

# A Workbook for small to medium sized care providers: how to complete the Data Security and Protection Toolkit

**Better Security,  
Better Care.**



Workbook contents:

Page

- 2** Introduction
- 9** First Steps
- 13** Things to Know
- 19** Where to Start
- 31** Evidence Items
- 76** Help and Support
- 77** Checklist of all Evidence Items



# 1. Introduction

This section describes how to use the Workbook, what the DSPT is, how the DSPT will help you and how it is structured.

Section contents:

Page

- 3 How to use the Workbook
- 5 What the DSPT is
- 6 How the DSPT will help you
- 7 How the DSPT is structured
- 8 Walkthrough of DSPT steps



# How to use this Workbook

This Workbook is designed to be used in many different ways to support the completion of the Data Security and Protection Toolkit (DSPT). Before you start, do take ten minutes to read the first four sections and consider what is the best way for the DSPT to be completed for your service.

In terms of who completes the DSPT, it is highly recommended that someone with senior responsibility for data protection and security completes it. This person will differ in different care providers. For the small to medium care homes, the person is likely to be the care home manager, however it does not have to be. Support on role descriptions is in here: <https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/> Other people in your organisation are likely to be needed to help, and this is explained in the 'Things to Know' section and within each description of the evidence item.

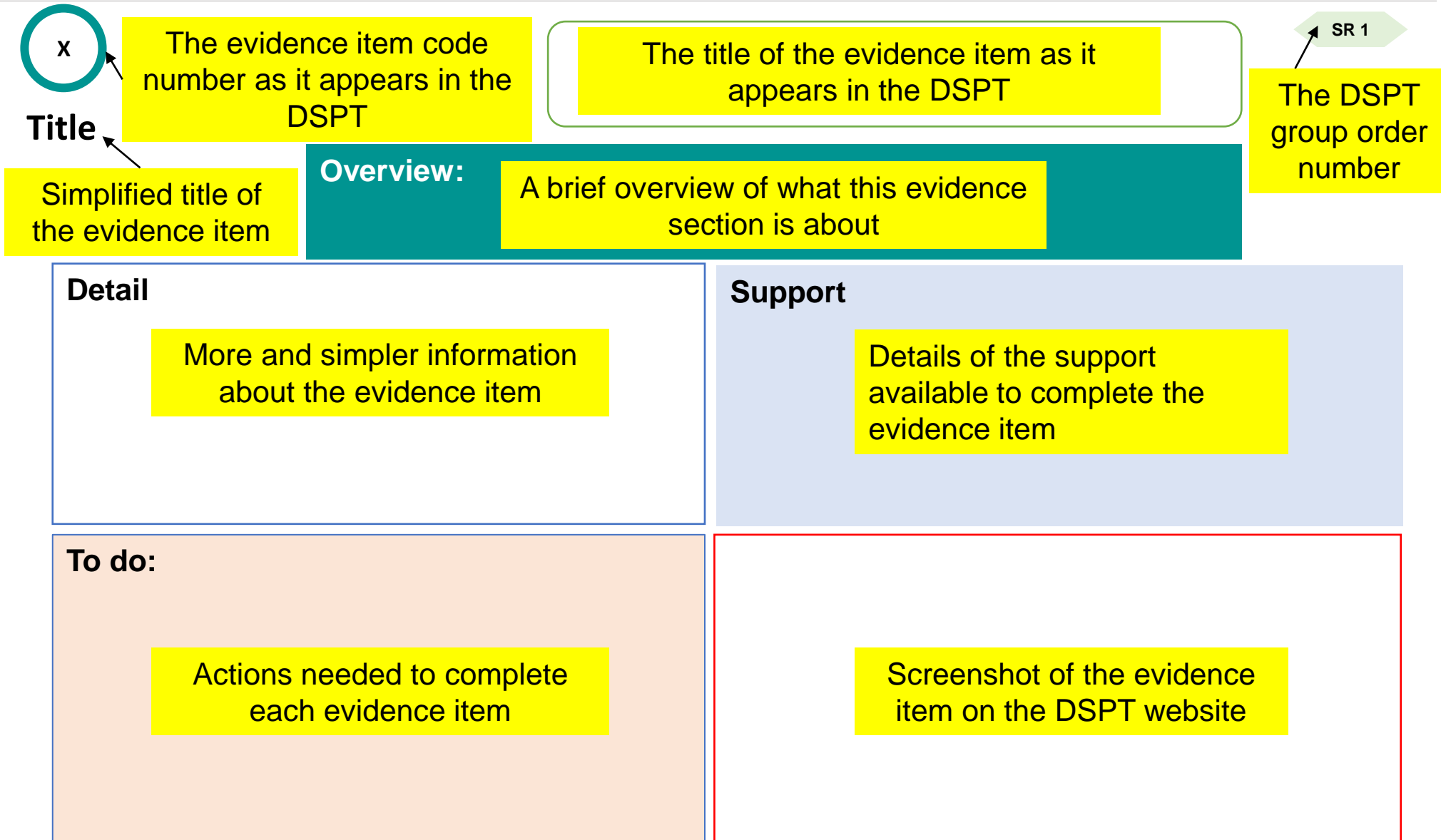
This Workbook is in six sections:

1. Introduction – what is the DSPT and how completing it **will help your organisation**
2. First Steps – registering for the DSPT and how to set-up your organisation
3. Things to Know – **top tips** on how to complete the DSPT more easily
4. Where to Start – **tailored approach for your organisation** to take to reach Standards Met
5. Evidence Items – a page for each evidence item containing a screenshot of the actual DSPT, what you need to do, and **how to access free support** including **downloadable templates and policies** for that evidence item (see layout on next page)
6. Appendices – links to more help and support and phone numbers for free support, plus a checklist listing all evidence items in numerical order on page 77 - you might want to print this out and make notes on it

Make sure you familiarise yourself with the Workbook – there are lots of top tips



# Page layout of each evidence item in this Workbook

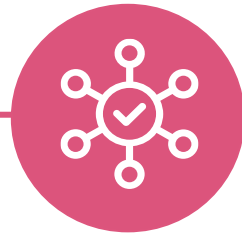


# What is the DSPT?

## DSPT = Data Security and Protection Toolkit = DSP Toolkit



An online self assessment of your organisation's data security



Demonstrates compliance with 10 data security standards and data protection law



Must be completed once and then reviewed each year, particularly if services are funded by the NHS



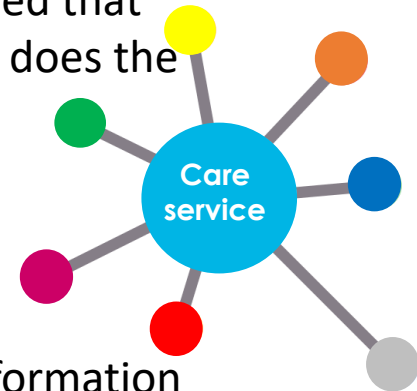
All adult social care services are strongly recommended to complete it

A video giving a general introduction to the DSPT is here: <https://vimeo.com/453700356>  
It is recommended that before starting you watch this video (it's only 7 minutes) or attend an introductory training session run by your local partner:

<https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/better-security-better-care/local-support-partners/>

# How will the DSPT help your care service?

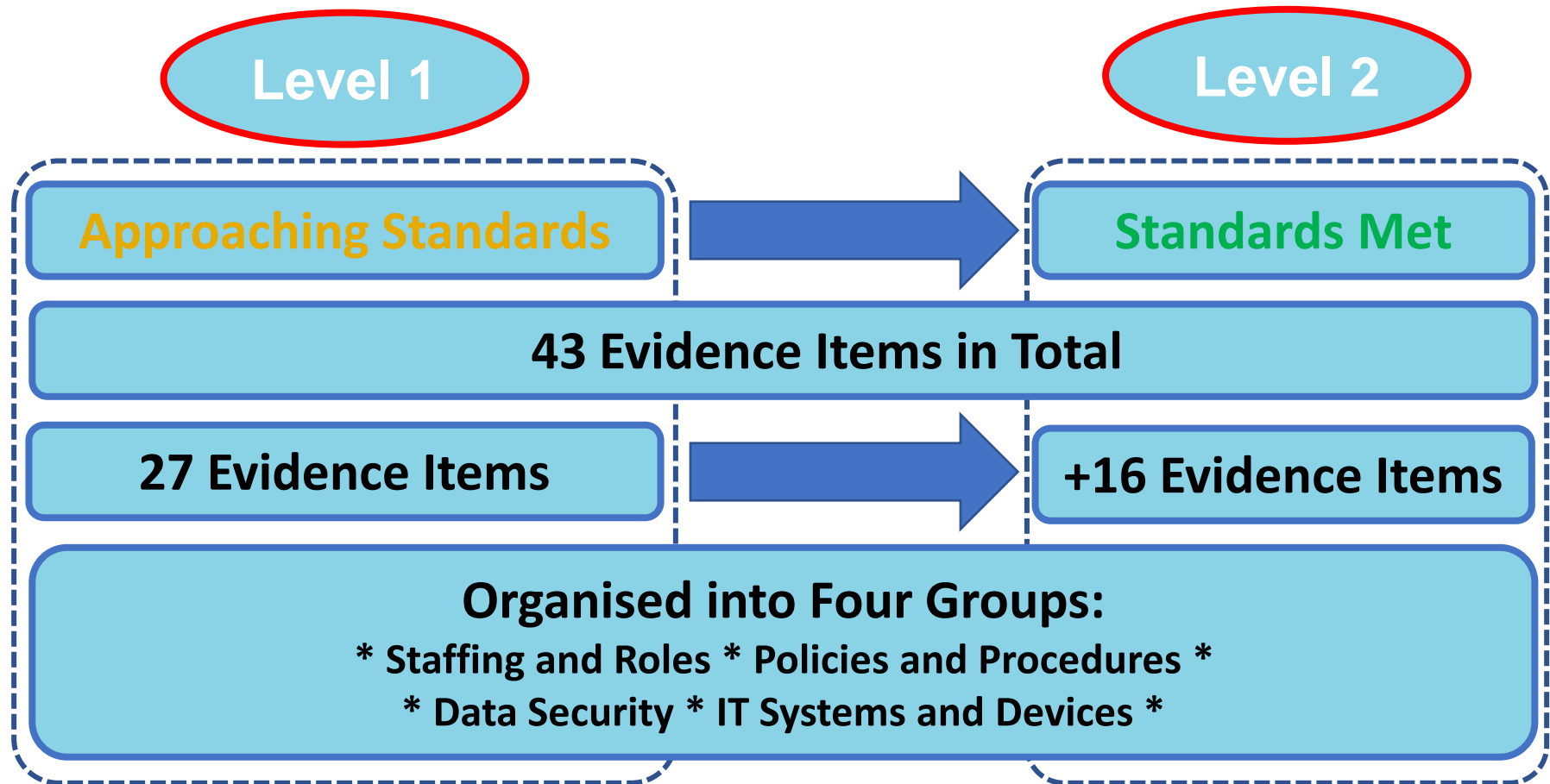
- 1 The **DSPT** is a good way to **know and demonstrate** that your service is practising good data security and handling data correctly, as well as **showing you** how to protect your business from serious risks like data breaches and cyber attacks
- 2 It will help your organisation to demonstrate it meets **CQC's expectations**. In particular, question C3.3 from the Key Lines of Enquiry (KLOE) asks: "How are people assured that information about them is treated confidentially...?" Question W2.8 asks: "How does the service satisfy itself that it has robust arrangements... in line with data security standards?"
- 3 The **DSPT opens up opportunities** for your service to:
  - share information digitally across health and care networks
  - be part of projects that allow care services to directly access NHS patient information systems, for example, GP records and shared care records. More information can be found here: <https://www.digitalsocialcare.co.uk/faqs/do-i-need-to-use-the-data-security-and-protection-toolkit-to-access-shared-health-and-care-systems/>
  - save you and your staff time and therefore improve the quality of care for the people you support



**The DSPT has two levels (Approaching Standards and Standards Met). Both help you to demonstrate your organisation's good practices.**

# How is the DSPT structured?

The DSPT's two levels help to manage the overall requirements



The DSPT covers all ten Data Security Standards that national policy states all health and social care providers must follow: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-policy/>

# DSPT walkthrough

## 01 Complete your Registration

1. See full details on page 10
2. Go to:  
<https://www.dsptoolkit.nhs.uk/Account/Login>

The first time you sign in, click on the “*Forgot your Password*” button. This will allow you to set your Administrator password using the email address you supplied.

