Completing Standards Met for the First Time

How-To-Guide

DSPT
Better security.
Better care.

Digital
Social Care

Introduction

This guide has been designed to help adult social care providers with achieving 'standards met' on the **Data Security and Protection Toolkit (DSPT)**. There are also '**Big Picture Guides**' for social care providers which include more detail and background on the DSPT.

The DSPT should be completed every year. It is an online self-assessment tool for demonstrating compliance with the ten data security standards for health and social care organisations. The **Data Security Meta Standard** provides more information on what the ten data security standards are and why they are important.

The DSPT will help evidence your compliance with data protection legislation (General Data Protection Regulation or GDPR and Data Protection Act 2018) as well as CQC Key Lines of Enquiry (KLOEs).

How to complete your organisation profile

Once you have registered, you will need to sign in to complete your organisation's profile.

1. Go to **https://www.dsptoolkit.nhs.uk/Account/Login**. The first time you sign in, click "*Forgot your Password*". This will allow you to set your Administrator password.

2. Once signed in, you will see the following screen:
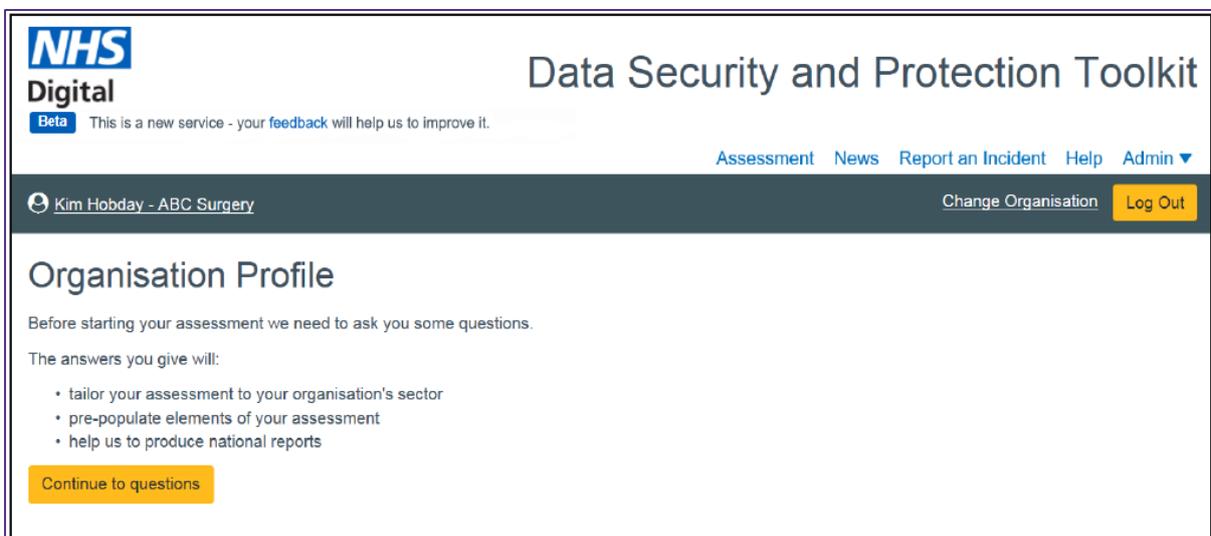
Click on the *"Continue to questions"* button to complete your profile.

3. Choose your organisation type. You should select "Social Care"

Which of these categories best describes your organisation?

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

○ Acute   ○ GP

○ Ambulance Trust   ○ Local Authority

○ AQP Clinical Services   ○ Mental Health Trust

○ AQP Non-Clinical Services   ○ NHS Business Partner

○ Arms Length Body   ○ NHS Digital

○ CCG   ○ Optician

○ Charity / Hospice   ○ Pharmacy

○ Community Services Provider   ○ Prison

○ Company   ○ Researcher / Department

○ CSU   ○ Secondary Use Organisation

○ Dentist (NHS)   ● Social Care

○ Dentist (Private)   ○ University

Save

4. You will be asked who has the following roles in your organisation:

    a. Caldicott Guardian

    b. Senior Information Risk Owner

    c. Information Governance Lead

    d. Data Protection Officer.

You **do not** have to enter any details. If you click the *"continue"* button you will move on to the next page.

None of these roles are well-known in adult social care. There is more detail about each role in our guide about **data security and protection responsibilities**.

5. You will be asked if your organisation uses NHSmail or has a Cyber Essentials Plus certification. Make sure you select the right option or "Not Sure" if you are uncertain.

