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

Contents

Glossary

CPA	Care Provider Alliance
CQC	Care Quality Commission
DPA	Data Protection Act 2018 (this is the UK's implementation of the General Data Protection Regulation (GDPR)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security & Protection Toolkit
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation 2016 (came into force May 2018)
IAR	Information Asset Register
ICO	Information Commissioner's Office
IG	Information Governance
KLOEs	CQC Key Lines of Enquiry
LA	Local Authority
NDG	National Data Guardian
NHS	National Health Service
ODS code	Organisation Data Service code/organisation code
ROPA	Record of Processing Activities
SAR	Subject Access Request
SIRO	Senior Information Risk Owner
TNA	Training Needs Analysis

Introduction

This guide has been designed to assist 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.

There is more information on who needs to complete the DSPT here.

The DSPT runs from 1 April to 31 March. It 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).

Information Governance (IG) Lead / Data Protection Champion

There are references throughout the DSPT to the IG Lead. This is the person who co-ordinates your data security and protection work. This doesn't need to be the Registered Manager.

We refer to this role as the Data Protection Champion throughout our materials. This is to match the job description which has been developed by Skills for Care.

The Data Protection Champion should have enough seniority to fulfil their responsibilities. It could be a shared role between several staff members. It is likely that as the individual completing the DSPT this will be your job.

Levels in the DSPT

There are four levels of compliance in the DSPT. One of which, 'entry level', is only available to social care providers. There is a separate guide to support 'entry level' compliance.

This guide supports care providers with achieving the higher 'standards met' level. For this, providers need to complete all mandatory requirements.

Name	Description
◆ **Entry Level**	• Time-limited level (subject to review) for social care providers. • Evidence items for critical legal requirements are being met; but some expected mandatory requirements have not been met. (https://www.dsptoolkit.nhs.uk/Help/32) • Allows access to NHSmail.
✓ **Standards Met**	• Evidence items for all mandatory expected requirements have been met. • Access to NHSmail, other secure national digital solutions, e.g. Summary Care Records, and potentially local digital information sharing solutions.
Standards Exceeded	• Evidence items for all mandatory expected requirements have been met. • The organisation has external cyber security accreditation. • Evidence of best practice.
Critical Standards Not Met	• Evidence items for critical legal requirements have not been met by the organisation. • No access to information sharing tools e.g. NHSmail.

There are four steps you need to complete before starting the DSPT. If you have already registered and set up your organisation account, jump to 'Step Four: Completing your Assessment'.

Step One: Registering for the DSPT

1. Go to https://www.dsptoolkit.nhs.uk/Account/Register
2. You will need your email address and your ODS Code (Organisation Code). If you don't know your ODS code, please contact exeter.helpdesk@nhs.net.

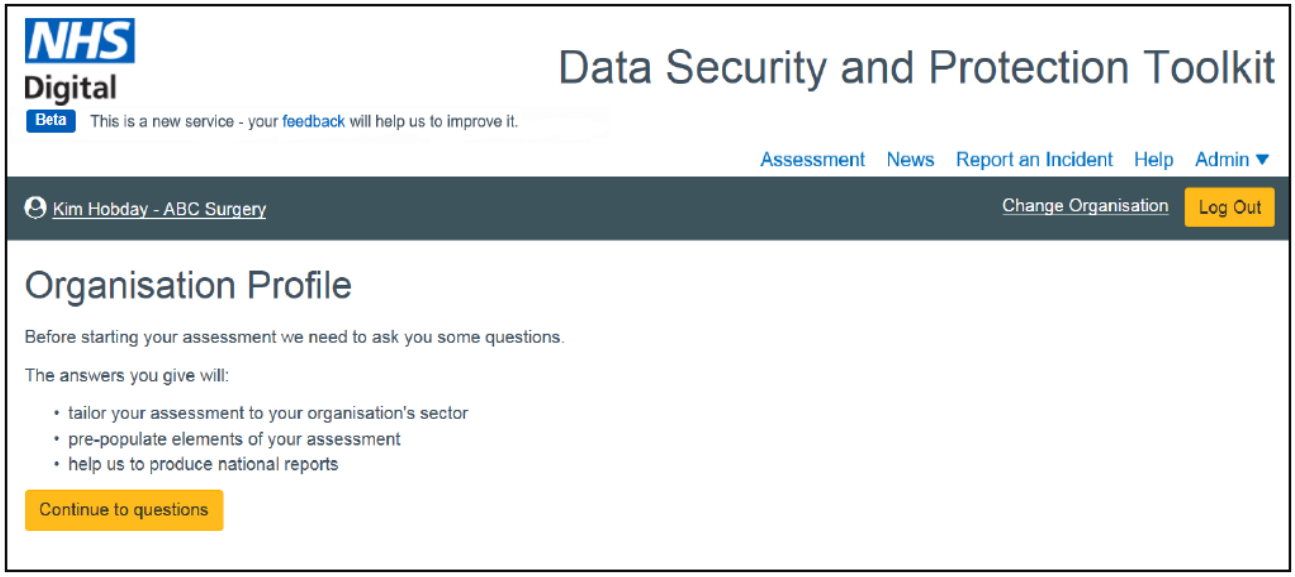
   There is more information on ODS codes for care homes and domiciliary care agencies here.
3. As you are registering your organisation, you will be the Administrator. You will be responsible for completing your organisation's profile and adding any other users.

   If you have difficulties with any step of registration, please check the Quick Start Guide. Email exeter.helpdesk@nhs.net if you have further issues.

Step Two: Completing your organisation profile

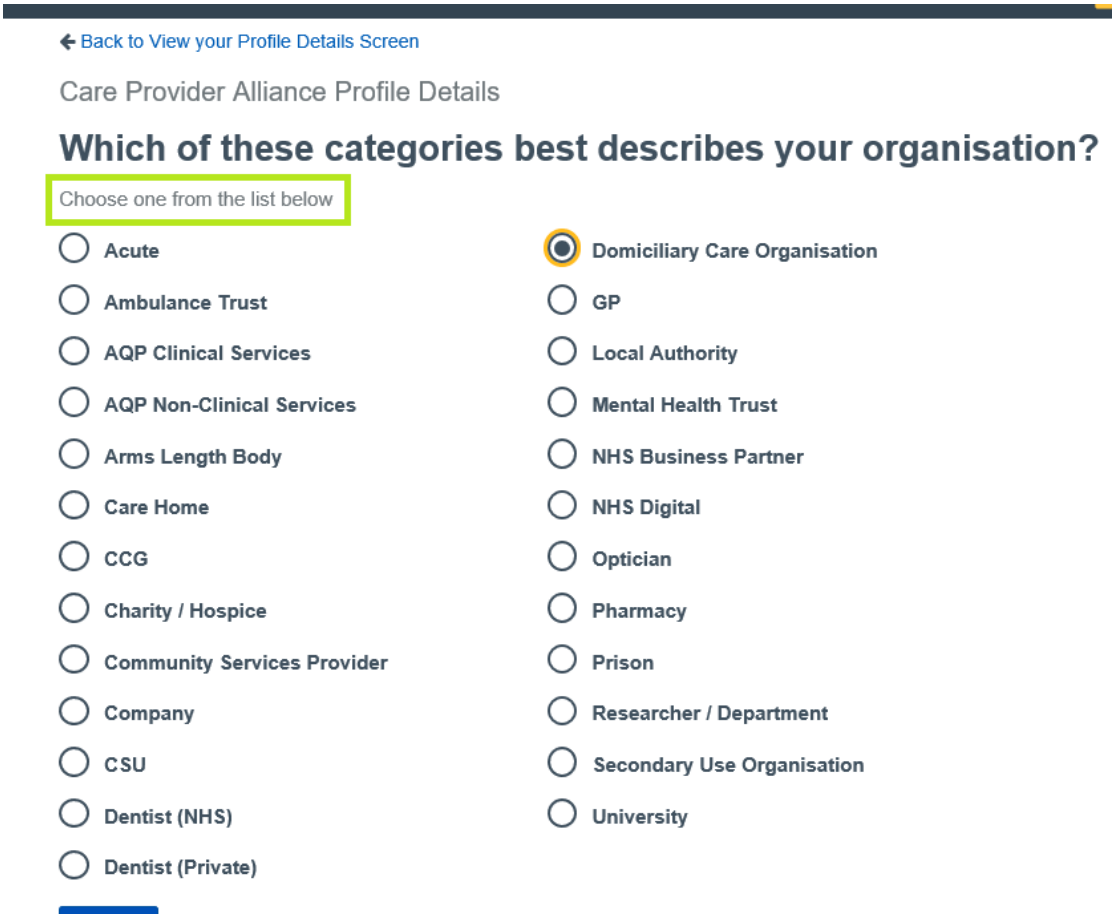
Once you have registered, you will need to sign in to complete your organisation's profile.

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



Click on the *"Continue to questions"* button to complete your profile.

3. Choose your organisation type. You can only choose one. If your organisation acts in different sectors (e.g. both residential and domiciliary care) then you should pick the one which makes up the bulk of your business.



4. You will be asked who has the following roles in your organisation:
    a. Caldicott Guardian
    b. Senior Information Risk Owner
    c. Information Governance Lead
    d. Data Protection Officer.

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

None of these roles are well-known in adult social care. There is more detail about each role in Key Roles and the DPO. That document covers all sectors, so do make sure you read the specific sections for social care.

We have also written sector specific guidance: Data Security and Protection Responsibilities.

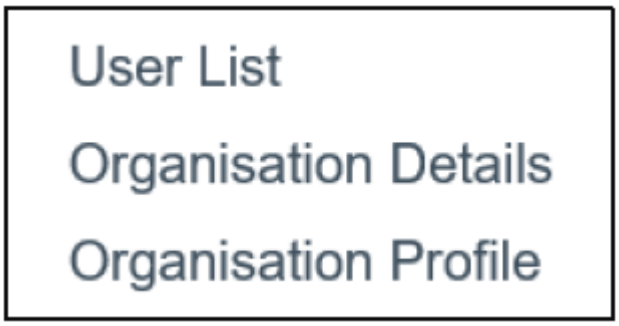
5. You will be asked if your organisation uses NHSmail or has a Cyber Essentials Plus certification. Make sure you select the right option or "Not Sure" if you are uncertain.
6. Check your answers and make changes if necessary. Once you're happy, click "*Accept and Submit*". You will be able to go back and make changes at any point.