## 02 Provide Evidence

1. To gain “**Approaching Standards**”, your organisation must complete 27 evidence items and agree an action plan
2. To gain “**Standards Met**”, your organisation must complete 43 evidence items for the 36 “*assertions*”
3. Each evidence item describes how to complete it and where to find **free support including templates and policies**
4. The remainder of the Workbook will help you identify what can be provided for each piece of evidence
5. Once you have added the evidence, always click save on the dialogue box. This will mark the section as complete

## 03 Publish at Standards Met

1. Once you can see “Standards Met” on the right hand side of your screen, you are ready to publish

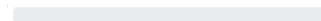
### Progress

[Go to progress dashboard and reports](#)

27 of 43 mandatory evidence items provided



0 of 36 assertions confirmed

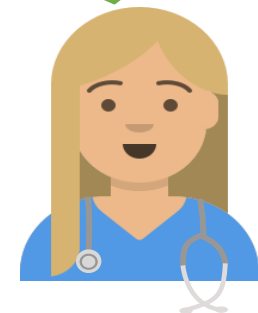
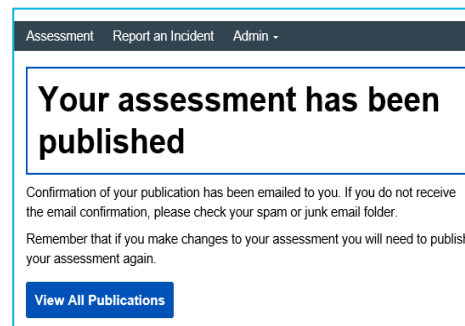


Your assessment status (if you were to publish now)



Note: the display will differ depending on whether or not you have previously published. This is how it will display if you've previously published

2. Click on “*Publish Assessment*”
3. You'll go to a screen called “Publish Assessment”
4. Click “*Publish Assessment*”
5. You will see this:







## 2. First Steps

This section describes what you need to do to register and set up your profile on the DSPT

Section contents:

Page

- 10 How to register for the DSPT
- 11 How to set up your profile
- 12 Password reset instructions

# How to Register for the DSPT

## Registration All sites must be registered individually.

If your organisation is a:

- multi-site provider, please look here for more guidance:

<https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/data-security-and-protection-toolkit/multisite-organisations>

- single site provider, please follow these instructions to register:

1. You will need your current work email address, or your NHSmail address, and your ODS Code (Organisation Code) which begins with a V.
2. If you don't know your ODS code, check the ODS portal by typing in the postcode of your site: <https://odsportal.digital.nhs.uk/Organisation/Search>

or if you are still having trouble, please contact the Helpdesk **0300 303 4034** or [exeter.helpdesk@nhs.net](mailto:exeter.helpdesk@nhs.net)

3. Register on DSPT by going here:

<https://www.dsptoolkit.nhs.uk/Account/Register>

4. If you are registering your organisation for the first time, you will be the Administrator. You will be responsible for completing your organisation's profile and adding any other users. Other users can have the same or different access rights as you. It is important to add other users. More information can be found here: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/data-security-and-protection-toolkit/single-site-organisations-including-domiciliary-care-operating-out-of-one-office-location/>

### Organisation / Practitioner Search

Search for an organisation or practitioner using their code, type, name, address or postcode.  
You must enter at least one search value, although partial matching is possible on postcodes.  
GP Practice search criteria – please note GP Practice information is held as Prescribing Cost Centre in the Type drop down menu.

Search Criteria:

Code:

Type:

Name:

Address:

Postcode:

## NHS Data Security and Protection Toolkit

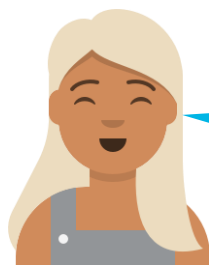
Digital

### Before You Register

You will need.

- Your email address
- A valid organisation code

You can look up your organisation code via the [ODS Portal](#) or alternatively [contact us](#).

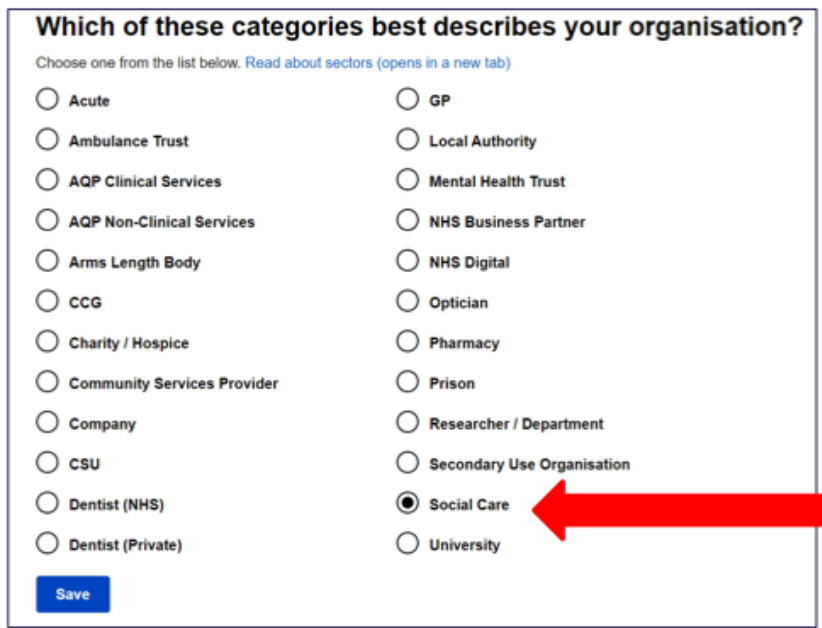
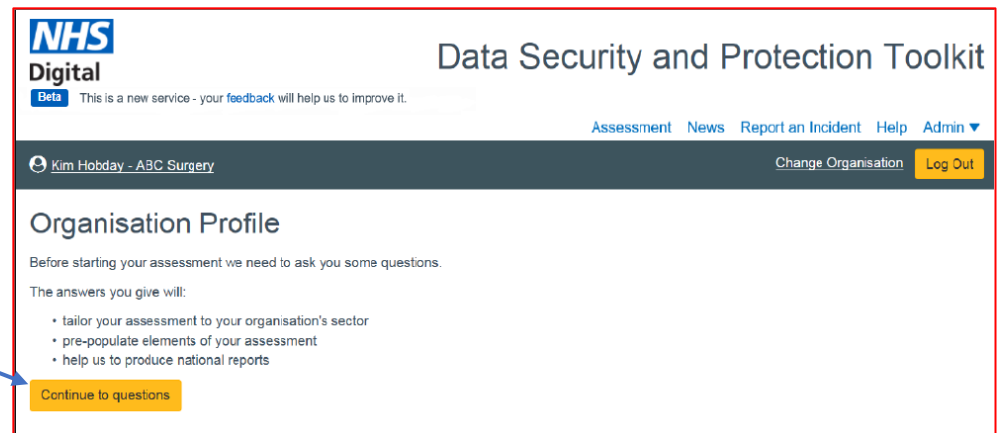


Remember to add other users – see the section on 'Things to Know' for more info!

# How to set-up your Profile on the DSPT

## Profile set-up

1. Go to: <https://www.dsptoolkit.nhs.uk/Account/Login>  
The first time you sign in, click on the “*Forgot your Password*” button. This will allow you to set your Administrator password using the email address you supplied.
2. Click on “*Continue to Questions*” on following screen.
3. Choose your organisation – ‘Social Care’
4. Do not enter any details under ‘Caldicott Guardian’, ‘Senior Information Risk Owner’, ‘Information Governance Lead’ and ‘Data Protection Officer’. Just click on the “*Continue*” button.
5. Answer the questions about whether your organisation has NHSmail, or has a Cyber Essentials Plus certification. If you don’t know, select “*Not Sure*”. You can always come back to any question.
6. Check your answers, once you’re happy, click “*Accept and Submit*”.
7. You will now be responsible for adding any other users. Other users can have the same or different access rights as you. It is important to add other users. For how to do this, look at back of this pack.
8. Your DSPT Profile is DONE!



You can go back and make changes at any point



# Already registered but forgotten your password?

If you've forgotten your DSPT password, go to the login page here:

<https://www.dsptoolkit.nhs.uk/Account/Login>

Click on 'Forgot your password?'

The system then sends you an email

Follow the link in the email to reset your password

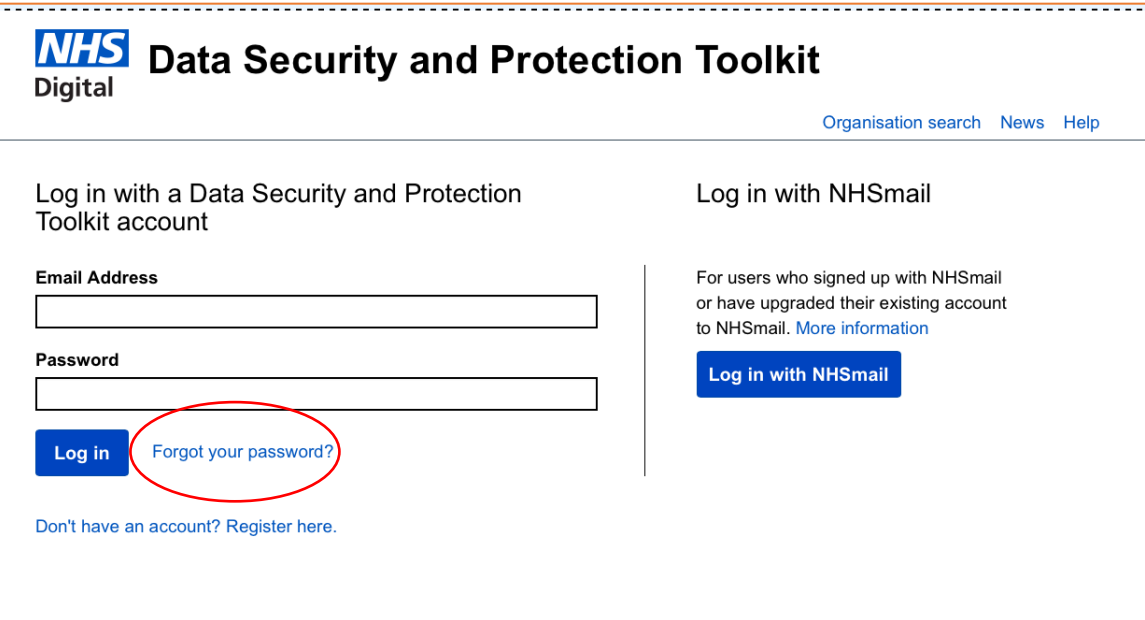
There is onscreen guidance for resetting (and setting your password)

**If you require help, contact:**

**Telephone:** 0300 303 4034

**Email:** [exeter.helpdesk@nhs.net](mailto:exeter.helpdesk@nhs.net)

Please provide your ODS code or address when raising queries via email





## 3. Things to Know

This section gives you top tips on the key things you need to know before you start. It includes how to add more users and which evidence items you can request they complete.