6. Check your answers and make changes if necessary. Once you're happy, click "*Accept and Submit*". You can go back and make changes at any point.

How to set up other users

You might share your work on the DSPT with several people. As an administrator, you can add more users and assign their access level.

1. Sign in to the DSPT and click on the "*Admin*" tab, this will reveal a drop-down list:

```
User List

Organisation Details

Organisation Profile
```
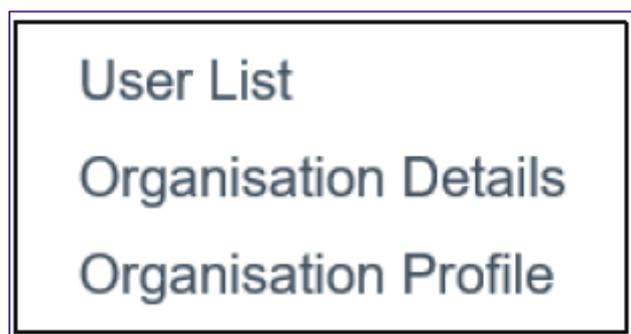
Select "*User List*".

2. Once on the User List page, you can add more users. Users can be allocated one of three roles:

   a. Auditor - view assertions/evidence/organisation profile, reset own password and update own personal details.

   b. Member - view assertions, view/add/edit evidence, view organisation profile (but not edit), reset own password and update own personal details.

   c. Administrator member - view and confirm assertions, view/add/edit evidence, allocate assertion owners, submit and publish assessment, view and edit organisation profile, create and edit users for own organisation, reset own password and update own personal details.

Completing your Assessment for the First Time
INTRODUCTION

Once you have completed your Profile questions, the Social Care Assessment is displayed. You can only see this view the first time you complete the Toolkit. If you have completed the Toolkit before, please skip to the next section.

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

1.1.2	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.2.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.2.2	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 April 2020?	
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 April 2020?	
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

1.2.1	Does your organisation have up to date policies in place for data protection and for data and cyber security?	Mandatory

Evidence items are numbered and organised under four headings:
- Staffing and roles
- Policies and procedures
- Data security
- IT systems and devices

To achieve 'Approaching Standards', you must complete all evidence items shown as MANDATORY. **If you complete all of the evidence items, then you will achieve 'Standards Met'**.

There is no specific order to completing the DSPT. You can start anywhere and move back and forth between the evidence items. The system will autosave at regular intervals.

HOW TO COMPLETE AN EVIDENCE ITEM

To complete an evidence item, click on it. This opens a dialogue box to complete.

Evidence item 1.1.2

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).

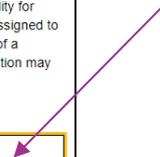Read more about data security and protection responsibilities and specialised roles.

Comments (optional)

Save or Cancel

In this example, type text into this box.

Once you have filled in the box, click "*Save*". This will close the box, and the evidence item will be marked as "*COMPLETED*".

Staffing and roles

1.1.2	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	COMPLETED
2.2.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory	
2.2.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory	

Staffing and Roles

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

Tool Tip	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 at: **https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/**.
Video Guide	**https://vimeo.com/654218225**

2.1.1 Does your organisation have an induction process that covers data security and protection, and cyber security?

Tool Tip	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date. There is an 'Introduction to Information Sharing for Staff' available: **https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/**
Video Guide	**https://vimeo.com/654230540**

2.1.2 Do all employment contracts, and volunteer agreements, contain data security requirements?	
Tool Tip	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security. There is an example staff contract clause available: **https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/**
Video Guide	**https://vimeo.com/654230540**

3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	
Tool Tip	A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation. Your organisation's training needs analysis should identify the level of training or awareness raising required by your staff, directors, trustees and volunteers if you have them. It should be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation. An example training needs analysis is available to download: **https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/**
Video Guide	**https://vimeo.com/654231923**

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?	
Tool Tip	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need.

	There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data. We have guidance on training, including sources of free online data and cyber security training: **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/**
Video Guide	**https://vimeo.com/654231923**

3.4.1 Have the people with responsibility for data security and protection received training suitable for their role?	
Tool Tip	It is likely that the person or people within your organisation who are responsible for data security and protection will need additional and more in depth training than the majority of your staff. Your organisation's training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).
Video Guide	**https://vimeo.com/654231923**

4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	
Tool Tip	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.
Video Guide	**https://vimeo.com/649217784**

Policies and Procedures

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

Tool Tip	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**.
Video Guide	**https://vimeo.com/654218225**

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?

