Data Security and Protection Toolkit: 'Standards Met' Guidance for Social Care Providers

Contents

Version 7 – December 2020

Introduction

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

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

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

Who needs to complete the DSPT?

All adult social care services in England, including residential and nursing homes, supported living, homecare, extra care, shared lives and day services, are strongly recommended to complete the DSPT. It is increasingly what local authorities and CCGs will expect to see.

If you use NHSmail, there is a requirement for you to register with the DSPT now. If you don't register with the DSPT, then at some point in the future, you may no longer be able to use NHSmail.

You'll need to complete the DSPT before your service can be part of any of the projects and initiatives that allow care services to directly access NHS patient information systems, for example, GP records and shared care records.

If you have services funded by the NHS, for example under continuing healthcare, there is a contractual requirement to complete the DSPT every year.

You don't need to have completed or to register with the DSPT just to have video appointments with NHS services, but it is strongly recommended.

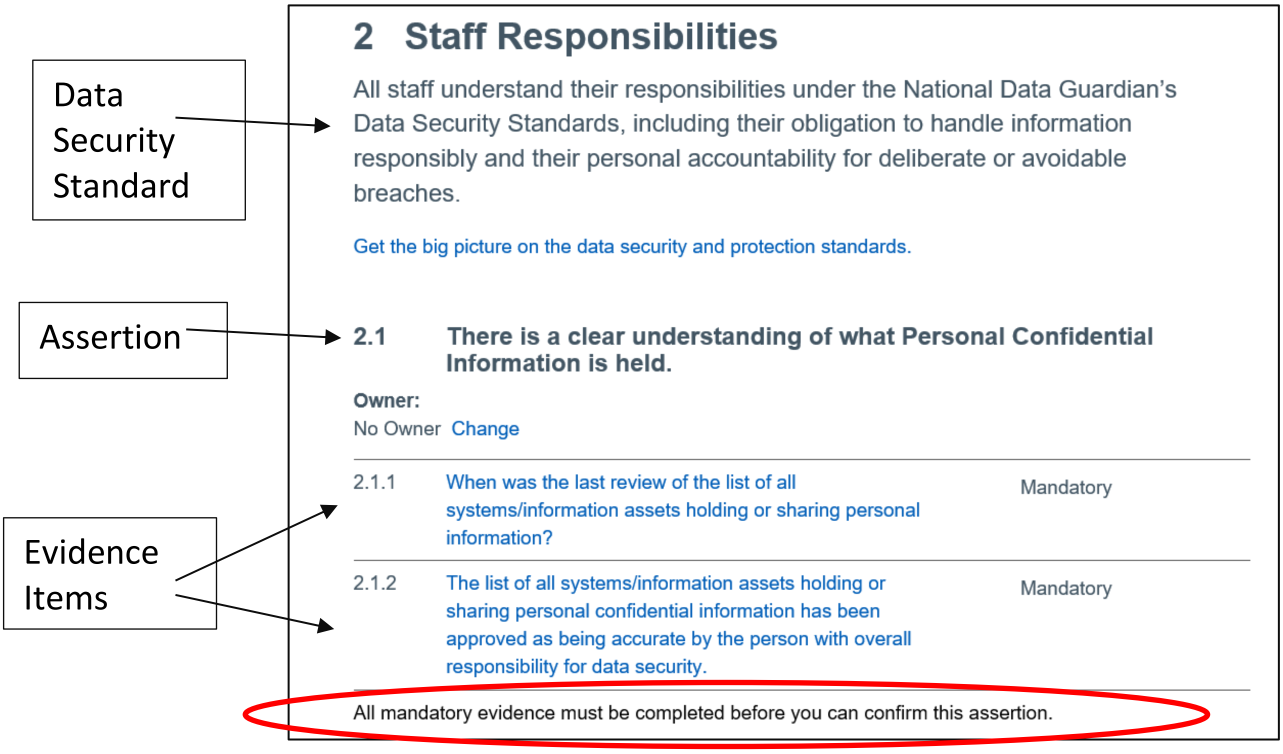
Completing your Assessment

INTRODUCTION

The DSPT is organised under the ten data security standards. Under each standard there are a number of “assertions” which you will need to work through.