Section contents:

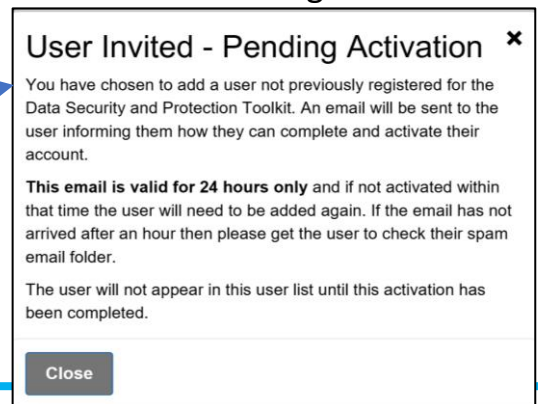
Page

- 14 Adding more users to the DSPT
- 15 Who to ask for assistance
- 16 Start on lengthy items
- 17 How to allocate assertions
- 18 Completing assertions

# Top Tip 1: Add more users to the DSPT

It is important to add other users to your organisation's DSPT so that there is more than one person with access.

- Decide who you would like to add. Check with them that this is ok. Make sure that they are available in the next 24 hours to access their email and activate automatic request.
- To add new users, sign in to the DSPT. Click on the “*admin*” tab in the top right. This will reveal a drop down menu. Select “*user list*”. Click on “add user” in blue on top right of the screen.
- Once on the user list page, insert the email address of the user you'd like to add.
- Choose the type of access that you'd like the new user to have. There are three types of users:
  1. **Administrator** – access to view and edit everything, and can publish.
  2. **Member** – view everything, can edit evidence points but not organisation profile. They can reset their own password and update their own personal details.
  3. **Auditor** – view (but not edit) everything, they can reset their own password and update their personal details on the system.
- Here are some ideas of the roles for these types of users:
  - The **Administrator** could be the Registered Manager and possibly the Data Security and Protection Lead. This is advised as the Administrator will have editing and publishing rights for everything.
  - If you are part of a group which deals with all security policy and contracts centrally, it would be a good idea to add someone from the group as a **Member**. This will allow them to agree to evidence items that an individual manager does not have control of, such as the data security policy.
  - If you have a local champion – someone in the region who can help with the DSPT – it could be a good idea to add them as an **Auditor**.  
They can check the evidence you have uploaded is correct and keep track of your progress without having to travel to your home.
- Once you have invited the new user, you will see this message.
- Get in touch with the added user and ask them to check their email, including their spam



# Top Tip 2: Ask for assistance

You can ask the following roles for assistance on these evidence items and allocate them the related assertions. The numbers in bold are part of the Approaching Standards set.

Very  
Senior  
Leader

**1.1.2**  
**1.1.5**  
**1.3.1**  
1.3.2  
3.1.1  
3.4.1  
**6.1.3**  
8.2.1

IT  
Supplier

1.3.14  
**4.2.4**  
**6.2.1**  
**7.3.1**  
7.3.4  
8.1.4  
8.2.1  
**8.3.5**  
9.1.1  
9.5.2  
10.2.1

HR

**2.1.1**  
**2.1.2**  
3.1.1  
3.2.1  
3.4.1  
**4.1.1**

Contracts  
Lead

**1.4.2**  
**10.1.2**

# Top Tip 3: Start early on the items that take the longest

These are the evidence items that take the longest, so start early on these

**IAR and ROPA: 1.2.1** (needed for publishing at 'Approaching Standards')  
Creating the IAR and ROPA can take time to complete if they have not been created before. By starting on these soon after beginning the DSPT, it is likely that the overall time to completion will be less as other people can be completing their evidence items whilst this one is being worked on. The guidance on how to document your data processing is here:

<https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/>

## **Training: 3.2.1 and 3.4.1**

Although these two items are within Standards Met, it is important to start them early as individuals will have to carry out training that they may not currently complete. Alerting people to carry out training when the DSPT completion process begins will help to complete the DSPT quicker as people can do the training whilst the rest of the evidence is being compiled.



# Top Tip 4: How to allocate assertions\* to people

Individuals with these roles can be added as users to the DSPT and be allocated the assertions\* for the evidence items that they have responsibility for.

Very  
Senior  
Leader

IT  
Supplier

HR

Contracts  
Lead

The DSPT can be completed in any order and by more than one person at a time by adding users (see page 14) and allocating them assertions to complete.

You allocate assertions by clicking on the word 'Assign Owner' beside 'No Owner:' which is just under the assertion statement. You are then asked 'Who would you like to confirm the assertion?' and provided with a list of names of people that are in your user list. Click on the person you want to allocate this assertion to and then click on 'Assign ownership to selected user'. You can change this at any time.

3.2 Staff pass the data security and protection mandatory test

Owner:  
No Owner [Assign Owner](#)

3.2.1 [Have at least 95% of staff, directors, trustees and](#)

The person with ownership can then filter the assertions that are allocated to them and complete them.

\* Note: in some views of the DSPT the assertions are not able to be seen. If you need help with this, please contact the helpdesk. Contact details on page 76

# Top Tip 5: Remember to click on the assertions

If you are at Standards Met when you review your DSPT, you will be viewing the DSPT in the **Social Care Assessment** view, and will see assertion boxes.

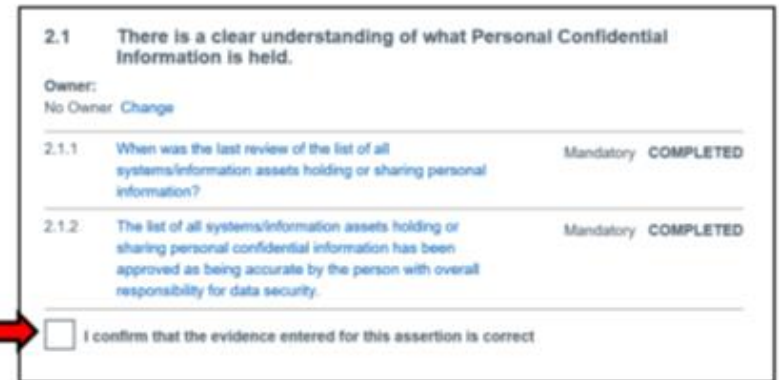
**Remember to tick them all!**  
**This page tells you how to do it.**

Once you have completed all the evidence items for a statement, the assertion box pops up at the bottom. You need to click on the box.

When you click on the box the whole area turns grey to show that it is complete.

If you need to change an evidence item that has been greyed out you need to click on the box with the tick in.

Note that all assertions need to be ticked, and therefore confirmed by that individual, before the user is offered the option to publish at Standards Met.



2.1 There is a clear understanding of what Personal Confidential Information is held.

Owner:  
No Owner [Change](#)

---

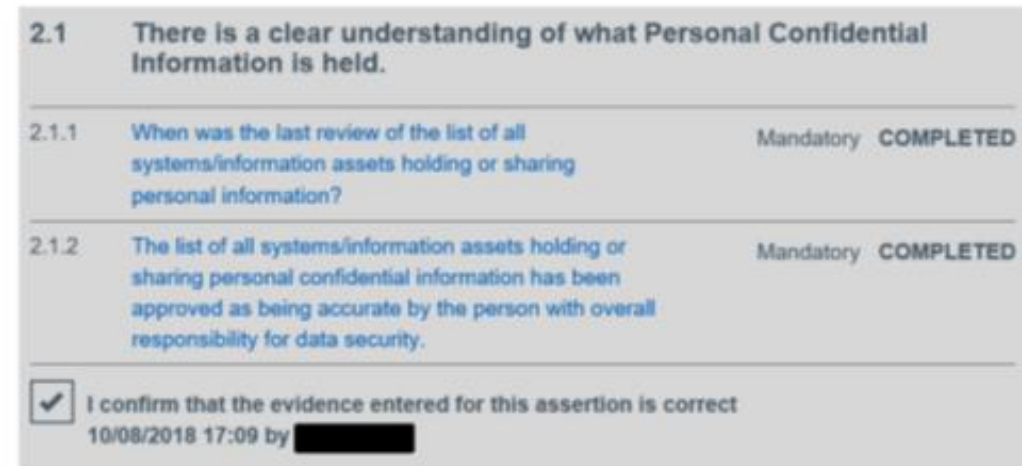
2.1.1 When was the last review of the list of all systems/information assets holding or sharing personal information? Mandatory COMPLETED

---

2.1.2 The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security. Mandatory COMPLETED

---

I confirm that the evidence entered for this assertion is correct



2.1 There is a clear understanding of what Personal Confidential Information is held.

---

2.1.1 When was the last review of the list of all systems/information assets holding or sharing personal information? Mandatory COMPLETED

---

2.1.2 The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security. Mandatory COMPLETED

---

I confirm that the evidence entered for this assertion is correct  
10/08/2018 17:09 by [REDACTED]



## 4. Where to Start

This section describes where to start depending on what you have already completed.

It contains:

Page

- 20 Aim for Standards Met
- 21 Are you already at Standards Met?
- 22 New and Revised Evidence Items
- 23 Are you already at Entry Level?
- 24 Publishing at Approaching Standards
- 25 Action Plan
- 26 Order for Completing Evidence Items
- 30 Review Before Publishing

# Aim for Standards Met

It is recommended that all social care providers complete the DSPT to Standards Met

In the Social Care Assessment view, the 43 evidence items are collected together under the following groups:

- Staffing and roles (7 evidence items)
- Policies and procedures (12 evidence items)
- Data security (8 evidence items)
- IT systems and devices (16 evidence items)

You can start on any of these four groups but it's recommended you complete the evidence items in the order that they are shown on the four pages from page 26

The DSPT orders them in number order but our research showed that the ordering on the four pages makes more logical sense for providers

As you progress with each evidence item, we recommend that you use the support links included on the page for each evidence item. Remember to read the 'top tips', as well as look at the Help and Support page at the end of this Workbook. There is always someone available to help, so if you do get stuck, please reach out.

# Are you at Standards Met already? If you are, start here...

If you are at Standards Met for 2020/21 or a previous year, your next submission will require you to review your current responses and complete any new mandatory questions. There have been some changes to the numbering of the evidence items and some new mandatory items. Therefore it's recommended that you follow the route on pages 26 to 29 as this has been tested on care providers and makes sense to them. But of course it is up to you.

**Tip:** once you've answered all the evidence items, remember to tick the assertions! See how to do this on page 17.

**These are the steps you need to take to publish:**



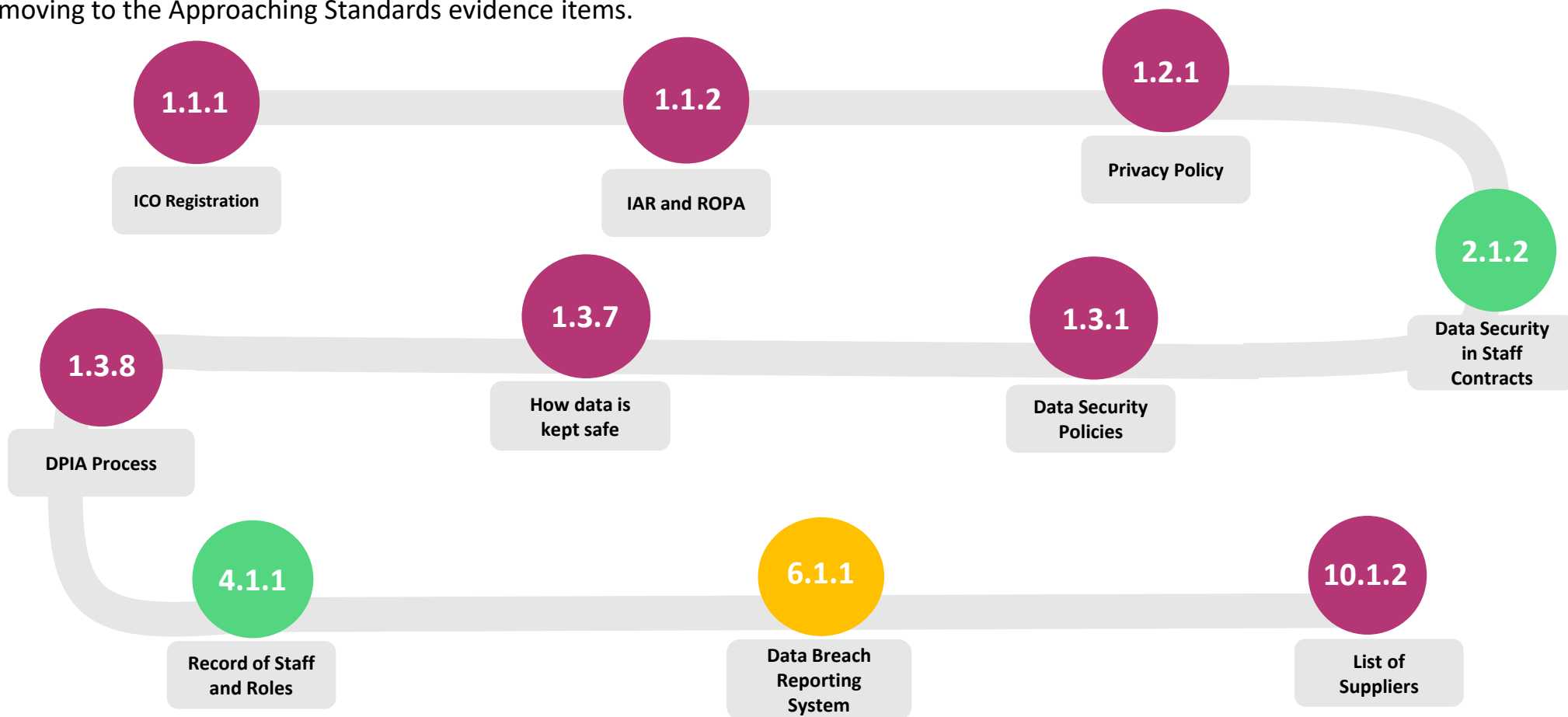
# For care providers at Standards Met 19/20: new and revised evidence items