Tool Tip	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved. Example IARs and ROPAs are available: **https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/**
Video Guide	**https://vimeo.com/654218225**

1.2.1 Does your organisation have a privacy notice(s)?	
Tool Tip	Your organisation must set out in clear and easily understood language what it does with the personal data it processes regarding the people it supports, staff and volunteers, and members of the public, for example relatives or other professionals etc. This is called a privacy notice and there may be more than one privacy notice e.g. one notice for staff and one for the people you support. Your organisation's privacy notice(s) should be made available to these people and inform them about their rights under data protection legislation and how to exercise them. It is good practice to publish your privacy notice on your website if you have one. An example privacy notice is available: **https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/**
Video Guide	**https://vimeo.com/654220870**

1.2.4 Is your organisation compliant with the national data opt-out policy?	
Tool Tip	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 31st March 2022. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from **NHS Digital** and **Digital Social Care**.
Video Guide	**https://vimeo.com/654220870**

1.3.1 Does your organisation have up to date policies in place for data protection and for data and cyber security?

Tool Tip	Confirm that your organisation has a policy or policies in place to cover: • data protection • data quality • record keeping • data security • where relevant, network security The policy or policies should be reviewed and approved by the management team or equivalent within the last 12 months. There is no set number of how many policies your organisation has to have on these topics as the different sizes and complexity of organisations means that some will have one all-encompassing policy, whilst others may have multiple policies. Policy templates are available**: https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**.
Video Guide	**https://vimeo.com/654222813**

1.3.2 Does your organisation carry out regular data protection spot checks?

Tool Tip	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download: **https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**.
Video Guide	**https://vimeo.com/654222813**

1.3.7 Does your organisation's data protection policy describe how you keep personal data safe and secure?

Tool Tip	Your policy should describe how your organisation considers privacy and data protection issues right at the start when embarking on a new project or

	process. This is called Data protection by design. This might be a new data sharing initiative for example if becoming part of a shared care record or if you are using personal data for a new purpose such as research. Your policy should also describe how your organisation only collect, use and share the minimum amount of data you need, how you limit access to only those how need to know, keep the data for a short time as possible and how you let people know what you do with their data. This is called 'data protection by default'. There is guidance on data protection by design and by default on **the ICO's website**. Our Data Protection Policy template covers this subject: **https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**.
Video Guide	**https://vimeo.com/654222813**

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 project involving personal data?	
Tool Tip	Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes. This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the **Information Commissioner's Office (ICO)**.
Video Guide	**https://vimeo.com/654222813**

1.4.1 Does your organisation have a timetable which sets out how long you retain records for?	
Tool Tip	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on **statutory requirements or other guidance**.
Video Guide	**https://vimeo.com/654227822**

1.4.2 If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed since 1st July 2021? This contract should meet the requirements set out in data protection regulations.	
Tool Tip	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If your organisation uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organisation, then the contract(s) or other written confirmation with third parties must include the requirement to have appropriate security measures and the facility to allow audit by your organisation. Further information about the destruction of records is in the **Records Management Code of Practice**. If you do not use third parties to destroy records or equipment, then tick and write "Not applicable" in the comments box. Advice on contracts for secure disposal of personal data is available: **https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/**
Video Guide	**https://vimeo.com/654227822**

1.4.3 If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	
Tool Tip	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old compute and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or

	equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box. We have a Record Keeping policy that has details on the safe destruction of personal data: **https://www.digitalsocialcare.co.uk//latest-guidance/template-policies/**
Video Guide	**https://vimeo.com/654227822**

10.1.2 Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	
Tool Tip	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then tick and write "Not applicable" in the comments box. A template example is available from **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/**
Video Guide	**https://vimeo.com/649223278**

Data Security

1.3.12 How does your organisation make sure that paper records are safe when taken out of the building?	
Tool Tip	Paper records may be taken out of your organisation's building(s), for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when 'on the move'? If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.
Video Guide	**https://vimeo.com/654222813**

1.3.13 Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.	
Tool Tip	Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your organisation's sites.
Video Guide	**https://vimeo.com/654222813**

5.1.1 If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	
Tool Tip	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place.