   If you require more guidance, see the Administrator Guide.

Step Three: Setting up other users

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

1. Sign in to the DSPT and click on the "*Admin*" tab on the top right-hand corner of the page. This will reveal a drop-down list:



   Select "*User List*".
2. Once on the User List page, you can add more users. Users can be allocated one of three roles:
   a. Auditor - view assertions/evidence/organisation profile, reset own password and update own personal details.
   b. Member - view assertions, view/add/edit evidence, view organisation profile (but not edit), reset own password and update own personal details.
   c. Administrator member - view and confirm assertions, view/add/edit evidence, allocate assertion owners, submit and publish assessment, view and edit organisation profile, create and edit users for own organisation, reset own password and update own personal details.

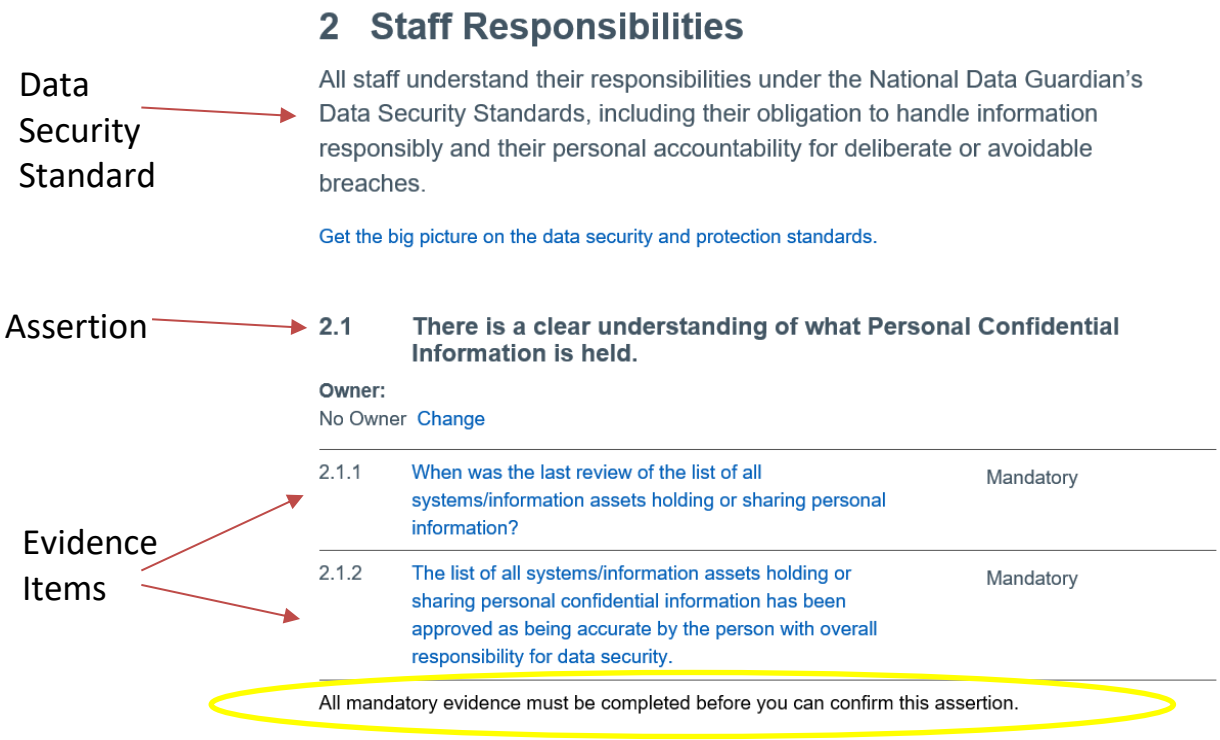
Step Four: Completing your Assessment

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.

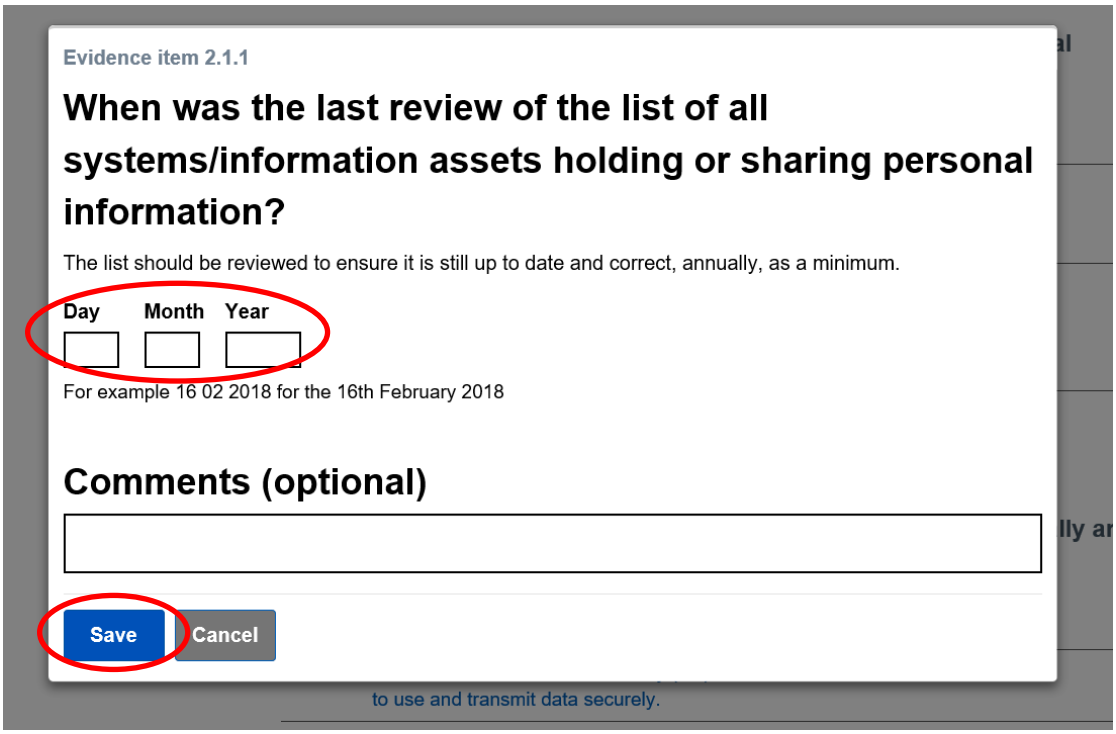
To achieve 'standards met', you must complete all mandatory evidence items.



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.

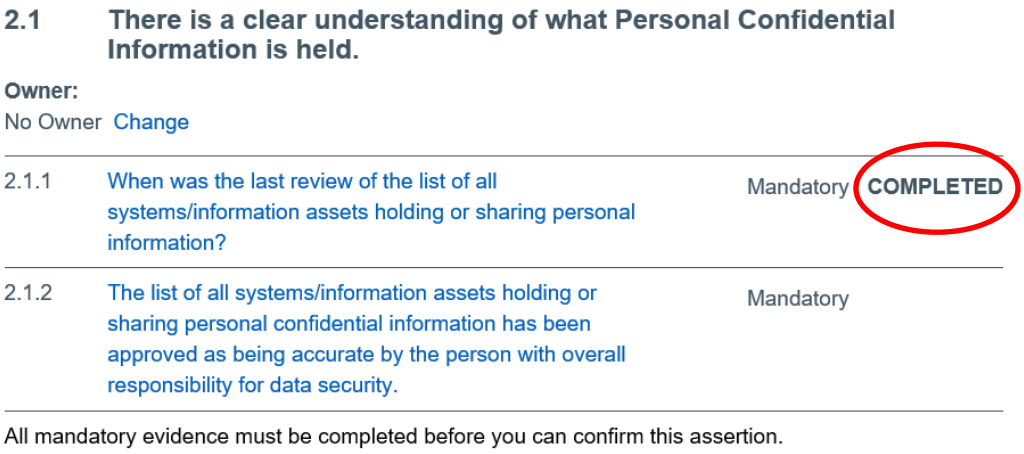
HOW TO COMPLETE AN EVIDENCE ITEM

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



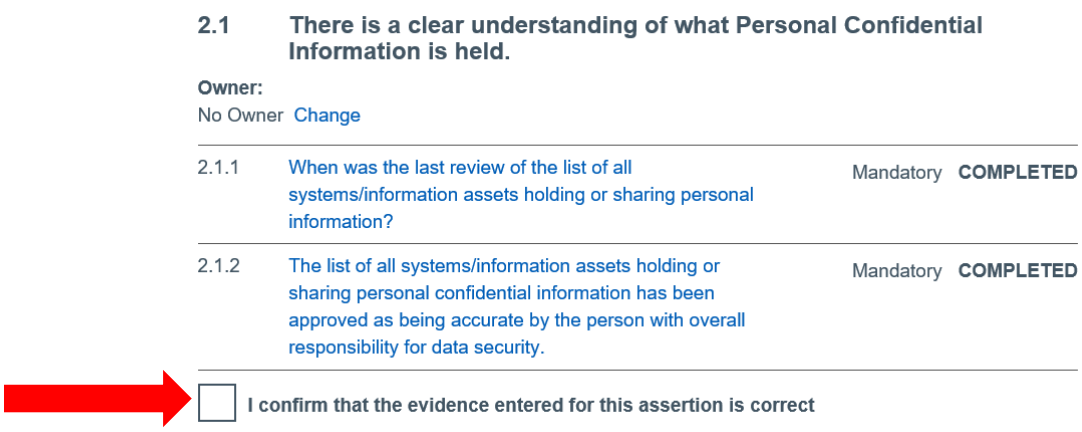
In this example, just enter the date.

