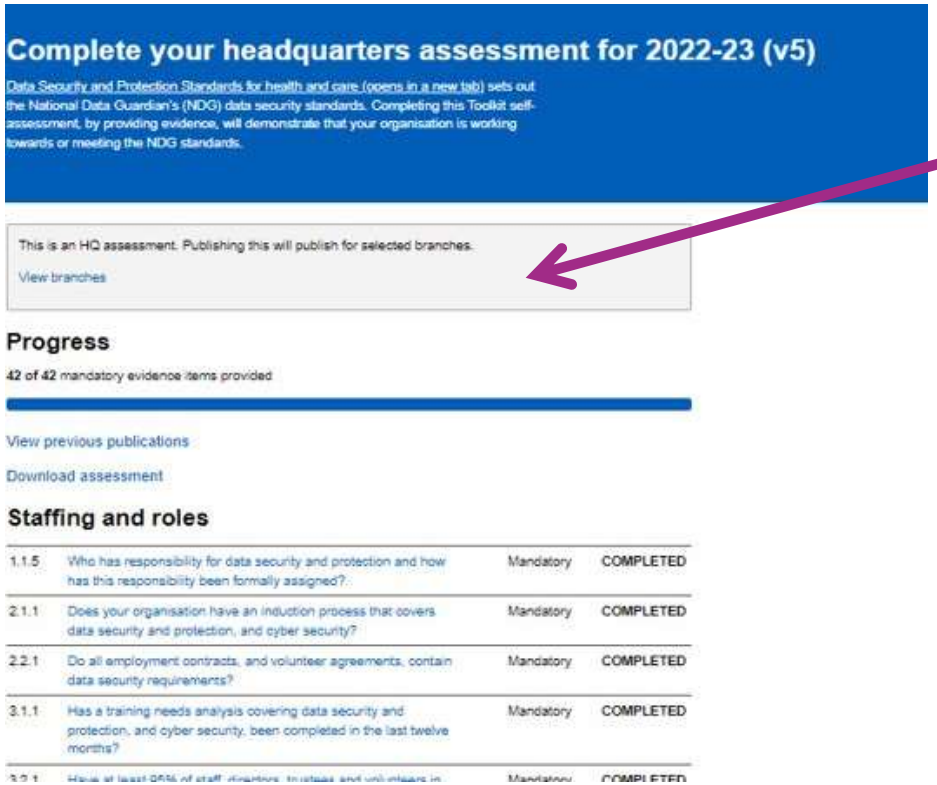
- When you have reviewed/updated and answered all 45 questions, and ticked to confirm your answers, click on publish assessment
- **Remember:** your DSPT status will be published. NOT your full report



9.3.5	The organisation understands and records all IP ranges in use across the organisation.		
9.3.6	The organisation protects its data in transit (including email) using appropriate technical controls, such as encryption.		
9.3.8	The organisation maintains a register of medical devices connected to its network.		
9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		
9.5.1	All devices in your organisation have technical controls that manage the installation of software on the device		
9.5.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	Mandatory	COMPLETED
9.5.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.		
10.2.1	Do your organisation's IT system suppliers have cyber security certification?	Mandatory	COMPLETED