As an easy way to keep track of your progress you can use this page to check off each of the new and revised items as you complete them



# Are you already at Entry Level? If so, start here...

Entry Level ended in March 2021 and the new stepping stone to reach Standards Met is called Approaching Standards. If you are already at Entry Level, then you would have completed the evidence items below. You must review and update your responses if that is required to these evidence items. Since these evidence items have been answered before, we recommend you update these items first then continue to the rest of the Approaching Standards evidence items. Read the page on Approaching Standards before moving to the Approaching Standards evidence items.



# Publishing at Approaching Standards

It is recommended that social care providers complete the DSPT to Standards Met. However, if this is not achievable, you are able to publish at [Approaching Standards](#).

The 27 evidence items are collected together under the following groups:

- Staffing and roles (4 evidence items)
- Policies and procedures (10 evidence items)
- Data security (5 evidence items)
- IT systems and devices (8 evidence items)

You can start on any of these four groups but it's recommended you complete the evidence items in the order that they are shown on the four pages from page 26. The DSPT orders them in number order but our research showed that the ordering on the four pages makes more logical sense for providers.

For Approaching Standards, complete the evidence items on pages 26 to 29 that have a red circle around them, and then you will have to produce an action plan. More help on the action plan is on the next page.

As you progress with each evidence item, we recommend that you use the support links included on the page for each evidence item. Remember to read the 'top tips', as well as look at the Help and Support page at the end of this Workbook. There is always someone available to help, so if you do get stuck, please reach out.



# Approaching Standards' Action Plan – agreement to reach Standards Met

Once you have completed the “Approaching Standards” evidence items, you will need to agree to reach Standards Met by completing an action plan.

You will have the option to download a blank template which lists the evidence items you are yet to complete.

Once completed, you need to upload it to the DSPT.

You will then be able to publish at “Approaching Standards”

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

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

December Social care test [Change organisation](#) [Organisation search](#) [News](#) [Help](#)

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

[← Assessment](#)

## Provide an action plan

Thank you for responding to all the mandatory requirements

- 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.
- You will then be able to publish your 'Approaching Standards' assessment.

Upload file

Drag and drop Action Plan or [click to browse](#)

[Publish Approaching Standards Assessment](#)

# DSPT Social Care Evidence Items to Reach Standards Met

It is recommended you complete the evidence items in the order that they are shown here

## Staffing and Roles (SR)



**X** Red circle = Approaching Standards evidence items

**X** Red circle, black text = Entry level evidence items

# DSPT Social Care Evidence Items to Reach Standards Met

It is recommended you complete the evidence items in the order that they are shown here

## Policies and Procedures (PP)



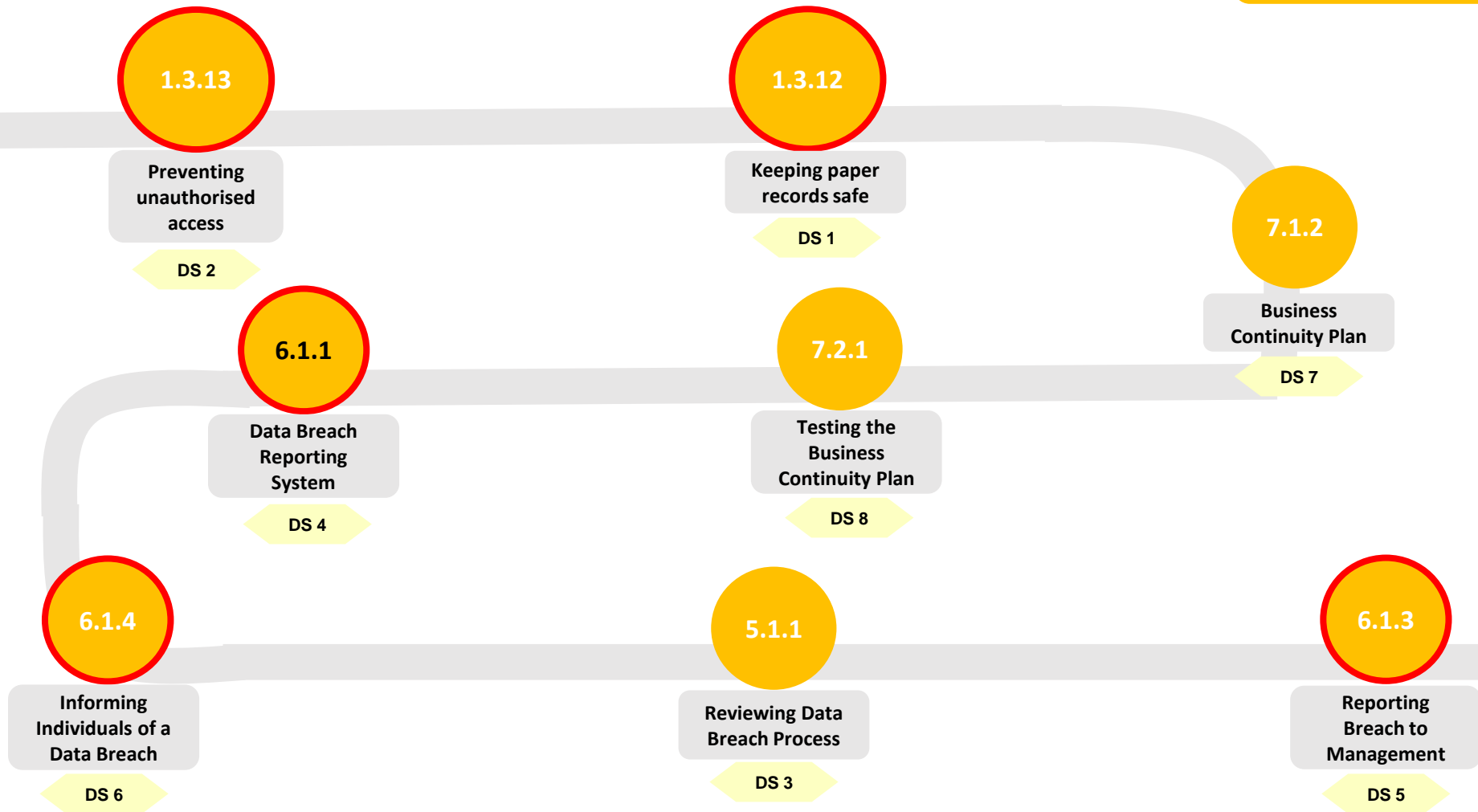
X Red circle = Approaching Standards evidence items

X Red circle, black text = Entry level evidence items


# DSPT Social Care Evidence Items to Reach Standards Met

It is recommended you complete the evidence items in the order that they are shown here

## Data Security (DS)



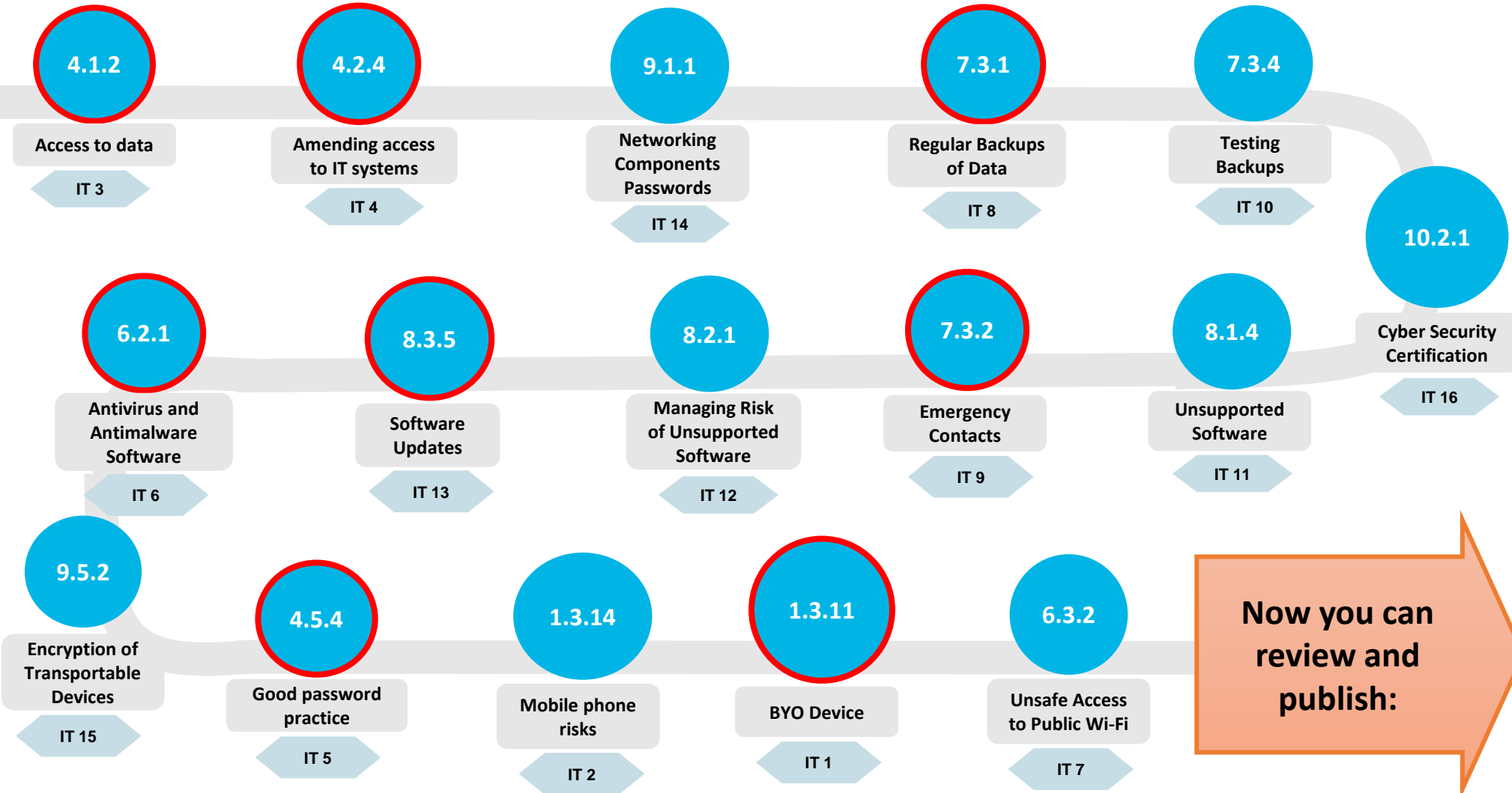
 Red circle = Approaching Standards evidence items

 Red circle, black text = Entry level evidence items

# DSPT Social Care Evidence Items to Reach Standards Met

It is recommended you complete the evidence items in the order that they are shown here

## IT Systems and Devices (IT)



Now you can review and publish:

**X** Red circle = Approaching Standards evidence items

# Review your responses before you publish

Review the responses to check they are all completed to your organisation's satisfaction

If you have items that still need completing, focus on publishing at Approach Standards with an agreed Action Plan

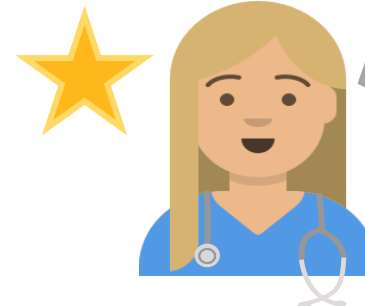
Make sure all Standards Met evidence items are complete

Publish at Standards Met and Celebrate

Great progress



Very Well Done



Now get in touch with your local support team to access data sharing systems



## 5. Evidence Items

This section has one page for each evidence item in numerical order.