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

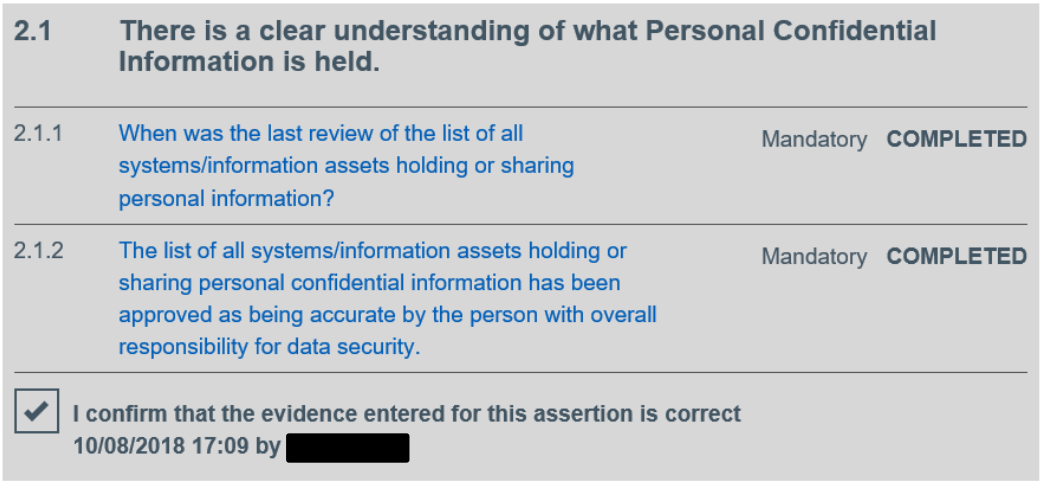


HOW TO COMPLETE AN ASSERTION

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.



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.



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 is by far the largest of the standards as it contains most of the requirements for the GDPR. Once you have completed that standard, you will have completed most of the DSPT's requirements.

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.

1.1.1 Name of Senior Information Risk Owner.	
Overview	A Senior Information Risk Owner (SIRO) is the person who understands, assesses and manages information risks. The SIRO ensures that information security risks are followed up and incidents managed. They provide leadership and guidance.
What to do	Ensure that someone at the highest level of your organisation has taken on these responsibilities. You do not have to call them a SIRO. Dependent on the size of your organisation this could be the owner, a member of the senior management team or member of the board. They need to have the authority to approve policies and oversee information risks. Make sure that their responsibilities are included in their job description. Our Data Security and Protection Responsibilities guide explains who would suit this role. The Big Picture Guide for Standard 1 contains expectations for the role. In small organisations it will be difficult to have multiple people fulfilling the roles required in the DSPT. It is recommended that you combine the roles so that there is a smaller burden. For example, the SIRO and Data Protection Champion (see below) could be combined. To complete this evidence item, provide the name of the person in your organisation who has taken on the SIRO role.

1.1.2 SIRO responsibility for data security has been assigned.	
Overview	See 1.1.1
What to do	Select the tick box once a SIRO (or equivalent job title) is assigned.

1.1.3 Name of Caldicott Guardian.	
Overview	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of peoples' health and care information. They make sure it is used properly. It is not mandatory for social care providers to appoint a **registered** Caldicott Guardian, though you may choose to do so if this makes sense for your organisation. There needs to be somebody at a high level in your organisation who takes on a "Caldicott function". This means that they take responsibility for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately. This might be combined with the Data Protection Champion (see below). The Caldicott Guardian manual can be a useful resource. The Caldicott Guardian Council can provide help and guidance.
What to do	To complete the evidence item, provide the name of your Caldicott Guardian. Write "n/a" if you do not have a registered Caldicott Guardian in your organisation.

1.1.4 Who are your staff with responsibility for data protection and/or security?	
Overview	You may have several members of staff who share data protection responsibilities between them. You need to have at least one person. This person is called the Information Governance (IG) Lead in the DSPT. We have referred to them as the Data Protection Champion in our guidance and materials. The role is like the "champion" role which is seen in other areas across the sector and can be shared between several people. The Data Protection Champion ensures effective management, accountability, compliance and assurance for all aspects of IG. Their key tasks include: 1. completing the DSPT by 31 March of each year; 2. ensuring that there is high-level awareness and support for IG;

	3. providing direction in creating, establishing and promoting IG policies; 4. ensuring that the approach to information handling is communicated to all staff and made available to the public; 5. ensuring that staff understand the need to support the safe sharing of personal confidential data for direct care as well as the need to protect individuals' confidentiality; 6. monitoring information handling activities to ensure compliance with law and guidance; 7. providing a focal point for the resolution and/or discussion of IG issues. Skills for Care have created a document with the core characteristics for Data Protection Champions.
What to do	Your Data Protection Champion will have the responsibilities noted above. In small organisations, the individual might also take on the responsibilities of the Caldicott Guardian function or the SIRO. The Data Protection Champion does not have to be the Registered Manager, but should either report to, or be a part of, the senior management team so that they can complete their tasks. As the individual who is completing the DSPT, it is likely that you will be the Data Protection Champion for your organisation. To complete the evidence item, provide the name and job title of anyone who has specific responsibility for data protection and/or security.

1.1.6 Name of Appointed Data Protection Officer/Data Protection Champion.	
Overview	A Data Protection Officer (DPO) is a new role which has been mandated, in specific situations, by GDPR. **It is unclear if all care providers will be required by law to have a DPO. There is advice below on why this is and What to do in this situation.** Under GDPR, you must appoint a DPO if:

	1. you are a public authority[1]; 2. your core activities include large scale regular and systematic monitoring of individuals (like online behaviour tracking); or 3. your core activities include large scale[2] processing of special categories of data (including health and social care information) or data relating to criminal convictions and offences. If your organisation is a public body under the Freedom of Information Act (e.g. Local Authority (LA)/NHS owned care homes) then you must have, or have access to, a DPO. Large organisations will need access to a DPO – this can be a consultant role and does not have to sit internally. For small organisation it is less clear if a DPO is needed. This is because there is no clear definition yet for "large scale processing". There is advice in the "**What to do**" section below on how to manage this. The GDPR does not say what qualifications a DPO needs. They should have experience working in and expert knowledge of data protection law. Ideally, they will also know the sector well. The DPO's responsibilities include: 1. informing and advising organisations about complying with GDPR and other data protection laws; 2. monitoring compliance with GDPR and data protection laws – including staff training and internal audits; 3. advising on and monitoring data protection impact assessments (DPIAs); 4. cooperating with the ICO; 5. being the first contact point for the ICO and citizens in terms of data processing. It will be difficult for many social care providers to appoint a DPO internally because of the position the DPO must occupy in the organisation. The GDPR specifies that the DPO must:

[1] As defined in the Freedom of Information Act 2000 – this will only apply to LA or NHS owned providers
[2] Note that there has not yet been a definition of what is meant by "large scale" and so there is some uncertainty around which size of provider would be expected to have a DPO.

	• not receive instructions on how to carry out their tasks; • not be dismissed or penalised for performing their tasks; and • report directly to the highest level of management. Additionally, the DPO cannot be the individual who decides how and why data is processed in your organisation. For example, a registered manager might decide that they want to start using a new digital rota system which includes personal data from staff. They could not be the DPO because they can decide how data is processed. Their decision-making process might conflict with data protection obligations.
What to do	**<u>For Local Authority (LA)/NHS Owned Care Providers:</u>** It is likely that the LA or CCG already has a DPO – find out who this person is. **<u>For large care organisations:</u>** A large care organisation could be characterised as multisite (perhaps on a regional or national level) with dedicated staff in roles such as IT, HR and estates. They have large volumes of care records. You should appoint, hire or contract a DPO for your organisation. There is more guidance below on what this role requires. If you choose not to have a DPO, you must record why you have made this decision. **<u>For small care providers</u>**: A small care provider could be characterised as having one or two sites, no dedicated staff IT or HR roles and a small volume of care records. You should assign someone in your organisation to be a "Data Protection Champion" who is responsible for ensuring your organisation complies with data protection legislation. Do not call this person a Data Protection Officer. Record the fact that you have not appointed a DPO and why you haven't. This is probably because you do not consider yourself to be processing special categories of data on a large scale. There is suggested wording for this in our Data Protection Policy template.

	We are continuing to discuss this matter with the Information Commissioner's Office (ICO), Information Governance Alliance and NHS Digital. We will provide updates if/when there are any changes. **There is more information on DPOs:** Skills for Care have produced guidance on DPOs and Data Protection Champions. The Information Governance Alliance have written guidance for health and social care organisations on the GDPR and DPOs. The ICO have written in-depth advice on DPOs. We have included this question in our FAQ and you can check there for updates. To complete this evidence item, provide the name of your DPO or write "n/a" if you do not have one.

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 There is a data security and protection policy or policies that follow relevant guidance.	
Overview	Policies are one of the foundations of having a strong data security and protection framework. The different sizes and complexity of organisations mean that some will have one all-encompassing policy, whilst others may have multiple policies supported by standards and procedures. There is no set number of how many different policies you must have on these topics. It is important the policies are effective, acknowledged and understood.
What to do	Confirm that you have a policy or policies in place that explain your organisation's plan for: • data protection; • data quality; • records management; • data security; • network security. We have created free, editable template policies and procedures which cover these topics. You can use them and make changes to align them with how things work in your organisation. Alternatively, you can use your own policies and procedures or those provided to you by your quality assurance system if you are happy that these cover the above topics. Some of the policies listed above might not be relevant for your organisation or may be too complicated – for example, the network security policy is unlikely to be necessary in many small organisations which use a limited amount of IT. Select the tick box to confirm your organisation has policies in place to complete this evidence item.

1.2.2 When were the data security and protection policy or policies last updated?	
Overview	See 1.2.1
What to do	Enter the date when your policies were last updated. If they are new policies, enter the creation dates.

1.2.3 Policy has been approved by the person with overall responsibility for data security.	
Overview	Your organisation should have someone at the highest level who takes overall responsibility for data security. Ideally this will be your SIRO (see section 1.1.1 for details). In small organisations, it is likely that this role will be an additional part of a pre-existing job role, rather than someone being hired exclusively to perform this function. Our 'Data Security and Protection Responsibilities' guide explains who would suit this role. They will be responsible for approving your data protection policies.
What to do	Select the tick box to confirm that your policies and procedures have been approved by the appropriate senior member of staff in your organisation. This might be the SIRO.

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

1.3.1 ICO Registration Number.	
Overview	**The Information Commissioner's Office (ICO) is the regulatory body for data protection (not CQC)**. Under Data Protection (Charges and Information) Regulations 2018, data controllers (i.e. care providers) need to pay a registration fee to the ICO.
What to do	The following link provides information on what fee you are required to pay. Your DPO (if you have one) should be registered with the ICO. There is more information here. (See section 1.1.6) Provide your ICO registration number to complete this evidence item.

