Data Security and Protection Toolkit: 'Entry Level' Guidance for Social Care Providers.

Contents

Glossary

CPA	Care Provider Alliance
CQC	Care Quality Commission
DPA	Data Protection Act 2018
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
IAR	Information Asset Register
ICO	Information Commissioner's Office
IG	Information Governance
KLOEs	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 'entry level' 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 and 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 the new 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 different levels of compliance with the DSPT. One of which, 'entry level', is only available to social care providers. This is because information governance, cyber security and the DSPT are new to the majority of the sector.

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.

Step One: Registering for the DSPT

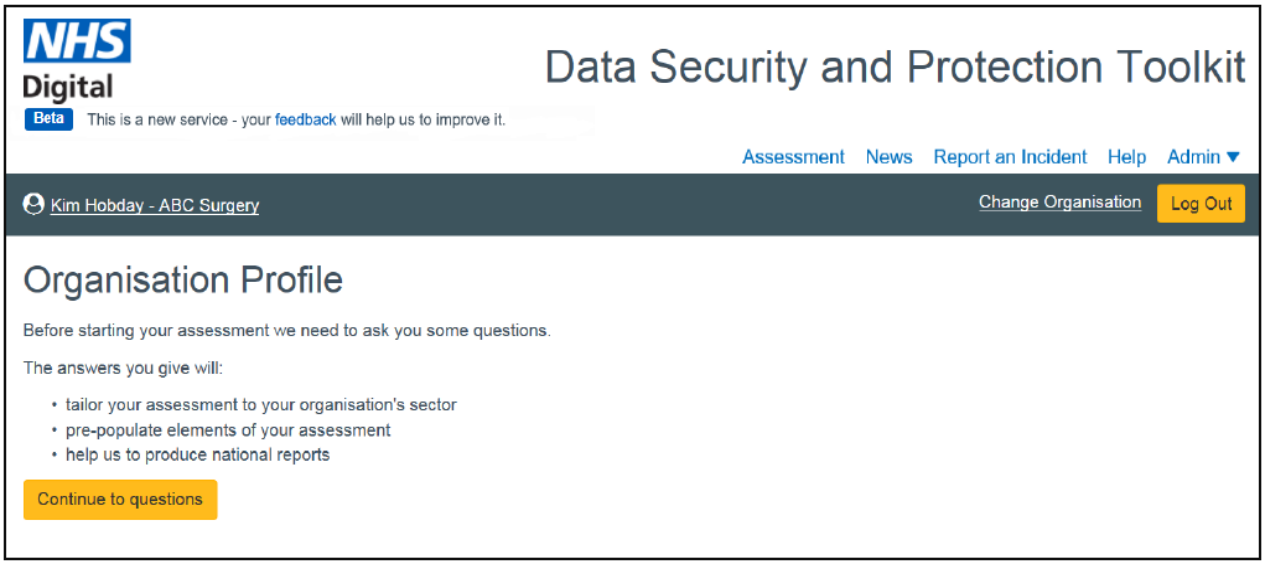
1. Go to https://www.dsptoolkit.nhs.uk/Account/Register
2. You will need your email address and your ODS Code (Organisation Code). If you don't know your ODS code, please contact exeter.helpdesk@nhs.net.
3. If you are registering your organisation for the first time, you will be the Administrator. You will be responsible for completing your organisation's profile and adding any other users.