To complete each assertion, you are required to provide evidence items which demonstrate compliance with the assertion.

To achieve ‘standards met’, you must complete all mandatory evidence items.



2 Staff Responsibilities

All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Get the big picture on the data security and protection standards.

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

Owner:
No Owner Change

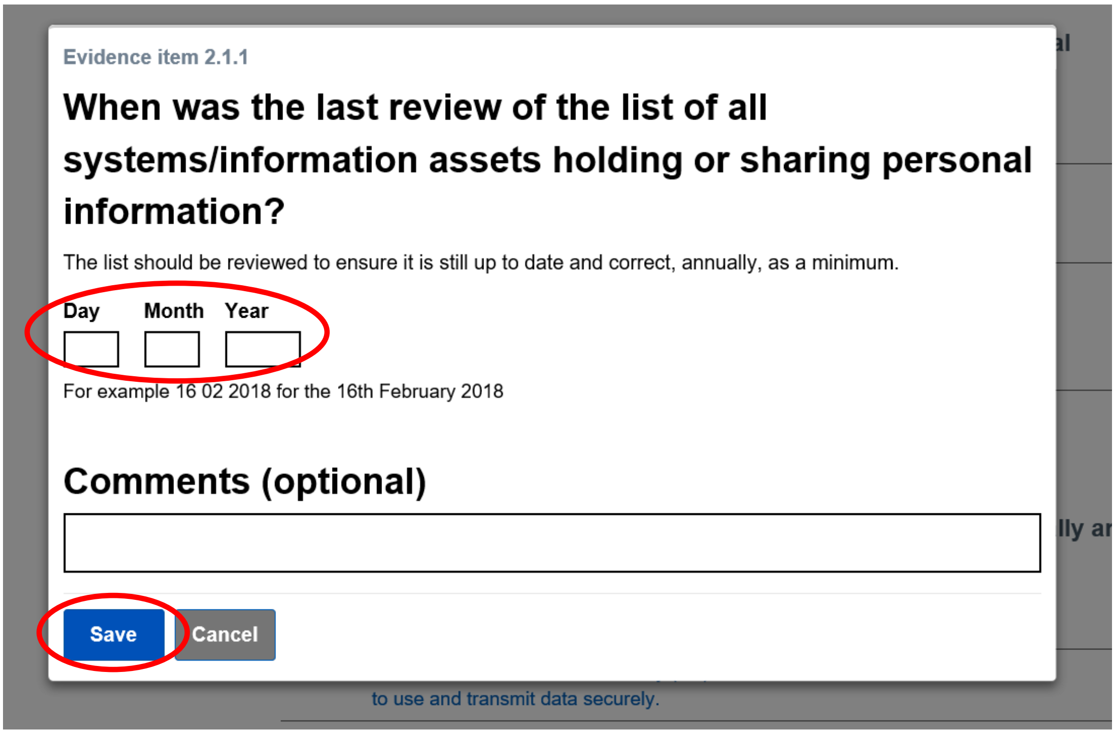
2.1.1	When was the last review of the list of all systems/information assets holding or sharing personal information?	Mandatory
2.1.2	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility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

All mandatory evidence must be completed before you can confirm this assertion.