1.3.2 Transparency information is published and available to the public.	
Overview	GDPR contains stringent transparency requirements so that people are properly informed about the use of their personal information and of their rights, before or at the time their information is collected. You need to set out in clear and easily understood language what you do with the personal data you process. This is called a transparency notice, privacy notice or privacy statement. People have the right to be informed about what data you use of theirs, why you use it and what the legal basis is for this. There is more information available here.
What to do	It is a requirement of GDPR that you let people know • what information you collect about them; • how this is stored; • why you have this information; • who this information is shared with; • how long you keep it for; and • their individual rights.

	This doesn't **only** apply to your service users, but also staff and visitors. There is a template Privacy Notice on our website and more information on how to create one in our How To Document Your Data Processing guide. If you have a website this should be published there. Otherwise, this needs to be made publicly available to people within your organisation, perhaps by having a copy displayed in reception, or having it always available on verbal request. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

1.3.3 How have individuals been informed about their rights and how to exercise them?	
Overview	As an extension of the privacy notice in 1.3.2, it is important that you can demonstrate that individuals have been informed of their rights. GDPR provides individuals with 8 new rights: 1. The right to be informed 2. The right of access 3. The right of rectification 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling. Not all of these rights apply in all instances. There is more information here.
What to do	You will need to explain how you are informing the people you support, their families and your staff about their information rights and what data of theirs you process. This might be through a website, a leaflet, letters or posters. It should be provided in the way which makes most sense for your organisation. For example, putting your privacy notice on your website is the easiest way of making it publicly available but older service users may not feel comfortable accessing it. A different method should be used as well.

	There is a template leaflet to give to your service users here. Remember that the information must be provided in a clear, concise and easily understood way. We have written Guidance on Subject Access Requests and the Rights for Individuals under GDPR. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

1.3.4 There is a staff procedure about how to provide information about processing and individuals' rights at the correct time.	
Overview	You must have a procedure on how your staff let your service users know about how you use their information and what information you use. Equally you must also have a procedure for how you inform your staff and visitors what information you keep. We have written guidance on data sharing for staff and a procedures in our Record Keeping Policy.
What to do	The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

1.3.5 There is an updated subject access process to meet shorter GDPR timescales.	
Overview	One of the rights which GDPR provides to individuals is the right to access their data. This is commonly called a Subject Access Request (SAR). People can make this request verbally or in writing (including via social media) to any member of staff, so it is important that you have a clear process which your staff are familiar with. Once a request has been made you have one month to respond to the request. You can no longer charge a fee for SARs and the deadline is shorter than before. We have written Guidance on Subject Access Requests and the Rights for Individuals under GDPR.

	There is also guidance on SARs available on the ICO website.
What to do	Have a clear procedure to follow for SARs. Our Record Keeping Policy has a template procedure to follow. You can adopt this for use in your organisation or adapt it. If you already have a procedure for dealing with SARs, make sure that it has been updated to comply with the shorter timescales for responding. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in the free text box.

1.3.6 Provide details of how access to information requests have been complied with during the last twelve months.	
Overview	Your organisation will need to record all SARs and, if applicable, Freedom of Information (FOI) requests. (Note that FOI only applies to NHS or LA owned care providers). Particularly keep records of any SAR which is not responded to within one month, with a reason for why the response has been delayed. The ICO have provided a model letter for SARs and detailed the sort of information that you might need to record.
What to do	Have a procedure for how you deal with SARs (and FOI requests if applicable) and make sure that your staff follow it. Ensure that someone is responsible for keeping and auditing these records. There are procedures for handling SARs in our Record Keeping Policy. Provide details of the number of requests received during the last 12 months in the free text box.

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 A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing.	
Overview	It is a legal requirement that organisations which process personal data keep a record of their processing and their legal basis for doing so. This does not mean that your organisation must record every single time any individual's information is used or shared (e.g. each time a carer reads or checks the care plan). We recommend that you have two registers, though you can combine them into one large register if you prefer: 1. Information Asset Register (IAR – see 1.4.4 below) – Records what types of information we have, where we keep it and how we protect it; 2. Record of Processing Activities (ROPA) (sometimes referred to as data or information flows) – record of where we receive data from, where we send it to and the legal basis for this. The ROPA must include: • Why you are processing data; • What legal basis you rely on (GDPR Article 6 and Article 9); • Which groups of people the data belongs to and what kind of data it is; • Who you are sending it to; • Whether information is transferred overseas; • Whether data is retained and disposed of in line with policies; • Whether a written data-sharing agreement or contract is in place and when it ends. Understanding what data will flow between organisations is one of the fundamental building blocks of good IG. Until data flows have been captured and mapped, they cannot be effectively risk assessed and secured against known risks.
What to do	This evidence item is concerned with your ROPA (see 1.4.4 below for IARs).

	In order to complete your ROPA, visit the section on our website entitled: How to record what data we share and why do we need to do it?. This contains guidance on how to go about creating your ROPA and explains the different legal bases used by care providers. Read "How to Document your Data Processing" first before trying to create your records. We recommend completing your IAR first before moving on to your ROPA. There is also a template ROPA which you can choose to use which sits alongside a template IAR. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in the free text box.

1.4.2 Have information flows been approved by the person responsible for data security?	
Overview	See 1.4.1
What to do	Select the tick box to confirm that your ROPA has been approved by the appropriate senior member of staff in your organisation. This might be the SIRO.

1.4.3 Date of when information flows were approved by the person with responsibility for data security.	
Overview	See 1.4.1
What to do	Complete the date when the ROPA was approved by the appropriate person within your organisation.

1.4.4 Provide a list of all systems/information assets holding or sharing personal information.	
Overview	An information asset is defined by the National Archives as "A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively.

Information assets have recognisable and manageable value, risk, content and lifecycles."

Personal information can be held in systems such as:

- care administration systems
- staff rostering systems
- payroll

Each of these are information assets.

Keep a record of the different types of **personal information** you hold.

You do not need to record each file, but groups of files. For example, care records are stored in this filing cabinet, employee pay records are stored in this computer system etc.

The information asset in these examples would be the filing cabinet and the computer system.

Normally information assets are recorded in an information asset register (IAR) (See section 1.4.1).

An IAR is a record of digital **and** hard copy files, who is responsible for ensuring the safety of the record, and what safety measures are in place.

It is best practice to risk assess each asset and to note what security you have in place, e.g.

Information Asset	Risk	Security Measures
Filing cabinet containing archived care plans	If inappropriately accessed, sensitive personal data could fall into the wrong hands. This would cause distress to the individual, loss of reputation and possibly fines to our organisation.	Filing cabinet is always locked and kept in a locked room. Access is restricted to those staff who need to see care plans.

	This isn't required as part of this evidence item, but it is necessary for you to do this to be compliant with our template policies.
What to do	In order to complete your IAR visit the section on our website entitled: How to record what data we share and why do we need to do it?. This contains guidance on how to go about creating your IAR. Read "How to Document your Data Processing" first before trying to create your register. There is also a template IAR which you can choose to use. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in the free text box.

1.4.5 List of systems which do not support individual login with the risks outlined and what compensating measures are in place.	
Overview	Systems that do not support individual logins by their very nature carry more risks than those that do. For example, a computer which only has one shared user account, a shared email address, paper records etc. These systems pose risks because: 1. they make audits and accountability difficult as you cannot guarantee who is making actions; 2. management is complicated when you cannot change a password without affecting other users. Account sharing leads to more password sharing which risks a password being disclosed to an inappropriate person.
What to do	List and risk assess each system. This might be in your IAR (see 1.4.4). As part of this risk assessment you should have: 1. controls and mitigations stated for each risk; 2. a description of the risk with its impact and likelihood. Consider the type of system, the amount of confidential personal data and how and where this is accessed. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

1.5. PERSONAL INFORMATION IS USED AND SHARED LAWFULLY.

1.5.1 There is approved staff guidance on confidentiality and data protection issues.	
Overview	It is important that your staff fully understand their confidentiality and data protection obligations, so that a culture of data security and protection thrives in your organisation. Align this guidance with the data protection policies you implemented as part of 1.2.1.
What to do	It is up to you how this guidance is disseminated to your staff – it could be through training or through updating staff handbooks and contracts. There are some templates and guidance materials available on our website: • Staff Data Security and Protection Code of Conduct; • Guidance on Data Sharing; • Guidance on Subject Access Requests and the Rights for Individuals under GDPR; • Guidance on Data Quality; • Guidance on Data Breaches; and • Staff Confidentiality Contract Clause. We have also provided advice on staff training. Select the tick box to confirm that there is approved staff guidance to complete this evidence item.

1.5.2 Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed.	
Overview	Ensure that your organisation has assigned overall responsibility for monitoring and auditing access to confidential personal information to an appropriate senior staff member. This member of staff is responsible for ensuring that confidentiality audit procedures are developed and communicated to all staff with the potential to access confidential personal information. These audits will be similar to audits that you undertake in other business areas. We have provided a template audit log which is at the end of our Data Security Policy.

What to do	Click the check box to confirm that audits have taken place over the last 12 months.

1.5.3 Results of staff spot checks and actions taken when data protection non-compliance is identified.	
Overview	See 1.5.2
What to do	Have documentary evidence of the audits which you have carried out and any actions which have arisen. This needs to be signed off by a senior member of staff – potentially the SIRO. We have provided a template audit log which is at the end of our Data Security Policy. The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

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

1.6.1 There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	
Overview	Data protection by design and by default means that your procedures and systems are designed to take account of data protection and security issues from when they are first implemented. Your data protection by design procedures aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent and where feasible allows individuals to monitor what is being done with their data. These procedures enable your organisation to improve data protection and security. Pseudonymisation is a technique whereby enough data is removed from a record to ensure that the individual whose data it is cannot be identified without additional information from another source. For example, if you were to contact social services about one of the people you support but used a unique identifier rather than their name to identify them, then you are using pseudonymised data. The individual could still be identified if social services were to match this information to another document linking names to unique identifiers. But they are not immediately identifiable to people who can't link the unique identifier to a name. Part of your data protection by design and by default will be assessing whether to undertake a Data Protection Impact Assessment (DPIA). There is more information on this in 1.6.7.
What to do	There is significant guidance on data protection by design and by default on the ICO's website. If you are using our policies, this is covered in our template Data Protection Policy. Select the tick box to confirm that you have these procedures in place to complete this evidence item.