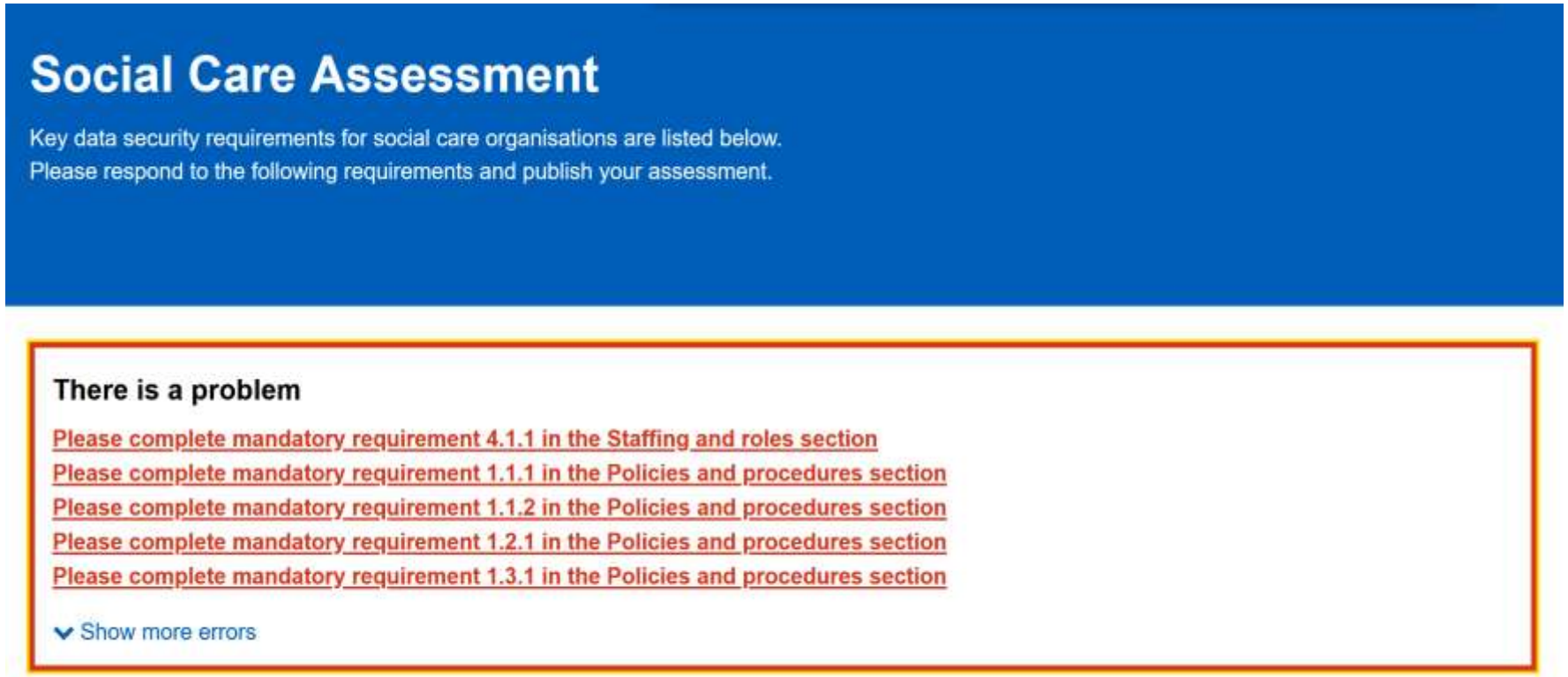
Publish Assessment

Headquarters Assessment Publish for all sites



- 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

Trying to Publish when not completed



Publication Notification

08/11/2021, 11:08 Liverpool Social Care Partnership Mail - Confirmation of the publication of your assessment

Gmail

Confirmation of the publication of your assessment

donotreply.dspt@nhs.net <donotreply.dspt@nhs.net> 8 November 2021 at 11:03

Thank you for publishing your 21/22 Standards Met Data Security and Protection Toolkit assessment for LIVERPOOL SOCIAL CARE PARTNERSHIP on 08/11/2021 11:03.

Everyone who uses health and care services should be able to trust that their personal confidential data is protected. Publishing your Data Security and Protection Toolkit provides assurance that your organisation is practising good data security and that personal information is handled correctly.

Your DSP Toolkit status of Standards Met is publicly available for your service users, commissioners, partner organisations and the public at https://www.dsptoolkit.nhs.uk/OrganisationSearch/J1V0S

Thanks

DSPT Toolkit team.

Please do not reply to this email as it has been generated automatically by the Data Security and Protection Toolkit.