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

HOW TO COMPLETE AN EVIDENCE ITEM

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



Evidence item 2.1.1

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

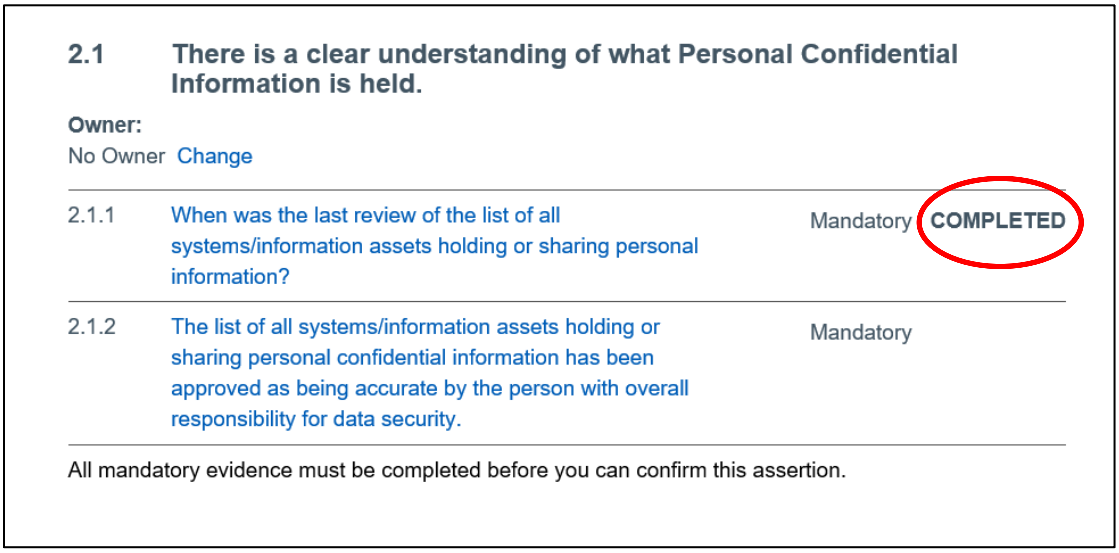
The list should be reviewed to ensure it is still up to date and correct, annually, as a minimum.

For example 16 02 2018 for the 16th February 2018

Comments (optional)

In this example, just enter the date.

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



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

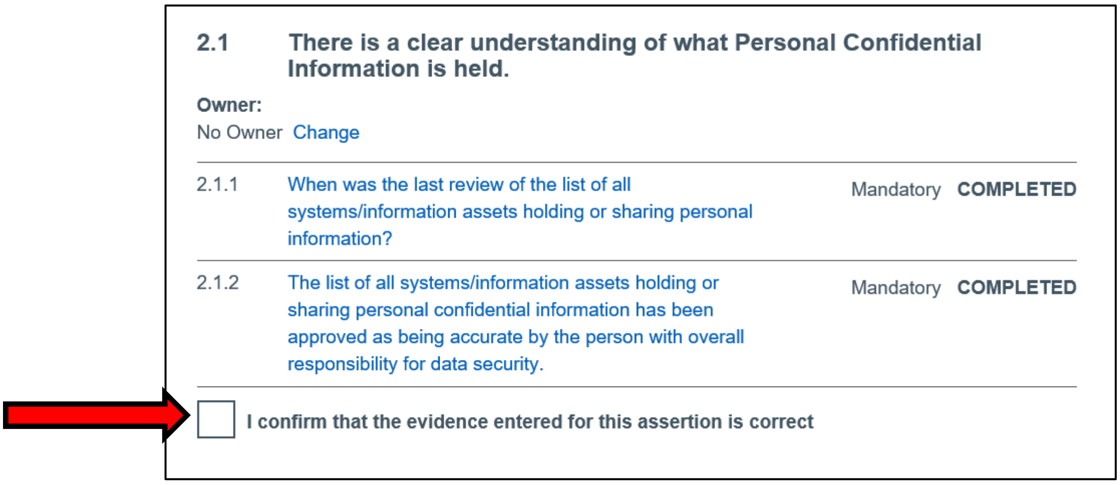
Owner:
No Owner Change

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	

All mandatory evidence must be completed before you can confirm this assertion.

HOW TO COMPLETE AN ASSERTION

To complete an assertion, complete all mandatory evidence items for that assertion. Once this is done, a tick box will appear at the bottom of the page.