1.6.2 Data Protection by design procedure has been agreed.	
Overview	See 1.6.1
What to do	Select the tick box to confirm that your procedure has been approved by the appropriate senior member of staff in your organisation. This might be the SIRO.

1.6.3 There are technical controls that prevent information from being inappropriately copied or downloaded.	
Overview	It is important to ensure that only the appropriate people have access to, or can change or delete, personal confidential information in your organisation. It is important that information cannot be copied or downloaded by those who don't have the right to see the information. Ensure that you have procedures in place to make sure that this cannot happen. For paper records, this will be about making sure that confidential information is kept secure when not in use. It must not be left lying around in public areas (for example, on top of a fax machine) where inappropriate people could have access to it. For digital records, you may need to employ more technical measures to ensure that information is not copied or downloaded. Some examples include: • each user has their own username and password so you can be more certain that only appropriate people are accessing your data. This reduces the likelihood of people sharing passwords. • staff have the minimum level of access to systems to carry out their role. For example, a nurse might have full access to the care planning system, but a receptionist would not. • not allowing USB sticks to prevent the risk of them being lost or misplaced. • blocking USB ports on computers so that you can control what data is copied to and from them.

	If you are using technology extensively, you will need to consider more options than those mentioned here. In which case, it would be good to speak to an IT specialist or IT support to help with this question. There are more examples of what you can do in the Big Picture Guide for Standard 1.
What to do	There are example procedures for preventing inappropriate copying and downloading of confidential information in our Data Security Policy. Update this policy with the procedures that you use in your organisation. For example, make sure that the password policy used in your organisation matches what is written in the policy. Remember to mention any specific auditing that you do for this evidence item – including if this is undertaken by your external IT support or supplier. This might match what you have covered in 1.5.2. Provide high level details of these procedures in the free text box to complete this evidence item.

1.6.4 There are physical controls that prevent unauthorised access to sites.	
Overview	As well as protecting digital information, it is important to ensure that unauthorised people do not gain access to your site(s). It is likely that you already have these procedures in place as they are often linked to the security of your staff and service users. These might include: • lockable doors, windows and cupboards; • clear desk procedures; • ID; • key card access; and • locks for secure areas.
What to do	There are example physical security procedures in our Data Security Policy. Make sure that whatever procedures you document match the actual practice within your organisation.

	Provide high level details of these procedures in the free text box to complete this evidence item.

1.6.7 There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.	
Overview	Data Protection Impact Assessments (DPIAs) are what were previously called Privacy Impact Assessments. They have not traditionally been commonly used in adult social care. GDPR has introduced a duty to complete one when there is "high risk" processing. "High risk processing" encompasses: • automated processing • large scale processing of special category data - which includes health, social care and genetic data • systematic monitoring of a public area. As with DPOs (see 1.1.6), the use of the term "large scale" causes some confusion – particularly for small organisations – about when a DPIA is required. It is considered good practice to, as a minimum, complete a DPIA for your existing care planning procedures. It is good practice to complete a DPIA when you are bringing in any new system which could impact on individual's data rights. If you choose not to do so, keep a record of why you made this decision. For example, if you move from a paper to electronic care planning system, complete a DPIA to assess if this would impact on individuals' rights. In essence, a DPIA is a risk assessment with a specific focus on data protection and privacy.
What to do	Decide which staff would be responsible for completing a DPIA (for a small organisation this might well be only one person). Ensure these staff understand the purpose of a DPIA. This might be by reading the ICO guidance on when and how to complete one. Have a procedure on how and when to complete a DPIA in your organisation. The ICO have written a checklist to run through to find out if you need one. They also have guidance on what you need to document in a DPIA.

	Select the tick box to confirm that you have this procedure to confirm this evidence item.

1.6.8 The Data Protection Impact Assessment Procedure has been agreed by the person in the organisation with overall responsibility for data security.	
Overview	See 1.6.7
What to do	Select the tick box to confirm that your procedure has been approved by the appropriate senior member of staff in your organisation. This might be the SIRO.

1.6.11 All high-risk data processing has a Data Protection Impact Assessment carried out before processing commences.	
Overview	See 1.6.7
What to do	Confirm that any new processing activities which involve personal data have undergone a DPIA. Ensure that you have completed a DPIA for your existing care planning system (paper or electronic). There is extensive guidance and a template DPIA on the ICO website. To complete this evidence item, select the tick box to confirm that all high-risk data processing has undergone a DPIA before starting. If you do not need to perform a DPIA, check the tick box to confirm and comment "n/a" in the comment box.

1.6.12 All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.	
Overview	If your DPIA identifies a high risk and you cannot mitigate that risk, you must consult the ICO **before** starting the processing. The ICO has stated that written advice will be provided within eight weeks, or 14 weeks in complex cases. In appropriate cases, the ICO may issue a formal warning not to process the data or may ban the processing altogether. For example, if you moved to an electronic care planning system which stores your care records on a public cloud in North America you won't be

	able to ensure the security of these records. Therefore, you cannot mitigate the risk of a data breach. However, most software suppliers will be able to tell you where their servers are and their security procedures for protecting your data, so it is unlikely that this will come up. To notify the ICO, email them on dpiaconsultation@ico.org.uk and attach your DPIA. Do not start processing until you have heard back from the ICO.
What to do	Select the tick box to confirm that all unmitigated risks have been reported to the ICO to complete this evidence item. If you have not needed to report any DPIAs to the ICO, check the tick box to confirm and comment "n/a" in the comment box.

1.7. EFFECTIVE DATA QUALITY CONTROLS ARE IN PLACE.

1.7.1 There is policy and staff guidance on data quality.	
Overview	Good governance is one of the fundamental regulatory standards for adult social care. Social care providers are required to keep accurate, contemporaneous records of care and audit them so that quality is maintained. Good quality, accurate records are vital in health and social care. When records are created or updated the information must have the following characteristics: a) It is *authentic* – i.e. the data is what is claims to be. b) It is *reliable* – i.e. data is complete, accurate and written down as soon after the (or during) the event as possible. c) It has *integrity* – i.e. any changes are clearly marked and the person who made the change is identified. d) It is *useable* - i.e. We know where records are kept and log this information. There is more guidance on this on the CQC website.
What to do	We have provided a template Data Quality Policy and Staff Guidance. Select the tick box to confirm that you have the policy and guidance in place to complete this evidence item.

1.8. PERSONAL INFORMATION PROCESSED BY THE ORGANISATION IS ADEQUATE (AND NOT EXCESSIVE) FOR THE PURPOSES.

1.8.1 There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.	
Overview	One of the principles of GDPR is "storage limitation". This means that you can only keep personal data for as long as you need it and can justify having it. As part of this principle, you are required to have a policy which sets out how long you retain records. The ICO has detailed guidance on the principle of storage limitation. Part of storage limitation is to have procedures in place to ensure that you are disposing of or archiving personal data correctly and legally.
What to do	It is likely that you already have a records retention schedule as part of your record keeping or record management policy. Update this to ensure it complies with new legislation. We have created a Record Keeping policy. This includes details on the safe destruction of personal data. Make sure that your staff are aware of the updates to your policy. We recommend that you look to the 'Records Management Code of Practice for Health and Social Care 2016' if you are unsure how long to keep data for. Select the tick box to confirm that there is guidance in place for staff on records retention and destruction to complete this evidence item.

1.8.2 A records retention schedule has been produced.	
Overview	See 1.8.1
What to do	Produce a records retention schedule. You can choose to use the records management code of practice for this. Record if you use different lengths of time than what is written in the code and why you have chosen to do so. This might be because your insurer requires that you keep information for longer than what it said in the code.

	Select the tick box to confirm that you have a retention schedule in place to complete this evidence item.

1.8.3 Provide details of when personal data disposal contracts were last reviewed/updated.	
Overview	If third parties are used to dispose of (destroy or archive) personal data, have a written contract in place. The contract must include: • the requirement to have appropriate security measures in compliance with data protection law; • The third party must allow you to audit them. Each disposed of item should be recorded on a destruction certificate. There is guidance on contracts for secure data disposal on our website.
What to do	Provide details in the free text box of when you last reviewed your data disposal contracts (this should be within the last 12 months) to complete this evidence item. If you do not use a third-party disposal service, then simply state this in the free text box and provide details of what you do instead, e.g. a cross-cut shredder with a log of which documents you have destroyed etc.

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.

2.1. 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?	
Overview	Maintain a list of systems holding personal confidential information. There is not a prescribed method, however this can be recorded in your IAR (see 1.4.4). If you have not completed the DSPT before, you might not have an IAR yet. Review this list periodically (at least annually) and amend if there are changes.
What to do	Provide the date of the last time you reviewed your IAR, or its creation date, to complete this evidence item.

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.	
Overview	See 1.4.4 & 2.1.1
What to do	Select the tick box to confirm that your IAR has been approved by the appropriate senior member of staff. This might be the SIRO.

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

2.3.1 There is a data protection and security induction in place for all new entrants to the organisation.	

Overview	Assess your current induction procedures for your staff to decide if they receive enough training about data security and protection. Staff can be at their most vulnerable during their induction period. They may not understand your organisation's systems, policies and procedures, its cultures or norms.
	
	The induction should help staff understand their obligations to the National Data Guardian's (NDG) data security standards. It should include:
	
	• the importance of data security in the care system
	• the NDG data security standards, particularly the three standards relating to personal responsibility (standard 1, 2 and 3)
	• the applicable laws (GDPR, FOI (if applicable) etc.)
	• when and how to share and not to share
	• understanding:
	  ○ what social engineering is;
	  ○ safe use of social media and email;
	  ○ the dangers of malicious software;
	  ○ how to protect information;
	  ○ physical security;
	  ○ how to spot and report data security breaches and incidents.
	
	It is important that the messages are local and specific to your organisation. They should include local procedures and policies and, if possible, local incidents.

What to do	Have an induction in place for your new members of staff which covers the points above. You can choose how you do this. Either with face to face teaching, online modules or other methods. Make sure that you keep a record as part of your training matrix.

	We have written An Introduction to Information Sharing for Staff which covers many of these topics. If you use the Care Certificate, Standard 14 covers information handling. Select the tick box to confirm that you have an induction in place for your new starters to complete this evidence item.