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

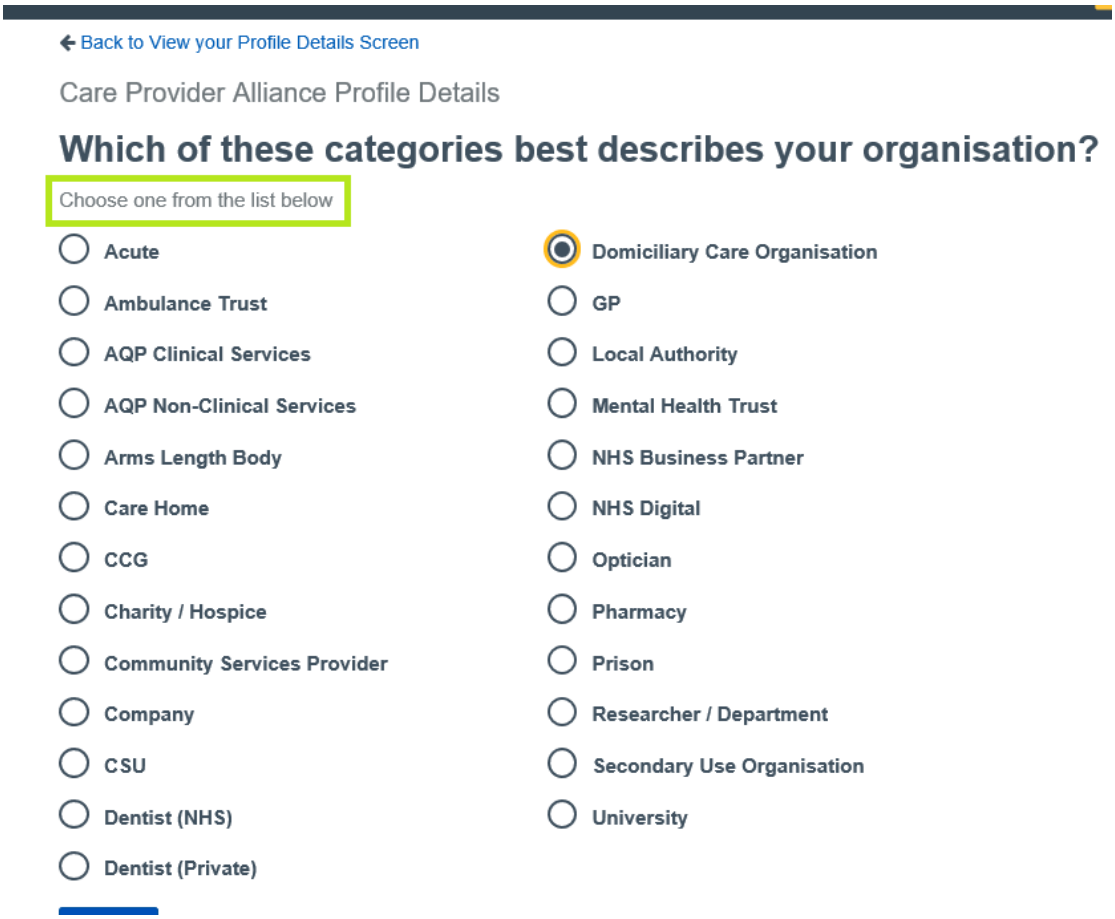
Once you have registered, you will need to sign in so that you can complete your organisation's profile.

1. Go to https://www.dsptoolkit.nhs.uk/Account/Login. The first time you sign in, click on the "*Forgot your Password*" button. This will allow you to set your Administrator password.
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 then be asked to fill in 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 in these sections. 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 what each role means in [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 select "Not Sure" if you are uncertain.

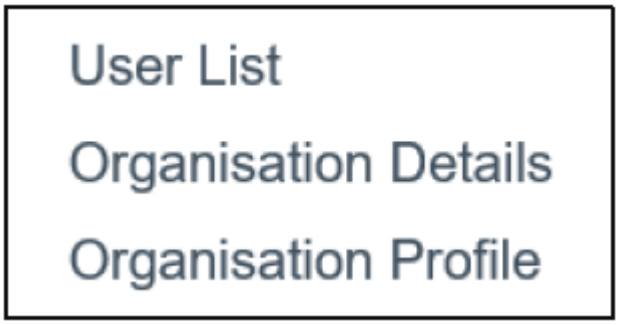
6. Check your answers and to make changes if necessary. Once you're happy, please click on "*Accept and Submit*". You will be able to go back and make changes at any point.

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.