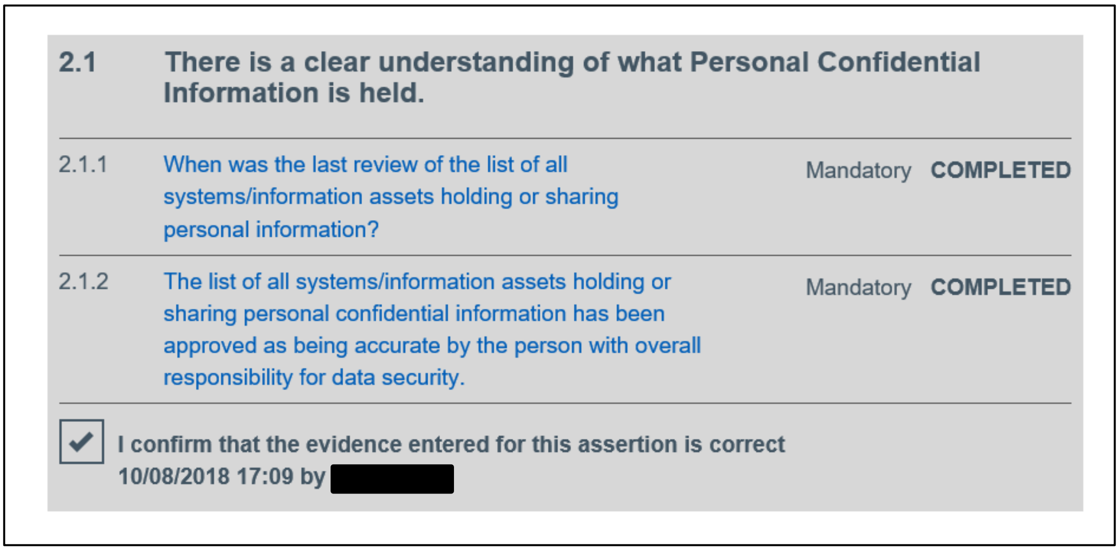
2.1 There is a clear understanding of what Personal Confidential Information is held.

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**

If you select this box, the assertion is marked as complete and turns grey. You can click the box again to unmark it if you need to make any changes.



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]

The following sections describe all the mandatory evidence items in detail, with advice on how to complete them, plus links to a range of relevant resources.

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

1.1. THERE IS SENIOR OWNERSHIP OF DATA SECURITY AND PROTECTION WITHIN THE ORGANISATION.

1.1.2 Who has responsibility for data security and protection and how has this responsibility been formally assigned?	
Tool Tip	Whilst data security and protection are 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 in https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/.
Video Guide	https://vimeo.com/digitalsocialcare/11

1.2. THERE ARE CLEAR DATA SECURITY AND PROTECTION POLICIES IN PLACE AND THESE ARE UNDERSTOOD BY STAFF AND AVAILABLE TO THE PUBLIC.

1.2.1 Does your organisation have up to date policies in place for data protection and for data and cyber security?	
Tool Tip	Confirm that your organisation has a policy or policies in place to cover: • data protection • data quality

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

1.3. INDIVIDUALS' RIGHTS ARE RESPECTED AND SUPPORTED (GDPR ARTICLE 12-22).

1.3.1 What is your organisation's Information Commissioner's Office (ICO) registration number?	
Tool Tip	Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should register as a matter of urgency using the following link https://ico.org.uk/for-organisations/data-protection-fee/. You can check whether you are registered and what your ICO registration number is on the Information Commissioner's Office website https://ico.org.uk/esdwebpages/search
Video Guide	https://vimeo.com/digitalsocialcare/13

1.3.2 Does your organisation have a privacy notice(s)?	
Tool Tip	Your organisation must set out in clear and easily understood language what it does with the personal data it processes regarding the people it supports, staff and volunteers, and members of the public, for example relatives or other professionals etc. This is called a privacy notice and there may be more than one privacy

	notice e.g. one notice for staff and one for the people you support. Your organisation's privacy notice(s) should be made available to these people and inform them about their rights under data protection legislation and how to exercise them. It is good practice to publish your privacy notice on your website if you have one. An example privacy notice is available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/
Video Guide	https://vimeo.com/digitalsocialcare/13

1.4. RECORDS OF PROCESSING ACTIVITIES ARE DOCUMENTED FOR ALL USES AND FLOWS OF PERSONAL INFORMATION (GDPR ARTICLE 30 AND DATA PROTECTION BILL 2017 SCHEDULE 1 PART 4).