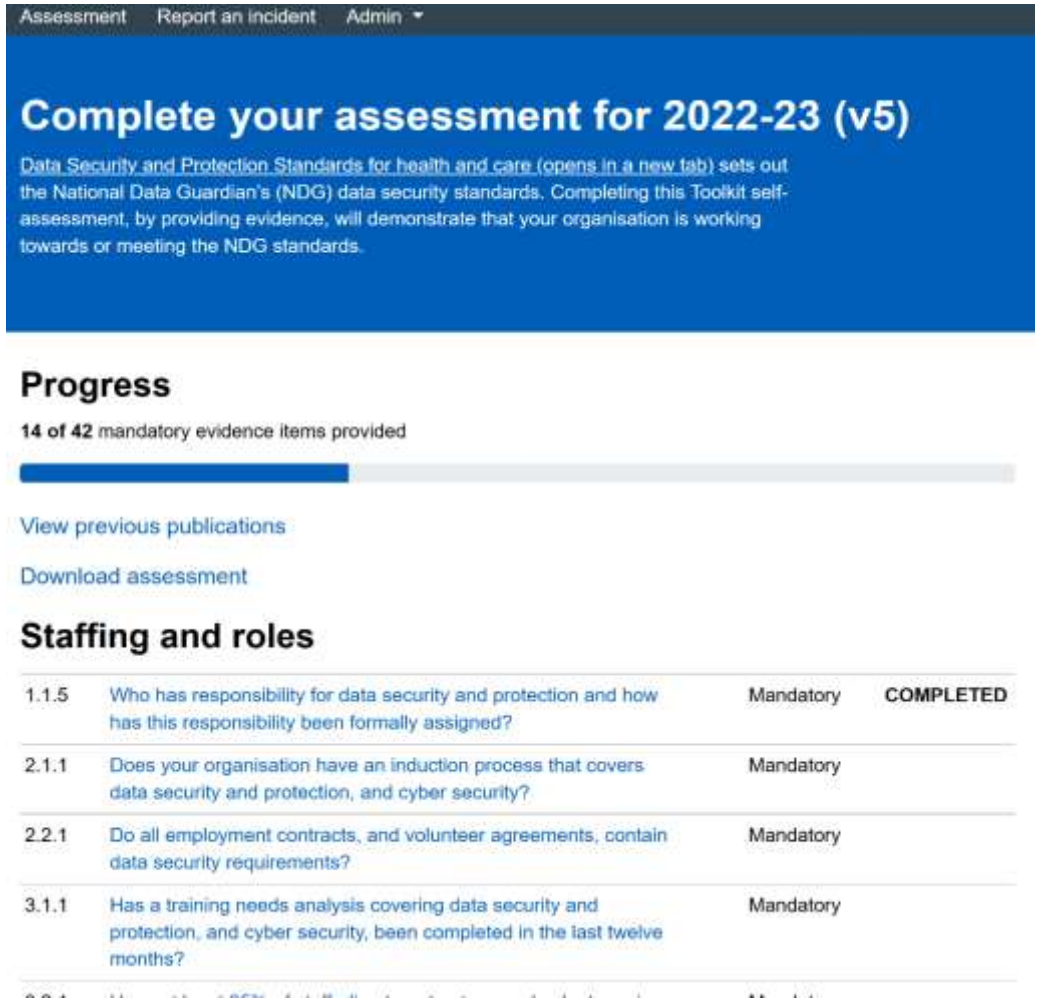
Useful Tips

Tip: Set up other users

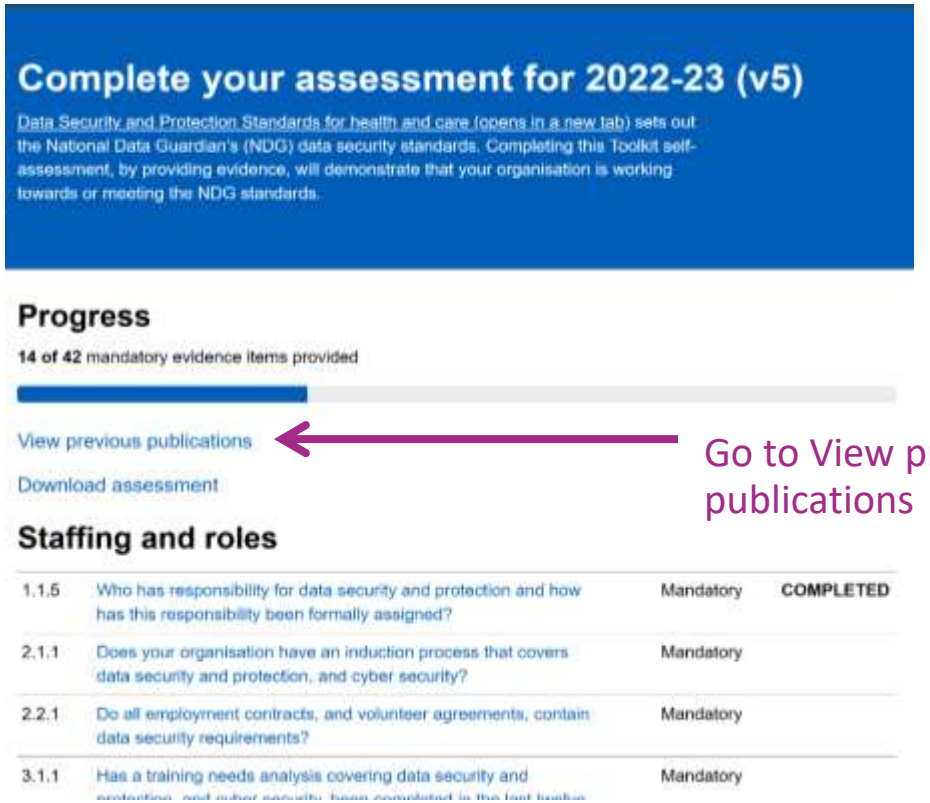
Tip:
Export your assessment to Excel

Click on download

The Excel file will download into your device straight away



Tip: Save your published DSPT as a PDF



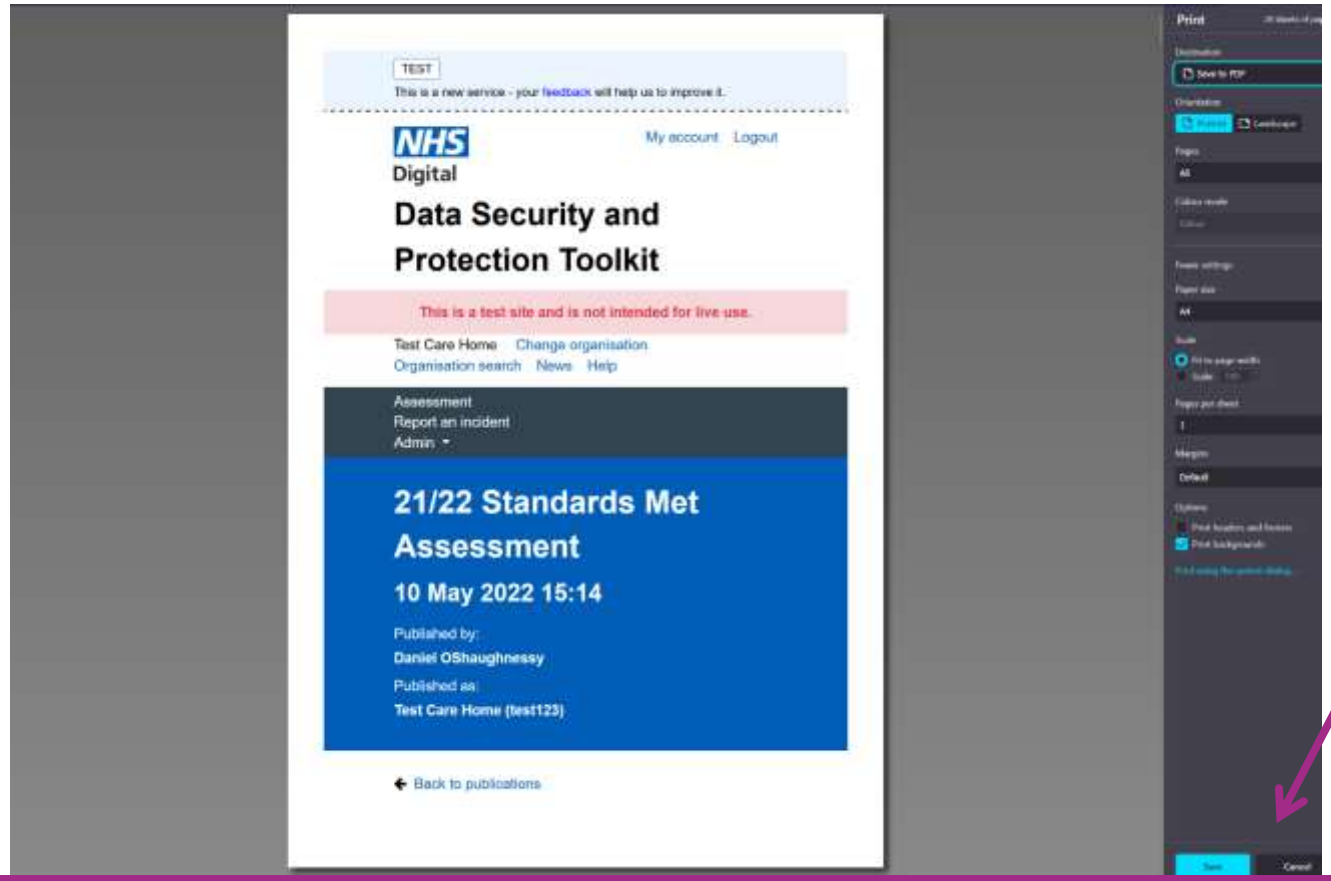
Go to View previous publications

Click on View Details to save as a PDF