Each page describes what you need to do and where you can access support, such as videos and templates.

All the policy documents you require are available for free on the Digital Social Care website. Links to them are provided.

1.1.1

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

## ICO registration

**Overview:** The Information Commissioner's Office (ICO) is the regulatory body for data protection and your organisation must be registered unless it is a small charity and therefore exempt.

### Detail

Social care providers are legally obliged to register with the ICO and pay a small registration fee (most care providers will already be registered).

### To complete this evidence item:

1. Enter your ICO registration number in the text box
2. No information is required in the optional comments box
3. Click on the blue 'save' button

### Support

- If your organisation is part of a group, head office is likely to have your organisation's ICO number
- If your organisation is not registered, register here urgently by following the link: <https://ico.org.uk/for-organisations/data-protection-fee/>
- If your organisation is likely to be registered, and the ICO number is unknown, the ICO register can be searched here: <https://ico.org.uk/esdwebpages/search>
- Video - <https://vimeo.com/654218225> (0:58 seconds)

#### 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](#)

Comments (optional)



or



# 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?

## IAR and ROPA

**Overview:** Care providers are legally obliged to keep a record of all personal and sensitive information they hold for staff and residents and how they share it.

### Detail

To be compliant with data protection legislation your organisation must describe how it:

- holds personal and sensitive information
- shares personal and sensitive information with others

Examples of ways that information is 'held' are: filing cabinets, care planning system, laptop, allergy folder and medications trolley. The list that contains the information 'held' by your organisation is called an Information Asset Register (IAR).

Examples of the information that is shared with others are: needs assessments, prescriptions, payslips and care plans. The list that contains shared information is called a Record of Processing Activities (ROPA).

For this evidence item your organisation needs at least one list covering both of these:

1. Information Asset Register (IAR) – contains what type of information is held, where and how it is stored and how it is kept safe
2. Record of Processing Activities (ROPA) – contains where data is received from, where it is sent to, the legal basis for doing this and how it is kept safe

### To complete this evidence item:

1. Choose the option that is most suitable:
  - Upload a document
  - Reference an existing uploaded document
  - Specify an intranet or internet link to a document
  - Enter text describing the document's location
2. Follow the instructions for that option. It is easiest to use the last option and state where the documents are, for example, in the DSPT folder on the manager's computer.
3. No information is required in the optional comments box
4. Click on the blue 'save' button

### Support

- Example IARs and ROPAs are available here: <https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/>
- Senior leadership is required for this evidence item
- Video: <https://vimeo.com/654218225> (2:16 minutes)


#### Evidence item 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?

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 from [Digital Social Care](#).

	test	<a href="#">Remove</a>	<a href="#">Edit</a>
---	------	------------------------	----------------------

- Upload a document
- Reference an existing uploaded document
- Specify an intranet or internet link to a document
- Enter text describing the document's location

Comments (optional)

or

1.1.5

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

## Responsibility for Data Security

**Overview:** There is a requirement for at least one person within your organisation to take overall responsibility for data security and protection

### Detail

The person's responsibility is to provide leadership and guidance on data security and protection from a senior level. This could be a senior administrator, such as the person in charge of bringing together reporting data for CQC. They need to have senior influence to make decisions about data security and protection. Read more about data security and protection responsibilities and specialised roles:

<https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/>

### To complete this evidence item:

1. Write the name(s) of the person (people) within your organisation with overall responsibility for data security and protection
2. For each of those people, write a description of how this responsibility has been formally assigned to each person. For example, this responsibility could be in their job description, be noted in the minutes of a management meeting, or be in an email from a director.
3. No information is required in the optional comments box
4. Click on the blue 'save' button

### Support

- Video - <https://vimeo.com/654218225> (6:02 minutes)
- Senior leadership may be required for this evidence item

### Evidence item 1.1.5

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

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

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

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

Comments (optional)

**Save** or Cancel

# Does your organisation have a privacy notice?

## Privacy Policy

**Overview: Your organisation must have a privacy notice in clear language that people can understand. The privacy notice has to cover everyone your organisation collects personal information about. There can be more than one notice.**

### Detail

The privacy notice(s) must state:

- what personal data your organisation collects
- what your organisation does with the personal data it collects
- what the rights are of the people whose personal data is being collected how those people can exercise their rights

The privacy notice has to cover: the people being supported (for example, residents and service users), staff and volunteers, and members of the public, for example relatives or other professionals etc.

The privacy notice must be made available to everyone in a language they can understand. It is good practice to publish the privacy notice on your organisation's website, if there is one.

### To complete this evidence item:

1. For each document, choose the option that is most suitable:
  - Upload a document
  - Reference an existing uploaded document
  - Specify an intranet or internet link to a document
  - Enter text describing the document's location
2. Follow the instructions for that option. It is easiest to use the last option and state where the documents are. For example, if your organisation uses a leaflet for residents, then write a short description and where it is held, such as: "The Welcome Pack in each resident's room includes the privacy notice and the original document is stored on the manager's PC in the 'data protection folder'". **Remember to include all your notices.**
3. No information is required in the optional comments box
4. Click on the blue 'save' button

### Support

- An example privacy notice is available here: <https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/>
- There is also a 'citizen leaflet' which is useful for resident handbooks
- Video – <https://vimeo.com/654220870> (0:30 seconds)

### Evidence item 1.2.1

## Does your organisation have a privacy notice?

If you use and share personal data then you must tell people what you are doing with it. This includes why you need the data, what you'll do with it, who you're going to share it with and individual's rights under data protection legislation e.g. to access the information.

This should be set out in writing in 'a privacy notice'. You should provide this information in a clear, open and honest way using easily understood language.

Privacy notice should cover all data you process for example the data relating to the people you support and their relatives, staff, volunteers, members of the public. You may have more than one privacy notice e.g. one for staff and another one for the people you support.

An example privacy notice is available from [Digital Social Care](#)



- [Upload a document](#)
- [Reference an existing uploaded document](#)
- [Specify an intranet or internet link to a document](#)
- [Enter text describing the document's location](#)

Comments (optional)

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

## Is your organisation compliant with the national data opt-out policy?

### National Data Opt-Out Policy

**Overview:** Your organisation must be compliant with the national data opt-out policy by 31 March 2022. The policy gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some minor exclusions.

#### Detail

As a provider, your organisation needs to help the people who use your services to understand that they can opt out of their data being used for purposes other than relating directly to their care.

Your policies, procedures and privacy notice must cover the national data opt-out. All health and social care CQC-registered organisations in England must be compliant with the national data opt-out by 31 March 2022 (deadline moved from 30 September 2021).

#### To complete this evidence item:

1. If you are completing the DSPT before 31 March 2022, and your organisation is not compliant with the national data opt-out policy, then click on the box at the top and in the optional comments box write "Not applicable at time of completion".
2. If your organisation is compliant with the national data opt-out, then click on the box at the top by the title. No information is required in the optional comments box.
3. Click on the blue 'save' button

#### Support

More detailed guidance that gives advice about compliance with the national data opt-out policy (NDOP) is available from:

- NHS Digital: <https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out>
- Digital Social Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-data-opt-out/>
- Video: <https://vimeo.com/654220870> (2:29 minutes)

#### Evidence item 1.2.4



#### Is your organisation compliant with the national data opt-out policy?

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 30 September 2021.

More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital](#) and [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

1.3.1

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

## Data Security Policies

**Overview:** The policies your organisation needs must cover Data Protection, Data Quality, Record Keeping, Data Security and, where relevant, Network Security. The policies must be approved by the management team or an equivalent.

### Detail

Policies are required to support staff guidance and staff training. Without effective (understandable and comprehensive) policies your organisation is at risk of not having a solid framework for your staff to carry out their duties of data protection and data and cyber security.

The policies must cover all the areas listed below. Some organisations will have one policy covering all areas, whilst others may have multiple policies. The policies will vary depending on the size and complexity of your organisation.

Your organisation's policy or policies must cover: Data Protection; Data Quality; Record Keeping and Data Security.

Your organisation may need a Network Security policy. It is required if there is a network over which multiple devices are connected. If a Network Security Policy is not required, then your organisation's Data Quality Policy can describe how automatic updates are completed on your organisation's computers and make sure your WiFi password is changed from the default.

The policies must be reviewed and approved within the last 12 months by the management team or equivalent group of senior members of staff in your organisation. If your organisation is small to medium sized, these are likely to be the data security and protection lead, team leaders, manager and owner.

### To complete this evidence item:

1. Once your organisation has these policies in place and approved, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

### Support

- Policy templates are available for free from Digital Social Care: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies>
- Video: <https://vimeo.com/654222813> (0:35 seconds)
- Senior leadership is required for this evidence item

#### Evidence item 1.3.1

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

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 from [Digital Social Care](#)

Comments (optional)

Save

ancel

1.3.2

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

### Data Protection Spot Checks

**Overview:** Your organisation is required to carry out data protection spot checks at least once a year, to make sure that staff are complying with your organisation's data protection policy and/or staff confidentiality policy/guidance.

#### Detail

It is useful to complete a checklist to capture your evidence that spot checks have been carried out, including details of any actions, who has approved the actions and, if applicable, who is taking them forward. The checklist can include items such as: ensuring no personal information is laying around the building, and all cupboards containing personal data are locked.

The spot checks must be carried out at least every year and can be part of other audits carried out.

Once the checks have been completed, the record can be saved and accessed when required.

#### To complete this evidence item:

1. Once your organisation is sure that it carries out regular data protection spot checks, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- There is an example audit checklist from Digital Social Care: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- Video: <https://vimeo.com/654222813> (2:15 minutes)

#### Evidence item 1.3.2

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

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 from [Digital Social Care](#).

Comments (optional)

**Save** or Cancel



1.3.7

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

### How Data is Kept Safe

**Overview:** How your organisation keeps personal data safe and secure must be described in your data protection policy through detailing what procedures staff must follow.

#### Detail

Your policy needs to describe how your organisation keeps personal data as safe as possible. There are two ways that data can be kept safe:

- by design
- by default

Here are some examples of what 'data protection by design' is:

- staff use codes instead of names when sharing data with others
- staff make emails secure, such as through encryption, so that only authorised people can read them
- the amount of personal information on residents' doors to their rooms and on notice boards is kept to a minimum

Here are some examples of what 'data protection by default' is:

- only the minimum amount of data is collected
- access is limited to only those who need to know
- data is kept for as short a time as possible
- people are informed about what is done with their data

Your organisation's policy must describe 'how' these examples are to be carried out.

#### To complete this evidence item

1. Once your organisation is sure that your data protection policy contains how data is kept as safe as possible, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- The Digital Social Care's data protection policy template contains information on how to keep data secure: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- There is guidance on data protection by design and by default on the [ICO's website](#).
- Video: <https://vimeo.com/654222813> (5:17 minutes)

#### Evidence item 1.3.7

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

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 who 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](#). The Data Protection Policy template that is available from [Digital Social Care](#) covers this subject.