1.4.1 Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	
Tool Tip	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent within the last 12 months. 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 https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/
Video Guide	https://vimeo.com/digitalsocialcare/14

1.4.4 Is your organisation compliant with the national data opt-out policy?	
Tool Tip	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 31 March 2021. If you are not CQC registered the below link gives advice. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out and Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-data-opt-out/
Video Guide	https://vimeo.com/digitalsocialcare/14

1.5. PERSONAL INFORMATION IS USED AND SHARED LAWFULLY.

1.5.2 Does your organisation carry out regular data protection spot checks?	
Tool Tip	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download from Digital Social Care: https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/.
Video Guide	https://vimeo.com/digitalsocialcare/15

1.6. THE USE OF PERSONAL INFORMATION IS SUBJECT TO DATA PROTECTION BY DESIGN AND BY DEFAULT

1.6.1 Does your organisation's data protection policy describe how you keep personal data safe and secure?	
Tool Tip	Your policy should describe how your organisation keeps personal data as safe as possible. It should set out, for example: how you might use codes instead of names when sharing data with others; how you might secure or encrypt messages so that only authorised people can read them. This is called 'data protection by design'. Your policy should also set out, for example: how you only collect the minimum amount of data that you need, how you limit access to only those who need to know, keep the data for as short a 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 https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/.
Video Guide	https://vimeo.com/digitalsocialcare/16

1.6.2 How does your organisation make sure that paper records are safe when taken out of the building?	
Tool Tip	Paper records may be taken out of your organisation's building(s), for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when 'on the move'? If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.
Video Guide	https://vimeo.com/digitalsocialcare/16

1.6.3 Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.	
Tool Tip	Physical controls that support data protection include lockable doors,

	windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your organisation's sites.
Video Guide	https://vimeo.com/digitalsocialcare/16

1.6.4 What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	
Tool Tip	Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile phones, write "Not applicable" in the text box. Guidance is available from Digital Social Care: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/
Video Guide	https://vimeo.com/digitalsocialcare/16

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

	Guidance.
Video Guide	https://vimeo.com/digitalsocialcare/16

1.6.6 If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	
Tool Tip	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, write "Not applicable" in "Enter text describing document location". A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from Digital Social Care: https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/
Video Guide	https://vimeo.com/digitalsocialcare/16

1.7. EFFECTIVE DATA QUALITY CONTROLS ARE IN PLACE AND RECORDS ARE MAINTAINED APPROPRIATELY.

1.7.2 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 within the last 12 months? This contract should meet the requirements set out in data protection regulations.	
Tool Tip	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If your organisation uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organisation, then the contract(s) or other written confirmation with third parties must include the requirement to have appropriate security measures in compliance with the General Data Protection Regulations (GDPR) and the facility to allow audit by your organisation. Details are available from the ICO.

	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: https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/
Video Guide	https://vimeo.com/digitalsocialcare/17

1.7.3 If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	
Tool Tip	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old compute and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write “Not applicable” in the text box. 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 Guide	https://vimeo.com/digitalsocialcare/17

1.7.4 Does your organisation have a timetable which sets out how long you retain records for?	
Tool Tip	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on statutory requirements or other guidance.
Video Guide	https://vimeo.com/digitalsocialcare/17

1.8. THERE IS A CLEAR UNDERSTANDING AND MANAGEMENT OF THE IDENTIFIED AND SIGNIFICANT RISKS TO SENSITIVE INFORMATION AND SERVICES

1.8.3 What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	
Tool Tip	All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk.
Video Guide	https://vimeo.com/digitalsocialcare/18

STANDARD TWO: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

2.2. STAFF ARE SUPPORTED IN UNDERSTANDING THEIR OBLIGATIONS UNDER THE NATIONAL DATA GUARDIAN'S DATA SECURITY STANDARDS

2.2.1 Does your organisation have an induction process that covers data security and protection, and cyber security?	
Tool Tip	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date. There is an 'Introduction to Information Sharing for Staff' available from Digital Social Care: https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/
Video Guide	https://vimeo.com/digitalsocialcare/22

2.2.2 Do all employment contracts, and volunteer agreements, contain data security requirements?	
Tool Tip	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security. There is an example staff contract clause available from Digital Social Care: https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/
Video Guide	https://vimeo.com/digitalsocialcare/22