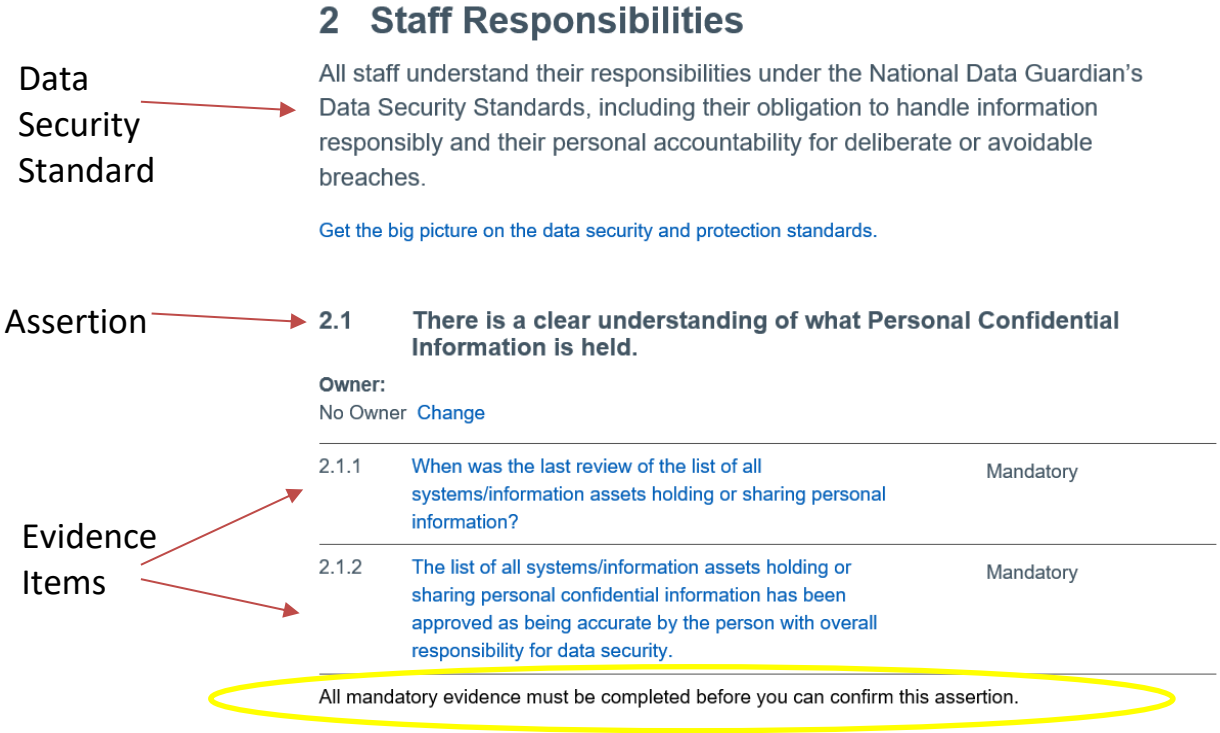
Step Four: Completing your entry level assessment

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.