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

Tip: Save your published DSPT as a PDF

Ctrl + P
to Save as PDF



Click on save

Tip: Make the most of your DSPT

- Multi-sites: tell your branches
- Tell your registered managers
- Download a certificate to prove your DSPT status
- Add your DSPT status to your website (e.g. your privacy statement). Consider adding a link directly to the DSPT status. Include in all your bids
- Tell your commissioners – including ICSs
- 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.

Free, expert support from
Better Security, Better care

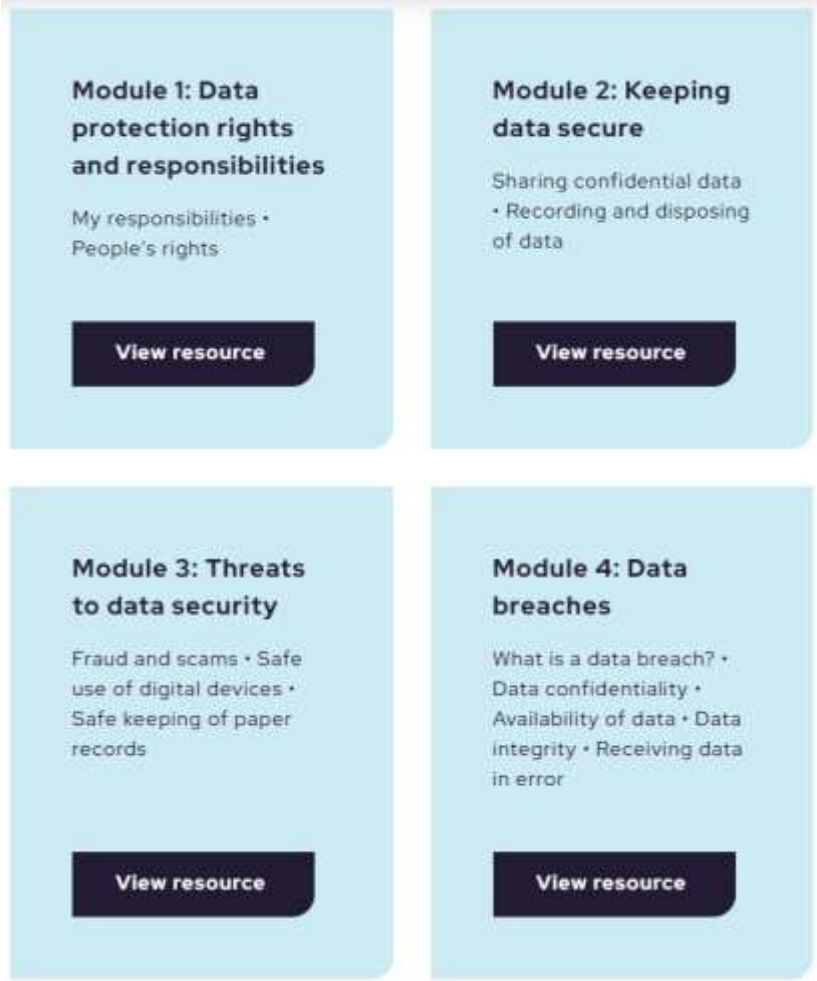
Full programme of support

- ✓ 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/bettersecuritybettercare