STANDARD THREE: All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

3.1. THERE HAS BEEN AN ASSESSMENT OF DATA SECURITY AND PROTECTION TRAINING NEEDS ACROSS THE ORGANISATION.

3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed in the last 12 months?	
Tool Tip	A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation. Your organisation's training needs analysis should identify the level of training or awareness raising required by your staff, directors, trustees and volunteers if you have them. It should be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation. An example training needs analysis is available to download from Digital Social Care
Video Guide	https://vimeo.com/digitalsocialcare/31

3.2. STAFF PASS THE DATA SECURITY AND PROTECTION MANDATORY TEST.

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, within the last 12 months?	
Tool Tip	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data. 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 Guide	https://vimeo.com/digitalsocialcare/32

3.4. LEADERS AND BOARD MEMBERS RECEIVE SUITABLE DATA PROTECTION AND SECURITY TRAINING.

3.4.1 Have the people with responsibility for data security and protection received training suitable for their role?	
Tool Tip	It is likely that the person or people within your organisation who are responsible for data security and protection will need additional and more in depth training than the majority of your staff. Your organisation's training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).
Video Guide	https://vimeo.com/digitalsocialcare/34

STANDARD FOUR: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

4.1. THE ORGANISATION MAINTAINS A CURRENT RECORD OF STAFF AND THEIR ROLES.

4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	
Tool Tip	Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.
Video Guide	https://vimeo.com/digitalsocialcare/41

4.1.2 Does your organisation know who has access to personal and confidential data through its IT system(s)?	
Tool Tip	Your organisation should know who has access to the personal and confidential data in its IT system(s). Each person needs to have their own account to access a system. If that is not currently possible, and users share a login, the organisation must risk assess the situation and agree a plan to end the use of shared logins. If your organisation does not use any IT systems, then tick and write “Not applicable” in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/41

4.2. ORGANISATION ASSURES GOOD MANAGEMENT AND MAINTENANCE OF IDENTITY AND ACCESS CONTROL FOR IT'S NETWORKS AND INFORMATION SYSTEMS.

4.2.5 Does your organisation have a reliable way of removing or amending people’s access to IT systems when they leave or change roles?	
Tool Tip	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people’s access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and

	procedures. This includes access to shared email addresses. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box
Video Guide	https://vimeo.com/digitalsocialcare/42

4.3. ALL STAFF UNDERSTAND THAT THEIR ACTIVITIES ON IT SYSTEMS WILL BE MONITORED AND RECORDED FOR SECURITY PURPOSES.

4.3.1 Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?	
Tool Tip	The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/43

4.5. YOU ENSURE YOUR PASSWORDS ARE SUITABLE FOR THE INFORMATION YOU ARE PROTECTING

4.5.4 How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	
Tool Tip	If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password. If your organisation does not use any IT systems, computers or other

	devices, write “Not applicable” in the text box. Information about good password practice is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/
Video Guide	

STANDARD FIVE: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

5.1. PROCESS REVIEWS ARE HELD AT LEAST ONCE PER YEAR.

5.1.1 If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	
Tool Tip	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/51

STANDARD SIX: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

6.1. A CONFIDENTIAL SYSTEM FOR REPORTING SECURITY BREACHES AND NEAR MISSES IS IN PLACE AND ACTIVELY USED.

6.1.1 A data security and protection breach reporting system is in place.	
Tool Tip	All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner's Office ICO. If you are not sure whether or not to inform the Information Commissioner's Office of a breach, the toolkit's incident reporting tool and guide can help you to decide.
Video Guide	https://vimeo.com/digitalsocialcare/61

6.1.4 If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	
Tool Tip	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/61

6.1.5 If your organisation has had a data breach, were all individuals who were affected informed?	
Tool Tip	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then

	please tick and write "Not applicable" in the comments box. More information is available from the Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/personal-data-breaches/
Video Guide	https://vimeo.com/digitalsocialcare/61

6.2. ALL USER DEVICES ARE SUBJECT TO ANTI-VIRUS PROTECTIONS WHILE EMAIL SERVICES BENEFIT FROM SPAM FILTERING DEPLOYED AT THE CORPORATE GATEWAY.