2.3.2 All employment contracts contain data security requirements.	
Overview	There should be a clause in staff contracts which reference data security (Confidentiality, Integrity and Availability – see 6.1.1 for detailed explanation of each type of data security).
What to do	You will need to review your staff contracts to see if they need to be updated to include a clause on data security. Make sure staff are aware that not following data protection policies can result in disciplinary action and might be considered as gross misconduct. We have provided a draft clause. Select the tick box to confirm all employment contracts mention data security to complete this evidence item.

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 A data security and protection training needs analysis has been completed.	
Overview	A training needs analysis (TNA) is a means of identifying existing training levels for your staff and assessing whether that is enough or more training needs to be provided. You can use the following method to conduct your analysis: 1. Assess what training is already in place in your organisation for all staff. This will act as your baseline. You may have nothing in place, which gives you a clean slate to implement training. 2. Identify the scope - who should be included and excluded e.g. maternity / paternity, long term sick and agency staff. 3. Identify which staff will need a higher level of knowledge around data security and protection than others, e.g. the Data Protection Champion or senior staff who often handle and make decisions about personal information. 4. Make a note of each of these steps and ensure that each decision is signed off by the necessary person in your organisation as this will be evidence for your TNA. Consider if you would need to provide more training for members of staff who use computers or mobile devices during their work compared to any staff whose work is completely paper based.
What to do	Follow the steps above to identify the appropriate training which is required for your staff. Make sure that your TNA is signed off by the appropriate senior staff member. Select the tick box to confirm that you have completed your TNA to complete this evidence item.

3.1.2 Date of last data security and protection training needs analysis.	
Overview	See 3.1.1
What to do	Provide the date of the last time you reviewed your TNA, or its creation date, to complete this evidence item.

3.1.3 Training Needs analysis has been approved by the person with overall responsibility for data security.	
Overview	See 3.1.1.
What to do	Select the tick box to confirm that your TNA has been signed off by an appropriate senior member of staff.

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

3.3.1 Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.	
Overview	All staff must complete appropriate data security training. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of staff to receive training every year and so for the DSPT at least 95% must receive and pass training. National training has been developed with the assistance of various health and social care organisations. This training is **freely** available to everyone working in social care. The Data Awareness Training Level One is aimed at all staff and is followed by a test which evidences that the staff member understands the material. The training includes realistic and relevant case studies. The national training is not mandatory for social care providers and is not the only option for this requirement. There is more information on the options available for training on our website.
What to do	Once you have completed training your staff each year, enter the percentage who have received training to complete this evidence item.

3.4. STAFF WITH SPECIALIST ROLES RECEIVE DATA SECURITY AND PROTECTION TRAINING SUITABLE TO THEIR ROLE.

3.4.1 Number of staff assessed as needing role specialist training.	
Overview	As part of your TNA you will have identified which staff require additional training to fulfil their roles. This is may include any of the following job roles: • IG Lead(s) / Data Protection Champion • Data Protection Officer • Any IT leads • Registered Manager • Quality assurance team • Senior management team • Etc.
What to do	Write high-level details of which staff have received specialist training and how this has been delivered in the free text box to complete this evidence item. This might be just one person in small organisations

3.4.2 Number of staff completing advanced Data Security Training.	
Overview	See 3.4.1
What to do	Provide the number of staff who received specialist training in your organisation to complete this evidence item.

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

3.5.1 SIRO and Caldicott Guardian have received appropriate Training.	
Overview	The SIRO and Caldicott Guardians (or the equivalent job roles) are looked to as leaders for data protection and security within their organisations. As they are expected to lead from the top, it is important that they have received adequate and ongoing training to support them in their roles. Aside from the data security and protection training that all staff undertake. Caldicott Guardian training is currently in the form of a standalone workbook. It will be useful for both those who hold SIRO or Caldicott roles to have understood this workbook. Ensure that the person(s) holding these roles have received any additional training which has been identified as necessary by your training needs analysis.
What to do	Use the free text box to confirm that these roles have received appropriate training to complete this evidence item. As described in section 1.1.3 it is **not mandatory** for social care providers to appoint a registered Caldicott Guardian, although there needs to be somebody who takes on the "Caldicott function".

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 The organisation maintains a current record of staff and their roles.	
Overview	One of the biggest challenges for any organisation is tracking staff role changes, especially when they have multiple roles. It is important to maintain a record of all current staff, so you can be certain that people have the right access levels to different types of data.
What to do	Maintain a list of all staff and their roles. This should be up to date and reflect when staff are recruited, their change of role(s) or if they leave the organisation. This might be linked to your existing payroll or rostering system. Select the tick box to confirm that you maintain a current record of staff and their roles to complete this evidence item.

4.1.2 For each system holding personal and confidential data, the organisation understands who has access to the information.	
Overview	You should know who has access to the information in each system. This might be managed by the system itself – e.g. a rostering system where all staff can access a read-only view but only management can make alterations to rotas; or multiple systems might be accessed by one person through a single account – e.g. a user logs on to the computer and can access a rostering system, email and payroll. If information is shared with another system, you should know who has access to that system too, e.g. if your rostering system provides information to a payroll system run by a third-party, you need to know who has access to that information as well. Each system should have role-based access. Role-based access systems allocate user rights for different groups. For example, a user in an administrative group would be able to view, amend or delete everything,

<table>
<tr><td></td><td>whereas someone in a read-only group could only view. For each system using role-based access, record each group which exists within the system and the numbers of staff in each group.

Base access on the individual's job. For example, if a user only needs to view records there is no need for them to have an elevated role such as admin. The 'view user' role will allow them the access they require.</td></tr>
<tr><td>What to do</td><td>Record who has access to which system and what level of access they have. There is no set way to do this. Here are 2 examples of how this can be done:

1.

<table>
<tr><th colspan="3">Care planning system</th></tr>
<tr><th>Role</th><th>Description</th><th>Number of accounts</th></tr>
<tr><td>Admin</td><td>Ability to amend, delete and create new tables and look up fields</td><td>2</td></tr>
<tr><td>General user</td><td>Ability to add, amend and delete own created records and view others</td><td>50</td></tr>
<tr><td>Super user</td><td>Ability to add, amend and delete own created records, amend and view others</td><td>3</td></tr>
<tr><td>View user</td><td>Ability to view all records</td><td>8</td></tr>
<tr><td>Backup user</td><td>Technical account used to archive the systems database</td><td>1</td></tr>
</table>

Or

2. For small organisations, it might be easier to record each member of staff's role against the staff list and what systems they have access to, e.g.

<table>
<tr><th>Name</th><th>Job Title</th><th>Systems Accessed</th><th>Role</th></tr>
<tr><td>Patricia Personnel</td><td>Carer</td><td>Rostering System</td><td>General</td></tr>
</table>
</td></tr>
</table>

		Email	General
Colin Cloud	Data Protection Champion	Rostering System Email Computer network	General Administrator Administrator
Susan Septum	Registered Manager	Rostering System Email Computer Network Payroll	Administrator General General Administrator

The evidence item will ask that you either upload a document, provide a link to the document on your website, or you can enter the location of the document in your organisation in the free text box.

4.2. STAFF ROLES ARE LINKED TO IT ACCOUNTS. STAFF MOVES IN, OUT OR ACROSS THE ORGANISATION ARE REFLECTED BY IT ACCOUNTS ADMINISTRATION.

4.2.1 Date last audit of user accounts held.	
Overview	It is important to periodically audit IT accounts for new starters, movers and leavers. This is to make sure that people's access rights are at the right level. It is particularly crucial that leavers who had access to personal confidential information have their access rights revoked in line with your policies and procedures. As well your regular processes for dealing with starters, movers and changers, audit user accounts intermittently. Audit your user lists and roles, identify any changes and delete or disable unnecessary users. There is an audit checklist at the end of our Data Security Policy. There is also guidance and a template access policy on NHS Digital's cyber security knowledge base.
What to do	Enter the date of your last user access audit to complete this evidence item.

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

4.3.1 All system administrators have signed an agreement which holds them accountable to the highest standards of use.	
Overview	A system administrator is typically responsible for installing, configuring and maintaining hardware and software infrastructure. It is likely that many small care providers will not have someone in this position, or that the person fulfilling this role is a third-party contractor. System administrators have a great deal of system power and so must have the highest level of integrity in terms of the confidentiality, integrity or availability of the systems they support. In recognition of this responsibility, your system administrators should sign a System Administrator Agreement. You can include this in third-party contracts if you use external IT support.
What to do	Ensure that your system administrator(s), if any, has signed a contract which states that they have higher access privileges and that their conduct is expected to reflect this. Select the tick box to confirm that you have this in place. If you do not have a system administrator, select the tick box to complete this evidence item.

4.3.5 Staff have provided explicit understanding that their activity of systems can be monitored.	
Overview	It is important that staff are monitored and audited as a data protection and security precaution. The types of monitoring will be different dependent on how much IT you use. If you only use paper records, you might find that you only have very few audit methods – this might be limited to checking physical access procedures. If you use digital records, then your monitoring would be more extensive. The more sensitive information the system contains, the more granular and extensive the monitoring should be.

	The following are examples of the kind of monitoring which might be possible: • a rostering system monitors the creation, viewing, modification, deletion of shifts, allocated locations, holiday and sick leave. This is through the proprietary system within the application developed by the supplier; • for desktop computers, each user has an individual log-in which allows them access to certain areas of the network based on their role. This is monitored by our IT support and the details outlined in our contract. Typical recording events would also include the date and time, the user account used, and the device used. It is important that staff are reminded that their actions are being monitored as it promotes best practice. They also need to know that breaches of data protection policies can lead to disciplinary action.
What to do	Decide how to inform staff that they are being monitored. This can be part of the employee induction, face to face or digitally. You could use an annual email reminder, a Windows banner, a Windows background, screensaver or posters. We have provided draft clauses for your staff code of conduct. Select the tick box to confirm that your staff have been told that they are being monitored to complete this evidence item.