#### Comments (optional)

**Save** or Cancel

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?**

## DPIA Process

**Overview:** Your organisation's data protection policy needs to describe the process for making sure that your organisation systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data.

### Detail

The process for identifying and minimising the data protection risks is called a Data Protection Impact Assessment (DPIA). A DPIA is a "process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan" (ICO website).

For care providers, DPIAs are particularly relevant to new: care planning processes, care recording systems, CCTV, remote care or monitoring systems, and sharing data for research or marketing purposes.

The process is likely to be in your organisation's data protection policy.

### To complete this evidence item

1. Once your organisation is sure that your data protection policy has a process for carrying out a Data Protection Impact Assessment (DPIA), then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

### Support

- A DPIA template and guidance can be found on the ICO website: [bit.ly/DPIAGuide](https://bit.ly/DPIAGuide)
- Video: <https://vimeo.com/654222813> (7:19 minutes)

#### Evidence item 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?**

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 \(ICO\)](#).

Comments (optional)

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



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?

## BYO Device

**Overview:** Your organisation needs a policy to cover 'bring your own device' if staff use their own devices for work purposes, and it needs to demonstrate how the policy is enforced.

### Detail

Some care providers allow staff to use their own devices to access and manage data. The devices referred to include anything that can access or store personal data, such as, mobile phones, laptops, tablets, CDs, USB sticks etc. This question applies to staff using their own devices to access your organisation's system(s) whether the person is on duty or not.

### To complete this evidence item

- In the optional comments box:
  - If staff do use their own devices, then write a short statement clarifying that your organisation has a Bring Your Own Device policy and describing how the policy is enforced
  - If nobody uses their own devices, write "Not applicable"
- Click on the box at the top by the title
- Click on the blue 'save' button

### Support

- A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available here: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- Video: <https://vimeo.com/654222813> (10:30 minutes)

#### Evidence item 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?**

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 from [Digital Social Care](#)

#### Comments (optional)

**Save** or Cancel

1.3.12

## How does your organisation make sure that paper records are safe when taken out of the building?

### Keeping Paper Records Safe

**Overview:** Paper records may be taken out of your organisation's building(s), for example, for hospital appointments or visits to people's homes; however, leaving documents in cars, for instance, can be risky.

#### Detail

Your organisation needs to make sure that paper records taken out of the building are kept safe. Your organisation must describe how it makes sure that paper records are kept safe when they leave the building.

#### To complete this evidence item

- If your organisation has:
  - No paper records or they do not leave the building, then write in the text box "Not applicable"
  - Paper records that leave the building, then write in the text box a short statement describing how the records are kept safe when outside the building
- No information is required in the optional comments box
- Click on the blue 'save' button

#### Support

- The Digital Social Care's Data Security Policy has examples of physical controls
- Video: <https://vimeo.com/654222813> (13:33 minutes)

#### Evidence item 1.3.12

#### How does your organisation make sure that paper records are safe when taken out of the building?

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.

Comments (optional)



 or

1.3.13

## Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.

### Preventing Unauthorised Access

**Overview:** Personal data needs to be kept safe through physical control of buildings to stop unauthorised access.

#### Detail

Physical controls that support data protection include:

- lockable doors, windows and cupboards
- clear desk procedure
- security badges, and/or key coded locks, to access secure areas.

Some organisations have more than one building to keep safe and may have different physical controls in each of them.

#### To complete this evidence item

1. Write in the text box a short, high level statement of how your organisation assures compliance across all its sites
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/654222813> (15:02 minutes)

#### Evidence item 1.3.13

#### Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.

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.

Comments (optional)

**Save** or Cancel

1.3.14

## What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?

### Mobile phone risks

**Overview:** Personal data is often stored on mobiles phones, and other mobile devices, which need to be protected to stop personal data from loss, theft, hacking or in appropriate use.

#### Detail

Care providers are increasingly using mobile devices (including smartphones and tablets) to access and manage data for personal care. These devices often leave the organisation's building/s and therefore the safety of a fixed working environment. Your organisation needs to make sure that they are protected.

Your organisation needs to consider what data can be accessed from the devices, how that access is managed and agree on a policy with staff for the use of personal devices for work purposes.

Your organisation may have a policy in place which ensures PIN, fingerprint or a facial scan are on all smartphones to access them, as well as having an app to track the location of a lost or stolen device.

#### To complete this evidence item

- If your organisation has:
  - No mobile phones or devices with personal data on, then write in the text box "Not applicable"
  - Mobile phones and/or devices, then write in the text box a short statement describing what is in place to minimise the risk of the mobile phones and devices being lost, stolen, hacked or used inappropriately
- No information is required in the optional comments box
- Click on the blue 'save' button

#### Support

- Your IT supplier (if your organisation has one) might be able to assist with answering this question.
- Guidance is available from here: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/>
- Video: <https://vimeo.com/654222813> (17:34 minutes)

#### Evidence item 1.3.14

#### What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?

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 from [Digital Social Care](#)

Comments (optional)

**Save** or Cancel

1.4.1

## Does your organisation have a timetable which sets out how long you retain records for?

### Record Retention Timetable

**Overview:** Your organisation needs to have a timetable describing how long records are kept for.

#### Detail

Your organisation needs to 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, must be based on statutory requirements or other guidance.

#### To complete this evidence item

1. Once your organisation is sure that it has a record retention timetable, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- More information on record retention is here: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>
- Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016 contains a spreadsheet of the [detailed retention schedules](#). It sets out how long records need to be retained for, either due to their ongoing administrative value or as a result of statutory requirement.
- Video: <https://vimeo.com/654227822> (0:23 seconds)

#### Evidence item 1.4.1

**Does your organisation have a timetable which sets out how long you retain records for?**

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](#).

Comments (optional)

**Save** or Cancel

## 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 1<sup>st</sup> July 2021? This contract should meet the requirements set out in data protection regulations.**

## Destroying Records Contract

**Overview:** Your organisation must have a written contract that meets data protection regulations with all third-party organisations that destroy personal data on your organisation's behalf.

### Detail

When there is no longer a valid reason to keep personal data (i.e. when the data is outside of the retention period) it's important 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/USB sticks.

If your home uses a contractor to destroy any records or equipment, such as a document shredding or IT recycling company, the relevant contract(s) or other written confirmation, must include the requirement to have appropriate security measures in compliance with the General Data Protection Regulations (GDPR) and the facility to allow audit by your home.

If your home uses a personal shredder, you must conform to the HMG Information Assurance Standard (IS5). The specification of the shredder must be:

- P-4 security level or above
- Heavy duty shredder
- Cross cut or micro cut
- Anti-jam

### To complete this evidence item

1. Once your organisation has confirmed that contracts have been reviewed, then click on the box at the top by the title
2. If your organisation does not use third parties to destroy records or equipment, then write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

### Support

- The Information Commissioner's Office has guidance here: [https://ico.org.uk/media/fororganisations/documents/1475/deleting\\_personal\\_data.pdf](https://ico.org.uk/media/fororganisations/documents/1475/deleting_personal_data.pdf)
- Advice on contracts for secure disposal of personal data is available here: <https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/>
- Your organisation's lead on contracts (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/654227822> (3:12 minutes)

#### Evidence item 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 1<sup>st</sup> July 2021? This contract should meet the requirements set out in data protection regulations.**

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 chapter 5 of 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 from [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

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?

### Destroying Data Safely

**Overview:** It is important that personal data is disposed of securely when there is no longer a valid reason to keep it.

#### Detail

If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, then it needs to be carried out securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and USB/memory sticks.

#### To complete this evidence item

- In the comments box:
  - If your organisation does not destroy personal data, records or equipment, or it only uses a third party to do so, then write "Not applicable"
  - If your organisation does destroy personal data, records or equipment **yourselves**, then briefly describe how the organisation makes sure that this is done securely
- Click on the blue 'save' button

#### Support

- Digital Social Care has a Record Keeping policy that has details on the safe destruction of personal data: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- Video: <https://vimeo.com/654227822> (6:46 minutes)

#### Evidence item 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?

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 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.

Digital Social Care has a Record Keeping policy that has details on the safe destruction of personal data.

Comments (optional)

**Save** or Cancel



2.1.1

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

### Data Security in Staff Induction

**Overview:** All new staff, directors, trustees and volunteers who have access to personal data, need to have an induction that covers data protection and data and cyber security.

#### Detail

Protecting sensitive and confidential information is both a legal requirement and a contractual obligation. Protecting information is a shared responsibility across all staff in your organisation.

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. The induction can be delivered face to face or digitally.

#### To complete this evidence item

1. Once your organisation has an induction process that covers data protection, and data and cyber security, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- There is an 'Introduction to Information Sharing for Staff' available from Digital Social Care: <https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/>
- Your HR support (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/654230540> (0:39 minutes)

#### Evidence item 2.1.1

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

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 from [Digital Social Care](#).

Comments (optional)



 or



2.1.2

# Do all employment contracts, and volunteer agreements, contain data security requirements?

## Data Security in Staff Contracts

**Overview:** All employment contracts, and volunteer and trustee agreements (if applicable), must contain a clause which outlines employee responsibility for data security.

### Detail

Contracts or agreements need to have clauses that 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 your organisation includes them), need to be reviewed to see if they need updating to include a clause on data security. Older contracts of employment may require a contract variation in order to comply with updated data security requirements.

Data security involves:

- Confidentiality - data is not disclosed to people that do not have the right to see it.
- Integrity - all data is accurate and unchanged.
- Availability - data must be accessible to those authorised to see it.

### To complete this evidence item

1. Once your organisation has checked that all employment contracts and agreements contain data security requirements, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button.

### Support

- An example of a staff contract clause is available here: <https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/>
- Your HR support (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/654230540> (2:39 minutes)

### Evidence item 2.1.2

**Do all employment contracts, and volunteer agreements, contain data security requirements?**

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 from [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

3.1.1

## Has a training needs analysis covering data security and protection, and cyber security, been completed since 1<sup>st</sup> July 2021?

### Training Needs Analysis

**Overview:** Your organisation's training needs analysis identifies the level of training, or awareness raising, in data protection and data and cyber security, that is required by your organisation. It needs to be reviewed each year.

#### Detail

A training needs analysis is a process which helps identify the training and development needs across your organisation. Your training needs analysis for data protection, and data and cyber security, identifies the level of training or awareness raising required in these areas by each individual in your organisation, including staff, directors and trustees and volunteers.

It needs to be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation.

Staff requiring a higher level of knowledge around data security and protection than others, because they make decisions about personal information, need to be identified. These roles could include: Data Protection Officer (DPO), Information Governance (IG) lead, data security and protection lead, IT leads, Registered Manager and deputies, quality assurance roles and/or senior management team.

Your organisation needs to consider how training can be tailored for certain groups of staff, for example, those who use personal devices to carry out their work and those whose work is paper based.

#### To complete this evidence item

1. Once your organisation has completed a training needs analysis covering data protection, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button.

#### Support

- Digital Social Care has an example training needs analysis and guidance on how to carry out a training needs analysis for data protection and data and cyber security: <https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/> see: Staff Data and Cyber Security Training Materials
- Your HR support (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/654231923> (0:25 minutes)
- Senior leadership is required for this evidence item

#### Evidence item 3.1.1

**Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?**

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 from [Digital Social Care](#).

Cc    ents (optional)

**Save** or Cancel

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?**

## Staff Training in Data Security

**Overview:** All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year.

### Detail

It might not be possible for 100% of people to receive training every year, due to illness, maternity/paternity leave, attrition or other reasons. Therefore, the target is 95% of people with access to personal data.

Your organisation's training needs analysis identifies the level of training or awareness raising that each person needs. To make sure your organisation stays within the 95% target, records need to be kept of who has completed training on data security and protection, and cyber security, and when it was completed.

### To complete this evidence item

1. Once at least 95% of staff in your organisation have completed training in data protection, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

### Support

- Digital Social Care provides 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/>
- Your HR support (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/654231923> (2:30 minutes)

#### Evidence item 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?**

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.

Digital Social Care provides guidance on training, including sources of free online data and cyber security training.