	If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/649219311

6.1.1 Does your organisation have a system in place to report data breaches?	
Tool Tip	All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner's Office ICO. If you are not sure whether or not to inform the Information Commissioner's Office of a breach, the toolkit's incident reporting tool and guide can help you to decide.
Video Guide	https://vimeo.com/649220474

6.1.4 If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	
Tool Tip	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/649220474

6.1.5 If your organisation has had a data breach, were all individuals who were affected informed?	
Tool Tip	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

	More information is available from the Information Commissioner's Office: **https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/personal-data-breaches/**
Video Guide	**https://vimeo.com/649220474**

7.1.2 Does your organisation have a business continuity plan that covers data and cyber security?	
Tool Tip	Your organisation's business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire). An example business continuity plan is available: **https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**
Video Guide	**https://vimeo.com/digitalsocialcare/71**

7.2.1 How does your organisation test the data and cyber security aspects of its business continuity plan?	
Tool Tip	Describe how your organisation tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be in the last 12 months. Guidance for testing your business continuity plan for the data and cyber security aspects is available: **https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**.
Video Guide	**https://vimeo.com/digitalsocialcare/72**

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?	
Tool Tip	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, then tick and write "Not applicable" in the comments box. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available: **https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/**
Video Guide	**https://vimeo.com/654222813**

1.3.14 What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	
Tool Tip	Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile phones, write "Not applicable" in the text box. Guidance is available: **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/**
Video Guide	**https://vimeo.com/654222813**

4.1.2 Does your organisation know who has access to personal and confidential data through its IT system(s)?	
Tool Tip	Your organisation should know who has access to the personal and confidential data in its IT system(s). Each person needs to have their own account to access a system. If that is not currently possible, and users share a login, the organisation must risk assess the situation and agree a plan to end the use of shared logins. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/649217784

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?	
Tool Tip	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box
Video Guide	https://vimeo.com/649218826

4.5.4 How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	
Tool Tip	If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password. If your organisation does not use any IT systems, computers or other devices, write "Not applicable" in the text box. Information about good password practice is available: **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/**
Video Guide	

6.2.1 Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	
Tool Tip	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available: **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/**
Video Guide	**https://vimeo.com/digitalsocialcare/62**

6.3.2 Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?	
Tool Tip	Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write "Not applicable" in the comments box.
Video Guide	**https://vimeo.com/649222262**

7.3.1 How does your organisation make sure that there are working backups of all important data and information?	
Tool Tip	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write "Not applicable" in the text box. For advice about backups, see **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/back-up-your-data/**
Video Guide	**https://vimeo.com/654232639**

7.3.2 All emergency contacts are kept securely, in hardcopy and are up-to-date.	
Tool Tip	Contacts include phone number as well as email.
Video Guide	**https://vimeo.com/654232639**

7.3.4 Are backups routinely tested to make sure that data and information can be restored?	
Tool Tip	It is important that your organisation's backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question.

	If your organisation does not use any computers or IT systems, then tick and write "Not applicable" in the comments box.
Video Guide	**https://vimeo.com/654232639**

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?	
Tool Tip	Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems or software, then tick and write "Not applicable" in the comments box. For guidance (including information on how to check which software versions you have), see **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/**
Video Guide	**https://vimeo.com/digitalsocialcare/81**

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.	
Tool Tip	This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. If your answer to the previous question was yes, write "Not applicable" in "Enter text describing document location".

Video Guide	**https://vimeo.com/digitalsocialcare/82**

8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed?	
Tool Tip	It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box. Further information is available from **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/**
Video Guide	**https://vimeo.com/649222683**

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?	
Tool Tip	Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments box.
Video Guide	**https://vimeo.com/digitalsocialcare/91**

9.5.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	
Tool Tip	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example,

	by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box. For advice on encrypting mobile devices and equivalent security arrangements, see **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/**
Video Guide	**https://vimeo.com/654233192**

10.2.1 Do your organisation's IT system suppliers have cyber security certification?	
Tool Tip	Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on the Digital Marketplace (**https://www.digitalmarketplace.service.gov.uk/**), or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box. Guidance is available: **https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/**
Video Guide	**https://vimeo.com/654233438**

How to publish

When you have completed all items you can publish at Standards Met. To do this:

1. Click on the blue button at the bottom of the page
2. You will be asked to confirm that your organisation profile is correct
3. If you are part of a multisite organisation ensure that you have listed all of your sites you are publishing on behalf of

4. Click "Publish Standards Met Assessment"

When you have done this, you will receive an email confirming that you have published and confirmation will appear on the screen.

Congratulations, you have completed Standards Met on the DSPT.

Help!
If you are having technical difficulties with any part of the DSPT, please **contact the DSPT team**.

If you have any concerns or questions on any of the materials mentioned in this guide, please contact us: **help@digitalsocialcare.co.uk**