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

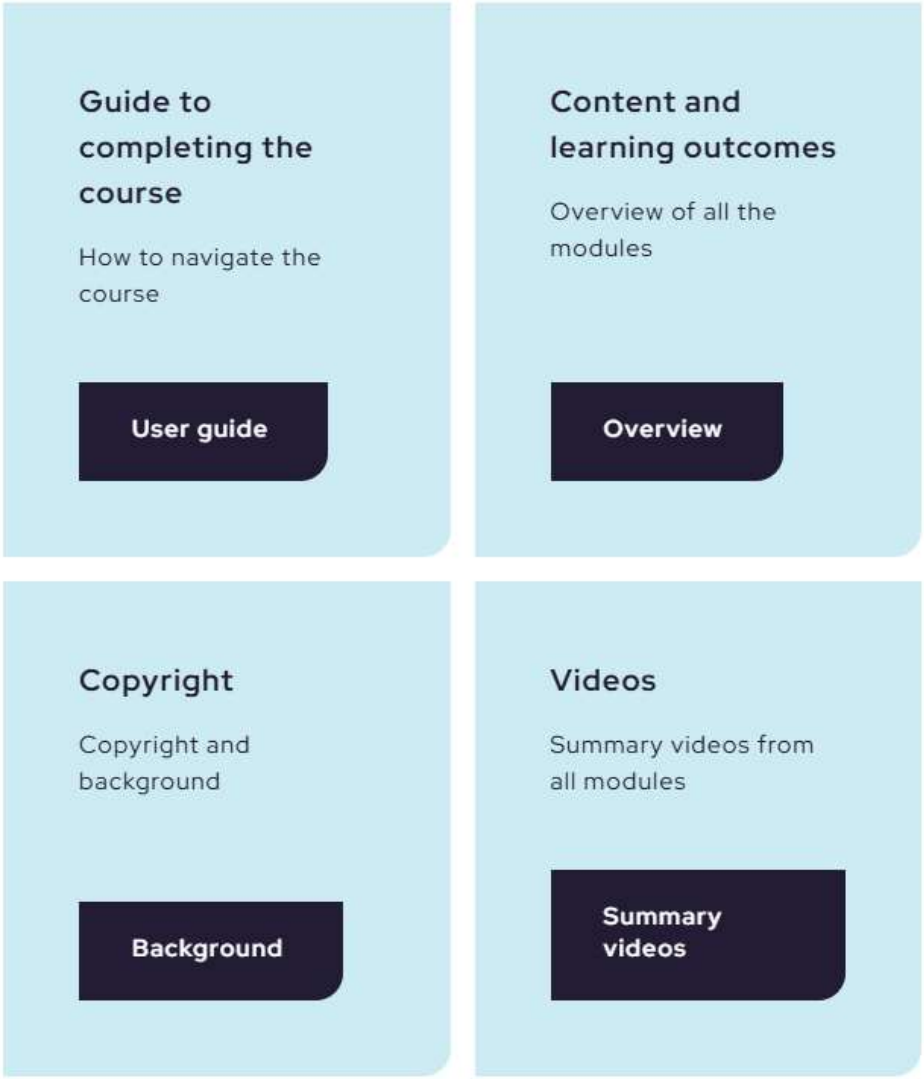
- Easily accessible
- 15-20 min per module
- Relatable case scenario-based
- learning for all staff.
- Free
- Compliant with question 3.2.1 on
- data protection training of staff.



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

- Join our launch webinar on 23rd Jan here



New guidance BYOD Policy Builder

- Free app to build and customise your data and cyber policies
- Available on mobile and desktop
- Avoid relying on 'cut and paste' template policies
- Understand the issues and customise your data and cyber security policies that work for your organisation
- The first policy is Bring Your Own Device
- More policies to follow

New guidance (forthcoming)

- Data quality
- Data Protection
- Data Security
- Information Asset Register (IAR)
- Record of Processing Activity (ROPA)
- Digital Asset Register (DAR)
- Record Retention
- Audit Checklist
- Acceptable Use Policy
- 3rd Party Suppliers

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 template policies to download on the 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

Further guidance: Digital Care Hub

Staff and workforce

- Data Security and Protection Responsibilities
- Staff Guidance
- Digital Skills and Training

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 Care Hub website – view guidance, register for free updates

Contact us for tailored support

32 Local Support Partners across the country:

- 1-2-1 and small group support
- Help you answer your questions
- Help you to publish
- Connected to LA and NHS digital leads

Find your Local Support Partner

Large Care Provider Groups

- Contact Digital Care Hub helpline for advice and support
- 0808 196 4848 (Mon-Fri 9-5)
- help@digitalcarehub.co.uk

DSPT technical issues:

- DSPT Helpline 0300 303 5035

Next steps

Check out the guidance on Digital Care Hub

Contact your Local Support Partner

www.digitalcarehub.co.uk/bettersecuritybettercare

X(Twitter) @DigitalCareHub

Any final questions?

Poll for care providers

- What impact has it had on your confidence with reviewing and republishing your DSPT?
- How likely is it that you will complete your DSPT in the next three months?
- How likely is it that you will contact your Local Support Partner?
- Would you recommend this webinar to a colleague?

Thank you.