Comments (optional)

**Save** or Cancel

3.4.1

## Have the people with responsibility of data security and protection received training suitable for their role?

### In-Depth Training for Senior Leaders

**Overview:** The people in your organisation with responsibility for data security and protection are likely to require additional and more in-depth training.

#### Detail

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 identifies any additional training required by people with increased data security and protection responsibilities or specialist roles.

This ensures staff involved in management of the organisation at the highest levels have had suitable training to ensure appropriate data security and protection process, controls, activities etc. are in place.

Free IG training on e-Learning for Healthcare website is available. See the data security awareness programme: <https://www.e-lfh.org.uk/programmes/data-security-awareness/>

Your NHSmail account, as well as being a social care organisation, will give you and your colleagues access to the training. Level 1 is a really good starting point.

Register here: <https://portal.e-lfh.org.uk/Register> and all the programmes will be available to you and your colleagues.

#### To complete this evidence item

1. Once the people with responsibility for data security and protection have received training suitable for their role, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- Your HR support (if your organisation has this) might be able to assist with answering this question
- Digital Social Care provides 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: <https://vimeo.com/654231923> (4:10 minutes)
- Senior leadership is required for this evidence item

#### Evidence item 3.4.1

**Have the people with responsibility for data security and protection received training suitable for their role?**

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).

Comments (optional)

**Save** or Cancel

4.1.1

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

### Record of Staff and Roles

**Overview:** It is important to maintain a record of all current staff and their roles, including any volunteers if your organisation includes them.

#### Detail

Your organisation's record might be linked to the existing payroll or rostering system or training schedule. The record needs to be up to date; detail when staff started their role, any role changes, as well as, when (and if) staff leave the organisation. The record can help keep your organisation's data secure by only allowing employees with the correct clearance access to information.

#### To complete this evidence item

1. Once your organisation has an up to date record of staff, and volunteers (if your organisation includes them) and their roles, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- Your HR support (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/649217784> (0:57 minutes)

#### 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 know who has access to personal and confidential data through its IT system(s)?

### Access to Data

**Overview:** Your organisation needs to know who has access to the personal and confidential data in its IT system(s), including all internal and external staff.

#### Detail

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. External staff may be able to access some data held by your organisation through a rostering system which may, for example, share payroll information.

Your organisation must retain a record of who has access to which system and what level of access they have.

#### To complete this evidence item

1. Once your organisation knows who has access to personal and confidential data through its IT system(s), then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any IT systems, then tick and write "Not applicable" in the optional comments box
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/649217784> (2:16 minutes)

#### Evidence item 4.1.2

**Does your organisation know who has access to personal and confidential data through its IT system(s)?**

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.

Comments (optional)

**Save** or Cancel



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?

### Amending Access to IT Systems

**Overview:** 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).

#### Detail

It's important to have a reliable way to amend or remove access to your IT system(s) when people change roles or leave your organisation. 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, including NHSmail.

#### To complete this evidence item

1. Once your organisation has a reliable way of removing or amending people's access to IT systems when they leave or change roles, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any IT systems, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

#### Support

- Your organisation's IT supplier, if you have one, may help with this question
- For support with NHSmail, get in touch with the NHSmail Helpdesk
- Video: <https://vimeo.com/649218826>

#### Evidence item 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?**

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

Comments (optional)

**Save** or Cancel

4.5.4

## How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?

### Good Password Practice

**Overview:** If your organisation has any IT systems or computers, it needs to provide advice for setting and managing good passwords.

#### Detail

Advice for setting and managing passwords needs to be given to all staff if your organisation has any IT systems or computers. Each staff member needs to have their own strong password which is hard to guess to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords need to be 'strong' i.e. hard to guess.

Did you know that if your password contains letters and is only 8 characters long, it'll take a hacker 14 minutes to guess but if it is 10 characters long and contains lower and upper case letters, numbers and symbols then it would take the hacker 928 years to guess!

The use of good passwords could be enforced through technical controls, such as, setting up your IT system(s) to require a minimum number of characters or a mixture of letters and numbers in a password.

#### To complete this evidence item

- If your organisation does:
  - not use any IT systems, then write in the text box "Not applicable"
  - use IT systems, then write in the text box a short statement about how your organisation makes sure that staff, directors, trustees and volunteers use good password practice. Do not include too much detail by keeping to a high level.
- Click on the blue 'save' button

#### Support

- Information about good password practice is available from Digital Social Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/>

Evidence item 4.5.4

#### How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?

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 from [Digital Social Care](#).

Comments (optional)

**Save** or Cancel



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?

### Reviewing Data Breach Process

**Overview:** Your organisation needs to review processes each year, particularly those processes that could have allowed data protection breaches or near misses to occur.

#### Detail

Your organisation needs to make sure it reviews all processes that have caused a breach or a near miss, and also processes which force people to use unauthorised workarounds that could compromise data and cyber security.

Examples of workarounds include:

- using unauthorised devices such as home computers or personal memory sticks and 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.

#### To complete this evidence item

1. Once your organisation has confirmed that it has reviewed any processes that have caused a breach or a near miss, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation has not had a data breach or near miss in the last year, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/649219311> (0:20 minutes)

#### Evidence item 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?**

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.

Comments (optional)

Save

or Cancel

## Does your organisation have a system in place to report data breaches?

### Data Breach Reporting System

**Overview:** All staff and volunteers (if your organisation has them), are responsible for noticing and reporting data breaches and it is vital that your organisation has a robust reporting system.

#### Detail

Your organisation needs a reporting system to enable the person with responsibility for data security to report data breaches, often referred to as data incidents, immediately it is known that the breach has happened.

There is a data breach incident reporting tool within this toolkit which needs to be used to report health and care data incidents to the Information Commissioner's Office (ICO). If it is not clear whether to inform the ICO of a breach, this toolkit's incident reporting tool and guide can help decide. There is a tab at the top of the assessment page called 'Report an Incident' for reporting data breaches. Once the tool has been used, all relevant bodies like the ICO will be notified if this is necessary.

Examples of incidents include: emailing confidential data to the wrong person; losing a USB memory stick which holds sensitive data, and losing keys to the filing cabinet holding personal data.

#### To complete this evidence item

1. Once your organisation has a system in place to report data breaches, then click on the box at the top by the title
2. No information is required in the optional comments box
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/649220474> (2:00 minutes)

#### Evidence item 6.1.1

**Does your organisation have a system in place to report data breaches?**

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.

Comments (optional)

Save

or Cancel

6.1.3

## 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?

### Reporting Breach to Management

**Overview:** In the event of a data breach your organisation's management team, or equivalent group, needs to be notified of the breach and any associated action plans and lessons learnt.

#### Detail

It is important that the management team, or equivalent group, is notified of all data breaches, and that it approves all the actions planned to minimise the breach happening again, as well as being involved in learning and sharing lessons.

#### To complete this evidence item

1. Once your organisation has confirmed that if there was a data breach, the management team were notified, and approved the actions planned to minimise the risk of a recurrence, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation has not had a data breach or near miss in the last year, then tick and write "Not applicable" in the optional comments box
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/649220474> (3:38 minutes)
- Senior leadership is required for this evidence item

#### Evidence item 6.1.3

- 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?**

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.

Comments (optional)

Save

or Cancel

6.1.4

## If your organisation has had a data breach, were all individuals who were affected informed?

### Informing Individuals of a Data Breach

**Overview:** If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then it needs to inform those individuals promptly.

#### Detail

Your organisation will need to assess the severity and impact on individuals as a result of the breach and the likelihood of this occurring. If the impacted breach is more severe, the risk is higher. If the likelihood of the consequences is greater, the risk is higher. In such cases, your organisation will need to promptly inform those impacted.

Examples of high risk data breaches include: damage to reputation, financial loss, unfair discrimination, negative or harmful impacts on an individual or individuals or other significant loss.

#### To complete this evidence item

1. Once your organisation has confirmed that, if there was a data breach, all individuals who were affected had been informed, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation has not had a data breach in the last year, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

#### Support

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

#### Evidence item 6.1.4

- If your organisation has had a data breach, were all individuals who were affected informed?**

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](#).

Comments (optional)

**Save** or Cancel

6.2.1

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

## Antivirus and Antimalware Software

**Overview:** Your organisation needs to make sure it has antivirus/antimalware software on all its IT equipment and that it is up to date.

### Detail

All IT equipment includes all servers, desktop computers, laptop computers, and tablets.

Note: antivirus software and antimalware software are the same as they perform the same function of preventing viruses and malicious software from attacking the IT equipment and systems.

### Support

- Your organisation’s IT supplier (if your organisation has one) may be able to check there is antivirus/antimalware software on your IT systems and that it is kept up to date
- Further information is available from Digital Social Care <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/>
- Video: <https://vimeo.com/453937047> (

### To complete this evidence item

1. Once your organisation has confirmed that all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any computers or other devices, then tick and write “Not applicable” in the optional comments box.
3. Click on the blue ‘save’ button

### Evidence item 6.2.1

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

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 from [Digital Social Care](#).

Comments (optional)

or

6.3.2

## Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?

### Unsafe Access to Public Wi-Fi

**Overview:** Your organisation needs to advise staff, directors, trustees and volunteers (if your organisation has them) that using public Wi-Fi for work purposes is unsafe.

#### Detail

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. Your organisation needs to advise staff, directors, trustees and volunteers (if your organisation includes them), that public Wi-Fi or unsecured Wi-Fi could be unsafe and lead to unauthorised access of personal data.

#### To complete this evidence item

1. Once your organisation has confirmed that all staff have been informed that public Wi-Fi is unsafe, then click on the box at the top by the title. Do not write in the optional comments box.
2. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/649222262> (0:17 minutes)

#### Evidence item 6.3.2

**Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?**

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.

Comments (optional)

**Save** or Cancel

7.1.2

## Does your organisation have a business continuity plan that covers data and cyber security?

### Business Continuity Plan

**Overview:** Your organisation needs to have a business continuity plan that includes data and cyber security.

#### Detail

Your organisation's business continuity plan needs to describe well defined processes to ensure the security of all your services in the event of a data security incident, failure or compromise. For example, how would service continue if: there was a power cut; the phone line and/or internet went down; your IT system was hacked; a computer broke down; the office became unavailable (e.g. through fire).

#### To complete this evidence item

1. Once your organisation has a business continuity plan that covers data and cyber security, then click on the box at the top by the title
2. Do not write in the optional comments box
3. Click on the blue 'save' button

#### Support

- An example business continuity plan is available from Digital Social Care: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- Video: <https://vimeo.com/453941378> (0:14 minutes)

#### Evidence item 7.1.2

- Does your organisation have a business continuity plan that covers data and cyber security?**

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 from [Digital Social Care](#).

Comments (optional)

**Save** or Cancel



7.2.1

## How does your organisation test the data and cyber security aspects of its business continuity plan?

### Testing the Business Continuity Plan

**Overview:** In order to know how well the data and cyber security aspects of the business continuity plan work, they need to be tested.

#### Detail

Your organisation must test the data and cyber security aspects of its business continuity plan each year. How this is done can be through a discussion with staff on what needs to happen if a specified incident on the plan occurred.

#### To complete this evidence item

1. Write in the text box a description of how your organisation tests the data and cyber security aspects of its business continuity plan, and what the outcomes were from the last test
2. Do not write in the optional comments box
3. Click on the blue 'save' button

#### Support

- Guidance for testing your business continuity plan for the data and cyber security aspects is available from Digital Social Care: <https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>
- Video: <https://vimeo.com/453943930> (0:30 minutes)

#### Evidence item 7.2.1

#### How does your organisation test the data and cyber security aspects of its business continuity plan?

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 since 1st July 2021.

Guidance for testing your business continuity plan for the data and cyber security aspects is available from [Digital Social Care](#).

Comments (optional)



or



7.3.1

## How does your organisation make sure that there are working backups of all important data and information?

### Regular Backups of Data

**Overview:** It is important to ensure backups are done regularly, that they are successful and that they include the right files and systems.