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

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

5.1.1 Dates of process reviews held to identify and manage problem processes which cause security breaches.	
Overview	'Processes' are the approved ways of working in your organisation. These are in your organisation's policies and procedures. e.g. You will have a procedure outlining how to safely dispose of confidential documents. If this procedure is not followed correctly this might result in a data breach as the data has not been securely destroyed. For the purposes of the DSPT, we are only interested in processes to do with data security and protection. Review the policies and procedures you implemented in 1.2.1. at least annually. There are examples of the type of processes that cause incidents and workarounds in the Big Picture Guide for Standard 5.
What to do	Review each process at least annually. This is a minimum not a maximum. Follow the same procedure for these reviews as with your annual policy reviews. In small organisations these reviews might be done by one person. However, where possible, a group should do the review. The number of participants will vary dependent on your organisation size. Think logically about who would provide the best input so that you can make the best use of your time. You should always look for staff input. The review should be a frank and honest look at where processes can be improved and streamlined. Focus on the root causes of any workarounds. The outcomes from the reviews will result in a list of actions. These actions should be monitored and assurance given to senior management. There are examples in the Big Picture Guide. Confirm that processes are reviewed at least annually in the free text box to complete this evidence item.

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.	
Overview	All staff are responsible for noticing and reporting data breaches. They should report to the Data Protection Champion. The Data Protection Champion will investigate in more detail. **The ICO is the regulator for data breaches not CQC.** If you are unsure whether to report something to the ICO (see 6.2.4 for more details) it is always better to overreport than to underreport. This shows proactive risk management. Some types of data security incident are: • disclosure or loss / theft of information; • inappropriate access and / or modification; • cyber-attacks on IT equipment / data; • obtaining information by deception; • human error; and • inappropriate processes. There are three goals for data security 1. <u>Confidentiality:</u> ensuring that information is not disclosed – either purposefully or accidentally – to people who don't have the right to see it. Normally when people talk about data breaches they mean confidentiality breaches. 1. <u>Integrity:</u> ensuring that data is accurate and unchanged. A good example is a care plan – we need to know who has inputted the information (so they are accountable for it) and that the record is accurate.

	For example, if there is missing or incorrect data in your care planning system – electronic or paper based - this could potentially cause significant harm to an individual. 2. Availability: to be useful, data needs to be available to those who are authorised to see it. A breach can be caused when – either maliciously or accidentally – data cannot be accessed by those who need it. For example, ransomware attacks on computers – a hacker locks you out of your device until you pay the ransom to have your data unlocked. If any of these are compromised, then there is a data security incident. If the incident also involves personal confidential information it can also be a data breach. Data breaches must be reviewed to see if the ICO or other parties must be notified. **An incident may involve digital and/or paper-based information**. It could involve one piece of equipment or a thousand, one personal record or millions. Some incidents are also data breaches, i.e. any failure to meet the requirements of the Data Protection Act, including but not limited to an unlawful disclosure or misuse of personal data. Such as when emails containing sensitive information have been sent to the wrong address, data is shared without consent, or peoples' records are misplaced or lost. Not all incidents are necessarily data breaches, e.g. a cyber-attack that brings down a system for a short time but does not access any information or have significant negative effect on services.
What to do	It is vital that you have a robust reporting system in your organisation. Your incident reporting system should make sense for your organisation. It should be streamlined so that the process can be managed appropriately. Have one simple reporting form – no more than two pages but preferably only one, with as few questions as possible. It should be in hard copy (and digitally if this makes sense for your organisation). We suggest that the required information is no more than: • date • location • short summary of what occurred

	• type of incident – e.g. e-mail, lost USB device or paper • contact details for obtaining further information. We have a template reporting form. All staff are responsible for reporting security incidents to the Data Protection Champion who will then investigate further. Your reporting system might be like your existing incident reporting in other business areas. There is an incident reporting tool within the DSPT which you can use to document incidents. You do not have to use this tool unless the ICO needs to be informed of the data breach, but it can be good to get into the habit of using it. Under GDPR, it is a legal requirement to notify the ICO within 72 hours if a breach is likely to result in a high risk to the rights and freedoms of an individual. The DSPT's incident reporting tool will automatically tell the ICO for you if the incident is rated as serious enough. If you are not sure whether to inform the ICO or not, the incident reporting tool and guide can help you to decide. It is better to overreport and be told by the ICO that something doesn't need to be investigated than to not tell the ICO. The DSPT incident reporting tool is a notification tool only. Once you have reported the incident via the tool you will need to deal with the ICO directly. It is a legal requirement that if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. Select the tick box to confirm that you have a data security breach reporting system in place to complete this evidence item.

6.1.3 List of all data security breach reports in the last twelve months with action plans.	
Overview	See 6.1.1.
What to do	Keep a list of all data security breach reports which have happened in the last 12 months with their action plans.

	Remember to redact the name of the person who reported the breach and any details which can identify individuals or could damage your organisation's data security. You do not need to upload this document. Select the tick box to confirm that you keep a list to complete this evidence item. If you have not had any breaches in the last 12 months, you can record "none" in the comment box and select the tick box to complete the evidence item.

6.1.4 The person with overall responsibility for data security is notified of the action plan for all data security breaches.	
Overview	See 6.1.1.
What to do	Select the tick box to confirm that the person with overall responsibility for data security has been informed of the action plan. This might be your SIRO or the person with the equivalent job role. If you have not had any breaches in the last 12 months, then select the tick box. Put "n/a" in the comment box to complete this evidence item.

6.1.5 Individuals affected by a breach are appropriately informed.	
Overview	6.1.1.
What to do	If you have had a data breach in the last 12 months which is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform the individual(s) as soon as possible. Select the tick box to confirm that you have informed them to this evidence item. If you had no breaches which affect individuals, select the tick box. Write "n/a" in the comment box to complete this evidence item.

6.2. USERS KNOW HOW TO SPOT AN INCIDENT AND WHERE TO REPORT IT, AND INCIDENTS ARE EFFECTIVELY REPORTED.

6.2.4 Number of breaches that have been reported to the Information Commissioner	
Overview	Under GDPR, it is a legal requirement to report some data breaches to the ICO within 72 hours. The time starts when you discover the breach. You need to report the breach if it is likely to result in a risk to the rights and freedoms of an individual or individuals. If you decide you do not need to report this to the ICO then document your decision. If you decide you do need to report this to the ICO then use the DSPT incident reporting tool to do this. There is more information on how to use this tool in 6.1.1 above. The ICO have more guidance. It is better to overreport if you are uncertain, than risk not reporting something which you have a legal requirement to report.
What to do	Write the number of breaches you have reported to the ICO in the last 12 months in the text box. If you have not had to report any breaches write “0” to complete this evidence item.

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

6.3.1 Name of anti-virus product.	
Overview	As well as reacting to any data breaches, it is important that we are proactive to prevent them from happening. This is done with solutions such as antivirus software. Some organisations, which use a lot of technology, may have a specific person or department with responsibility for updating antivirus software. Smaller organisations may use the automatic updates which the antivirus software does itself. Antivirus software can be found either free or very cheaply online. Often it comes with your computer.
What to do	Make sure that each desktop computer, laptop or tablet is protected by antivirus software which is automatically updated. There is guidance on antivirus software in our Introduction to Cyber Security. Write the name of the software supplier, product name and version type of your antivirus software(s). Briefly cover the scope of the antivirus e.g. does it cover your email and your files?

6.3.2 Number of alerts recorded by the AV tool in the last three months.	
Overview	Every time your antivirus software spots a threat or potential threat to your system, it will record an alert. These alerts often pop up on your computer, so you should recognise them. Your antivirus software should have a dashboard where you can see the number of recorded alerts over a specific period. If you have external IT support or an IT supplier, then they may be able to help you with this evidence item.
What to do	Provide the number of alerts which your antivirus has recorded in the last 3 months to complete this evidence item.

6.3.4 Number of spam emails blocked per month.	
Overview	If your organisation has an email system, make sure that you do not send any sensitive personal information via email unless it is secure. NHSmail is a free secure email solution which is available to social care providers, there is more information here. If you do not use NHSmail and would like information on how to ensure your email is secure then there is guidance available here. Email has many benefits and can improve organisations' efficiency. However, there are issues which arise from using email. To make sure you are as protected as possible: • make sure staff are trained in safe use of email; • have a spam filter; • make sure that all email users have robust passwords. This evidence item is interested in spam email filters, which can be sourced from a shop, online or from an IT supplier.
What to do	**Note that if you use NHSmail this will be monitored for you** You should have a filter in place to block spam emails from coming through to your main inbox. In some email systems your spam or junk email might be automatically filtered into a separate junk or spam folder. Our Introduction to Cyber Security has more information on spam filters. Record how many emails in the last month have been blocked by spam filters. Remember, this is not just your personal email address but the addresses of everyone in your organisation who has an email address.

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

7.1. THERE IS A CONTINUITY PLAN IN PLACE FOR DATA SECURITY INCIDENTS, AND STAFF UNDERSTAND HOW TO PUT THIS INTO ACTION.

7.1.1 There is an incident management and business continuity plan in place for data security and protection.	
Overview	It is likely that your organisation already has a business continuity plan in place for emergencies. There is advice on this on our website. You have probably already considered some aspects of data security, e.g. what you would do if there was a flood or fire and you couldn't access care notes. It is important that you also consider what would happen if your phone line or broadband went down. What workarounds would you use? The 2017 WannaCry attack made it clear that health and care organisations are vulnerable to cyber-attacks. Your organisation needs to have a plan if something similar were to happen again. Your business continuity plan for data security should cover both digital and paper data. This ensures your staff know **What to do** to maintain continuity of care.
What to do	There is a specific guidance document and checklist on our website to help you complete your business continuity plan. Select the tick box to confirm that you have an incident management and business continuity plan in place to complete this evidence item.

7.2. THERE IS AN EFFECTIVE ANNUAL TEST OF THE CONTINUITY PLAN FOR DATA SECURITY INCIDENTS.

7.2.4 All emergency contacts are kept securely, in hardcopy and are up-to-date.	
Overview	When there is an incident it is essential that people within your organisation know who to contact. Keep a hard-copy, up-to-date emergency contact list. It is important that you know when it was last updated and printed. Consider where to keep copies of the contact list, especially in a scenario that affects access to the site. Consider keeping a copy on an appropriate cloud service. Review and update the contact list regularly. When updated the contact list should be reprinted.
What to do	Select the tick box to confirm that you have got an emergency contact list which is kept securely, up-to-date and in hardcopy to complete this evidence item.

7.2.5 Location of hardcopy of emergency contacts.	
Overview	See 7.2.4
What to do	Provide the location of where the emergency contact list is kept in your organisation. If you also keep a digital copy, then please provide the link too.

7.2.6 Date emergency contact list updated.	
Overview	See 7.2.5
What to do	Provide the date that the emergency contact list was last reviewed. This needs to have been within the last 12 months.