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

6.3. KNOWN VULNERABILITIES ARE ACTED ON BASED ON ADVICE FROM CARECERT, AND LESSONS ARE LEARNED FROM PREVIOUS INCIDENTS AND NEAR MISSES.

6.3.2 Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?	
Tool Tip	Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/63

STANDARD SEVEN: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

7.1. ORGANISATIONS HAVE A DEFINED, PLANNED AND COMMUNICATED RESPONSE TO DATA SECURITY INCIDENTS THAT IMPACT SENSITIVE INFORMATION OR KEY OPERATIONAL SERVICES.

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

7.2. THERE IS AN EFFECTIVE TEST OF THE CONTINUITY PLAN AND DISASTER RECOVERY PLAN FOR DATA SECURITY INCIDENTS.

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

7.3. YOU HAVE THE CAPABILITY TO ENACT YOUR INCIDENT RESPONSE PLAN, INCLUDING EFFECTIVE LIMITATION OF IMPACT ON YOUR ESSENTIAL SERVICE. DURING AN INCIDENT, YOU HAVE ACCESS TO TIMELY INFORMATION ON WHICH TO BASE YOUR RESPONSE DECISIONS.

7.3.1 How does your organisation make sure that there are working backups of all important data and information?	
Tool Tip	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write "Not applicable" in the text box. For advice about backups, see Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/back-up-your-data/
Video Guide	https://vimeo.com/digitalsocialcare/73

7.3.2 All emergency contacts are kept securely, in hardcopy and are up-to-date.	
Tool Tip	Contacts include phone number as well as email.
Video Guide	https://vimeo.com/digitalsocialcare/73

7.3.4 Are backups routinely tested to make sure that data and information can be restored?	
Tool Tip	It is important that your organisation's backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, then tick and write "Not applicable" in the comments box.
Video Guide	https://vimeo.com/digitalsocialcare/73

STANDARD EIGHT: No unsupported operating systems, software or internet browsers are used within the IT estate.

8.1. ALL SOFTWARE HAS BEEN SURVEYED TO UNDERSTAND IF IT IS SUPPORTED AND UP TO DATE.

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

8.2. UNSUPPORTED SOFTWARE IS CATEGORISED AND DOCUMENTED, AND DATA SECURITY RISKS ARE IDENTIFIED AND MANAGED.

8.2.4 If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.	
Tool Tip	This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are

	acceptable. If your answer to the previous question was yes, write “Not applicable” in “Enter text describing document location”.
Video Guide	https://vimeo.com/digitalsocialcare/82

8.3. SUPPORTED SYSTEMS ARE KEPT UP-TO-DATE WITH THE LATEST SECURITY PATCHES.

8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed?	
Tool Tip	It is important that your organisation’s IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write “Not applicable” in the text box. Further information is available from https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/
Video Guide	https://vimeo.com/digitalsocialcare/83

STANDARD NINE: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

9.1. ALL NETWORKING COMPONENTS HAVE HAD THEIR DEFAULT PASSWORDS CHANGED.

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

9.6. YOU SECURELY CONFIGURE THE NETWORK AND INFORMATION SYSTEMS THAT SUPPORT THE DELIVERY OF ESSENTIAL SERVICES.

9.6.2 Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	
Tool Tip	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box. For advice on encrypting mobile devices and equivalent security arrangements, see https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/.
Video Guide	https://vimeo.com/digitalsocialcare/96

STANDARD TEN: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

10.1. THE ORGANISATION CAN NAME ITS SUPPLIERS, THE PRODUCTS AND SERVICES THEY DELIVER AND THE CONTRACT DURATIONS.

10.1.2 Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	
Tool Tip	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then tick and write "Not applicable" in the comments box. A template example is available from https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/
Video Guide	https://vimeo.com/digitalsocialcare/101

10.2. BASIC DUE DILIGENCE HAS BEEN UNDERTAKEN AGAINST EACH SUPPLIER ACCORDING TO ICO AND NHS DIGITAL GUIDANCE.

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

Video Guide	https://vimeo.com/digitalsocialcare/102

Help!

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

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