#### Detail

Access to devices is restricted if it is infected by a virus or the data may be damaged, deleted, stolen, or held to ransom if a criminal is involved. This is why it's important to make sure your organisation has backups of all important data and information somewhere that is separate from your computer such as an external hard drive or cloud.

#### To complete this evidence item

1. Write in the text box a description of how your organisation's backup systems work and how they have been tested. Do not write in the optional comments box.
2. If your organisation does not use any computers or IT systems, write "Not applicable" in the optional comments box
3. Click on the blue 'save' button

#### Support

- Your organisation's IT supplier, if you have one, may help with this question
- Advice about backups is available Digital Social Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/back-up-your-data/>
- Video: <https://vimeo.com/654232639> (0:29 minutes)

#### Evidence item 7.3.1

#### How does your organisation make sure that there are working backups of all important data and information?

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 [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

## All emergency contacts are kept securely, in hardcopy and are up-to-date.

### Emergency Contacts

**Overview:** Your organisation needs to have a hard copy list of emergency contacts that is kept up to date and secure and includes who to contact in the event of a data security incident.

#### Detail

It's important that emergency contacts are kept up to date and therefore are reviewed regularly to check changes in roles, contact numbers and emails.

Include all contact details such mobile number, landline number, email and how to make contact inside and outside of business hours.

#### To complete this evidence item

1. Once your organisation has a hard and electronic copy of up-to-date emergency contacts, then click on the box at the top by the title
2. Do not write in the optional comments box
3. Click on the blue 'save' button

#### Support

- Video: <https://vimeo.com/654232639> (1:57 minutes)

Evidence item 7.3.2

**All emergency contacts are kept securely, in hardcopy and are up-to-date.**

Contacts include phone number as well as email.

Comments (optional)

**Save** or Cancel

7.3.4

# Are backups routinely tested to make sure that data and information can be restored?

## Testing Backups

**Overview:** Your organisation's backups are to be tested annually to make sure data and information can be restored in case there are issues with the backup system.

### Detail

When there are issues with equipment, such as breakdown, the data and information can be hard to access, and in some cases, impossible to access. The backups must be tested to make sure that these do not go wrong, and your organisation knows how to restore the data and information quickly in an emergency.

### To complete this evidence item

1. Once your organisation's backups are routinely tested to make sure that data and information can be restored, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any computers or IT systems, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

### Support

- Your organisation's IT supplier, if you have one, may help with this question

Video: <https://vimeo.com/654232639> (3:57 minutes)

### Evidence item 7.3.4

**Are backups routinely tested to make sure that data and information can be restored?**

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.

Comments (optional)

**Save** or Cancel

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?

### Unsupported Software

**Overview:** 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.

#### Detail

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 electronic rostering, care planning, or medicine administration record (MAR) charts.

#### To complete this evidence item

1. Once all the IT systems and the software used in your organisation are either still supported by the manufacturer or the risks are understood and managed, then click on the box at the top by the title. Do not write in the optional comments box
2. If your organisation does not use any IT systems or software, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

#### Support

- Your organisation's IT supplier (if you have one) may help with this question
- For guidance (including information on how to check which software versions your organisation has), refer to Social Digital Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/>

#### Evidence item 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?**

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 [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

8.2.1

If your answer to 8.1.4 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.

## Managing Risk of Unsupported Software

**Overview:** If your organisation has unsupported systems, there must be a decision to accept and manage the associated risks.

### Detail

Your organisation's board or management team will have formally considered the risks of continuing to use unsupported items and have concluded the risks are acceptable. The risk assessment and conclusion needs to be documented.

### To complete this evidence item

- To provide the document, choose the option that is most suitable:
  - Upload a document
  - Reference an existing uploaded document
  - Specify an intranet or internet link to a document
  - Enter text describing the document's location
- Follow the instructions for that option. It is easiest to use the last option and state where the document is, for example, in the DSPT folder on the manager's computer.
- If your answer to the previous question (8.1.4) was Yes, then write "Not applicable" in the text box
- No information is required in the optional comments box
- Click on the blue 'save' button

### Support

- Your organisation's IT supplier (if your organisation has one) may help with this question
- Senior leadership is required for this evidence item

### Evidence item 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.**

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".

- [Upload a document](#)
- [Reference an existing uploaded document](#)
- [Specify an intranet or internet link to a document](#)
- [Enter text describing the document's location](#)

Comments (optional)

**Save** or Cancel

8.3.5

# How does your organisation make sure that the latest software updates are downloaded and installed?

## Software Updates

**Overview:** Your organisation's IT system(s) and devices need to have the latest software and application updates installed.

### Detail

Most software can be set to apply automatic updates when they become available from the manufacturer. Your organisation can schedule software updates in computers' settings so that they occur at convenient times. It's important to check the results of an automatic update to ensure it's been completed on all computers. This can be done using a vulnerability scanner.

The policy around frequency of software updates needs to be recorded.

### To complete this evidence item

1. Write in the text box how your organisation makes sure that the latest software updates are downloaded and installed.
2. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box.
3. No information is required in the optional comments box
4. Click on the blue 'save' button

### Support

- Your organisation's IT supplier (if your organisation has one) may help with this question
- Further information is available from Digital Social Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/>
- Video: <https://vimeo.com/649222683> (0:15 minutes)

### Evidence item 8.3.5

#### How does your organisation make sure that the latest software updates are downloaded and installed?

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 [Digital Social Care](#).

Comments (optional)



or

9.1.1

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

## Networking Components Passwords

**Overview:** All original passwords that come with your networking components need to be changed, including the 'admin' passwords.

### Detail

Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. They may come with default passwords which could be known by third parties which leads to security vulnerability.

### To complete this evidence item

1. Once your organisation makes sure that passwords of all networking components have been changed from their original passwords, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button
4. Click on the white box next to 'I confirm that the evidence entered for this assertion is correct'

### Support

- Your organisation's IT supplier (if your organisation has one) may help with this question
- If you still have the box your router came in, this will tell you how to change your WiFi password
- Video: <https://vimeo.com/454008253>

#### Evidence item 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?**

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.

Comments (optional)



 or



9.5.2

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

## Encryption of Transportable Devices

**Overview:** Your organisation needs to make sure that all transportable devices containing personal data are encrypted to keep data secure and protected.

### Detail

Mobile computers, like laptops and tablets, and removable devices, like memory sticks/cards/CDs, are vulnerable as they can be lost or stolen. They all can be encrypted to make these devices difficult to get into. Encrypting protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people.

Computers, laptops and other devices can be further protected by preventing the use of removable devices like memory sticks being inserted. This is called computer port control.

### To complete this evidence item

1. Once all laptops and tablets or removable devices that hold or allow access to personal data are encrypted, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

### Support

- 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/>
- Your organisation's IT supplier (if your organisation has one) may help with this question
- Video: <https://vimeo.com/654233192> (0:18 minutes)

### Evidence item 9.5.2

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

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 [Digital Social Care](#).

Comments (optional)

**Save** or Cancel



**Overview:** Your organisation’s list needs to include the supplier name, the product type and services they provide and their contact details.

## List of Suppliers

### Detail

Being a desirable, trustworthy organisation or supplier includes observing good practice and compliance when it comes to cyber and information security. If good practice is not followed, it may not only place your own organisation at risk but also others within the ‘supply chain’.

Your organisation’s list of external suppliers that handle personal information could include services such as: IT or care planning systems suppliers, IT support, accountancy, DBS checks, and HR and payroll services. The list does not include NHS organisations or Local Authorities.

### Support

- An example of a template can be found from Digital Social Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/>
- Information of supply chain security guidance can be found on: <https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security>
- Your organisation’s lead on contracts (if your organisation has this) might be able to assist with answering this question
- Video: <https://vimeo.com/649223278> (0:34 minutes)

### To complete this evidence item

1. Once your organisation has a list of its suppliers that handle personal information, the products and services they deliver and their contact details, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not have any such suppliers, then tick and write “Not applicable” in the optional comments box.
3. Click on the blue ‘save’ button

#### Evidence item 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?**

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 [Digital Social Care](#).

Comments (optional)

**Save** or Cancel

10.2.1

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

## Cyber Security Certification

**Overview:** If your organisation uses IT services, then any supplier of IT must have cyber security certification.

### Detail

IT systems suppliers include those providing electronic rostering, care planning, and medication administration records/charts, for example.

There are a number of ways for your organisation's IT system suppliers to demonstrate that they have cyber security certification:

- Having a [Cyber Essentials](#) certificate
- Have an ISO27001 certificate
- Being listed on the Digital marketplace  
<https://www.digitalmarketplace.service.gov.uk/>
- Completing the DSPT

### To complete this evidence item

1. Once all your organisation's IT systems suppliers have cyber security certification, then click on the box at the top by the title. Do not write in the optional comments box.
2. If your organisation does not use any IT systems, then tick and write "Not applicable" in the optional comments box.
3. Click on the blue 'save' button

### Support

- Guidance is available from Digital Social Care:  
<https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/>
- More information on Cyber Essentials certificate can be found on <https://www.ncsc.gov.uk/section/products-services/cyber-essentials>
- Video: <https://vimeo.com/654233438> (0:10 minutes)
- Your organisation's IT supplier (if your organisation has one) may help with this question
- Your organisation's lead on contracts (if your organisation has this) might be able to assist with answering this question

#### Evidence item 10.2.1

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

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 Digital marketplace, 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 from [Digital Social Care](#).

Comments (optional)

Save or Cancel



## 6. Appendices

This section describes where to find help and includes a checklist to tick off.

It contains:

Page

- 76 Help and Support
- 77 Evidence Item Checklist

## ***There is always someone to help. Please get in touch if you get stuck***

The Digital Social Care Team have set up a helpline for the duration of the Covid-19 crisis. Call them on 0208 133 3430 (Mon-Fri 9am – 5pm) or email [help@digitalsocialcare.co.uk](mailto:help@digitalsocialcare.co.uk) for free support

# Help and Support

- Register <https://www.dsptoolkit.nhs.uk/Account/Register>
- FAQs for all organisations, including training tool <https://www.dsptoolkit.nhs.uk/News/9>
- ODS and DSPT support **0300 303 4034** [Exeter.helpdesk@nhs.net](mailto:Exeter.helpdesk@nhs.net)
- ODS Portal <https://odsportal.digital.nhs.uk>
- Toolkit training and update events <https://www.dsptoolkit.nhs.uk/News/40>
- Digital Social Care <https://www.digitalsocialcare.co.uk/>
- Find your local support from Better Security, Better Care: <https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/better-security-better-care/better-security-better-care-local-support/>
- Latest guidance and templates <https://www.digitalsocialcare.co.uk/latest-guidance/>
- ICO DPIA guidance - <http://bit.ly/ICODPIAguide>
- Government advice for CCTV - <https://www.gov.uk/government/organisations/surveillance-camera-commissioner>
- DPIA for surveillance cameras - <https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras>

If there is anything you don't understand you can look it up in the 'Digital Signposting Glossary'.

<https://www.digitalsocialcare.co.uk/glossary/>

The Glossary is a compilation of entries to help explain digital terms used on the Digital Social Care website and elsewhere. At the end of the glossary there is a list of related health and social care organisations and what they do. Click on 'Z' to find out more.

# Evidence Item Checklist

Use this page to check off each item as you complete them as an easy way of keeping track of your progress!

1.1.1	3.2.1	3.4.1	8.2.1	8.3.5
1.1.2	3.1.1	4.1.1	8.1.4	9.1.1
1.1.5	2.1.2	4.1.2	7.3.4	9.5.2
1.2.1	2.1.1	4.2.4	7.3.2	10.1.2
1.2.4	1.4.3	4.5.4	7.3.1	10.2.1
1.3.1	1.4.2	5.1.1	7.2.1	<b>Publish Standards Met Assessment</b>
1.3.2	1.4.1	6.1.1	7.1.2	<b>Very Well Done</b> ★
1.3.7	1.3.14	6.1.3	6.3.2	★ <b>Get in touch for support to access data sharing systems</b> ✓
1.3.8	1.3.13	6.1.4	6.2.1	
1.3.11	1.3.12			