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.

8.1.1 What software do you use?	
Overview	It is important that you know what kinds of software you use in your organisation. Review this at least annually. This ensures your software is still supported so that you are not opening your organisation up to risks without realising it. See 8.2.1. for more detail on what is meant by “supported” or “unsupported” software.
What to do	Record what IT you have in your organisation and what operating system it is running. This can normally be found in your computer settings. For example, a desktop computer or laptop might have a Windows 7 or MacOS Sierra operating system. Once you have done this, consider what pieces of software you use on that machine. For most care providers this may include some or all of the following: • Payroll Software • Rota Software • Email Software • Microsoft Office / iWork • Care Planning Software • Training Software • HR Software Even in the smallest of organisations, it can be a challenge to think of a full list of all the different types of software that you use. It might be easier to use IT Asset Management software to assist with compiling your list or to speak to your IT support or supplier if you have one. There will be some overlap with the evidence required for this with your IAR (see 1.4.4). Your IAR will contain many of these details for the software you use which has personal data. You might like to extend your

IAR to cover the rest of your software, or you can use the following template or similar:

Software Name	Version Number	Is this software supported?	Risk Assessment	Mitigations

Prioritise this list. Start with the software which has the most risk to your organisation.

There is more information about unsupported software in our Introduction to Cyber Security.

To complete this evidence item, upload your list of software. Include version numbers and whether the software is still supported. If you don't upload the document, provide the location of where the document is kept.

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

8.2.1 List of unsupported software prioritised according to business risk, with remediation plan against each item.	
Overview	Software does not degrade over time. It does, however, become unsupported and therefore potentially vulnerable. Most widely available commercial software will have a support cut-off date. Once software is no longer supported, it is called "unsupported software". Unsupported software is no longer "patched" by the software owner. This means that it will no longer have security updates and that any bugs will not be fixed. The ramifications of using unsupported software will vary. Recently retired popular operating systems are a significant risk. Small bespoke packages are a lower risk. Generally, software will go through three phases: • active: current product fully supported and patched e.g. Windows 10 • limited: still patched for security though maybe not functionality e.g. Windows 7 (extended support ends 14th January 2020) • retired: system is unsupported, and you should migrate. e.g. Windows XP and Vista
What to do	On your software list from 8.1.1 you should have made a note if the software you use is supported or not. You may discover that you have unsupported software, but you cannot update it. If this is the case, risk assess the software. Make a record of why you are not upgrading the software e.g. too expensive, it will stop another piece of vital software from working etc. Ensure that you also record what mitigations you are using to protect the data which is held on this system. You may keep these risk assessments on the same document as you used for 8.1.1 You can reference the document which you uploaded for that. If you have kept this as a separate document, then please upload to complete this evidence item.

8.2.3 The person with overall responsibility for data security confirms that the risks of using unsupported systems are being treated or tolerated.	
Overview	See 8.2.1
What to do	Select the tick box to confirm that the appropriate person within your organisation has accepted the risks and mitigations in place (these should have been listed as per section 8.1.1) to complete this evidence item.

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

8.3.1 Provide your strategy for security updates.	
Overview	"Patching" or "patches" is another word for "updating". You need a strategy for implementing patches on a regular basis. For many organisations this might just be a case of allowing automatic patching (where your computers automatically update themselves). Sometimes staff can prevent automatic updates from happening because they are inconvenient. You should check to make sure that this isn't happening. You can schedule updates in your computer settings so that these only happen at convenient times. When you use automated patching, it is important that you follow up on any issues (such as where a patch cannot be applied to a specific computer). It is also good practice to check your results, you can do this with a product such as vulnerability scanner. There are vulnerability scanners freely available online. If you have an external IT support company, they might do this for you. Make sure you record what your policy is and keep it with your other policies and procedures.
What to do	Upload your plan for security updates for your organisation. This might be as simple as checking on a routine basis (perhaps monthly) that all automatic updates have been run and stating who is responsible for making these checks. If you have a lot of IT, speak to the person responsible for IT or your IT support about the details for this evidence item. There is additional guidance on patching in our Introduction to Cyber Security. NHS Digital have written guidance and a template policy on patching, but be advised that this is primarily aimed at larger organisations and it is complicated.

8.3.2 How regularly do you apply security updates to desktop infrastructure.	
Overview	See 8.3.1
What to do	Provide information on how frequently you run security updates on your computers to complete this evidence item. This might be a statement that you run automatic updates which are checked every month.

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 The person with overall responsibility for IT infrastructure confirms all networking components have had their default passwords changed.	
Overview	A computer network is one or more computers connected to the internet and possibly each other. Each device which is used to let computers talk to each other, i.e. create a network, is called a "network component". Networking components include (but are not limited to): • firewalls • switches and hubs • bridges • routers • wireless access devices. Many come with a generic password. This means that the password is available on the internet. This makes them very vulnerable to misuse. All network components need to have their default passwords changed. For many social care providers, you will probably just need to ensure that this is done for your router – the box you use to provide internet to your organisation. If you use a lot of IT, speak to the person responsible for IT in your organisation or to your IT support.
What to do	If you do not have an IT supplier or IT support, then look at the manual which came with your router. This will give you steps to follow to change your router password. Make sure the new password is a strong one. Our Introduction to Cyber Security contains more resources on networks. Confirm in the free text box that the person with overall responsibility for IT in your organisation is happy that all default passwords have been changed to complete this evidence item.

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.

10.1.1 The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.

Overview

You should know which of your suppliers handle your organisation's personal data digitally. This is simple for IT suppliers e.g. electronic care planning software. It's less obvious for suppliers who aren't providing you with IT, e.g. an external HR advisor.

Under GDPR, social care organisations are called "data controllers". Your suppliers are called "data processors". This is because you decide how and why your suppliers process the data or information you give them.

"Processing" is any way in which data can be used, stored, collected, created, destroyed or organised. As a data controller, you are expected to know and provide direction to your suppliers.

What to do

Record the products and services they deliver, their contact details and the contract duration. There is space for you to record this information in our template IAR (see 1.4.4 for more details). Or, if you would prefer you can use the template below:

Supplier	Products	Services	Contract	Start and end date
Care Planning System	Care Planning Product	Cloud based care planning system	C:\\Contract\IT\CPS	dd/mm/yy – dd/mm/yy
eRoster	eRoster Pro	Web based staff rostering system	\\sharepoint\contract\IT\eRoster	dd/mm/yy – dd/mm/yy
Outsourced HR advice	HR advice	Service to provide HR advice and guidance	Manager's filing cabinet	dd/mm/yy – dd/mm/yy

	Once you have completed this document, upload it or specify where you store it to complete this evidence item.

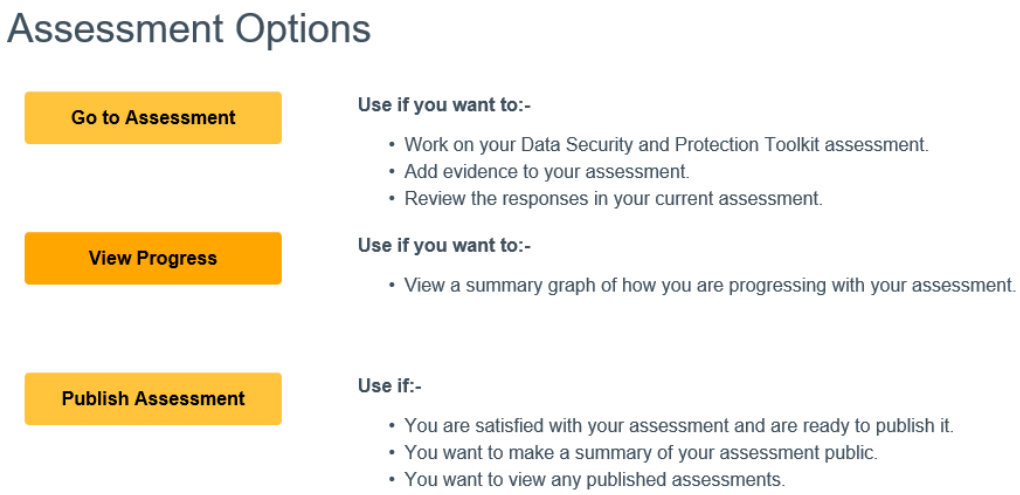
10.2. BASIC DUE DILIGENCE HAS BEEN UNDERTAKEN AGAINST EACH SUPPLIER ACCORDING TO ICO AND NHS DIGITAL GUIDANCE.

10.2.1 Basic due diligence has been undertaken against each supplier according to ICO guidance.	
Overview	Prior to starting a contract Before starting a new contract, undertake some due diligence so you are happy that they comply with data protection laws and the Data Security Standards. The ICO is the best place to check your potential suppliers. You can check the list of action taken by the ICO here.You can also check the news and sector specific publications. They may have details of breaches that are still under investigation by the ICO. You should check that potential suppliers are GDPR compliant. A way of checking GDPR compliance is to review the ICO checklist and the health and care GDPR checklist. During a contract Ask existing suppliers about their GDPR compliance. This can entail asking the supplier to complete the general ICO checklist or the health and care GDPR checklist (see above). If a supplier has their own plans for GDPR compliance, they should be checked against the ICO or health and care GDPR checklist to ensure completeness. This is especially important where you receive blanket assurances from suppliers stating that they are fully compliant in a relatively short time after GDPR has passed into law. Remember Plenty of organisations have changed following interaction with the ICO. Remember that because of the newness of GDPR, all the actions are likely to come from its predecessor, the Data Protection Act 1998.
What to do	Reassure yourself that your suppliers have demonstrated a sufficient level of compliance with data protection legislation for you to be happy working with them. The ICO have more guidance on contracts. We have created a checklist and guidance on approaching contracts with third parties. Select the tick box to confirm that you have undertaken due diligence activities and are satisfied to complete this evidence item.

Step Five: Publishing your assessment.

Only Administrator members can publish assessments.

1. Once you are satisfied that your assessment is complete click on the "*Publish Assessment*" button:



2. If you have missed any mandatory assertions you will be able to publish an 'entry level' submission. The DSPT will let you know if your submission is at 'entry level' rather than 'standards met'. To publish at 'standards met' level, complete the assertions you have missed and then come back to publish.

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: ig.feedback@careprovideralliance.org.uk