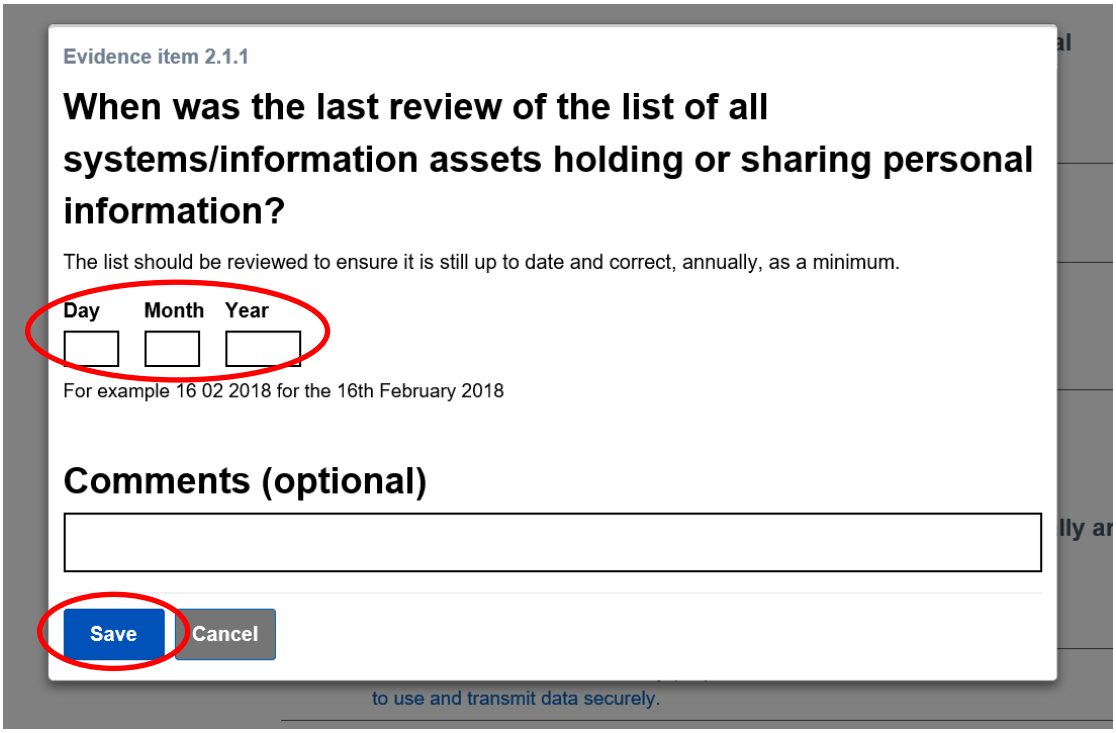
For 'entry level', you **do not** need to complete assertions. Just focus on the 16 evidence items required.



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

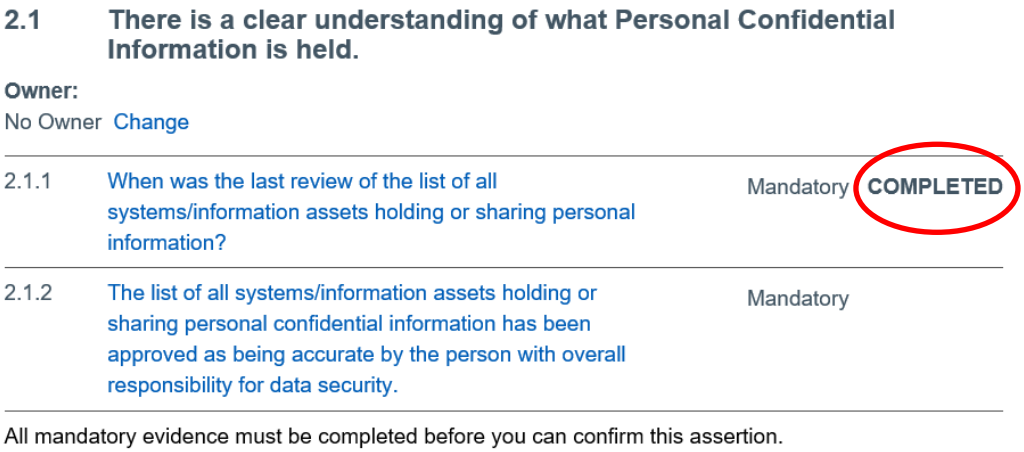
HOW TO COMPLETE AN EVIDENCE ITEM

To complete an evidence item, you should click on it. This will open a dialogue box which you should 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 then be as "*COMPLETED*".



COMPLETING YOUR ENTRY LEVEL ASSESSMENT

There are **16** evidence items which need to be completed for 'entry level'. These can be found in spreadsheet form on this link: https://www.dsptoolkit.nhs.uk/Help/32 or listed below.

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], except for courts acting in their judicial capacity; 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 (includes health and social care information) or data relating to criminal convictions and offences. If your organisation is considered a public body under the Freedom of Information Act (e.g. Local Authority/NHS owned care homes), then you must have, or have access to, a DPO. Large organisations will require a DPO or require access to a DPO – this can be a consultant role and does not have to sit internally. For small care providers it is less clear if a DPO is required 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 state exactly what qualifications a DPO should have. 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] 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.

	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 Information Commissioner's Office . 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: • 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 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.

	For small care providers: A small care provider could be characterised as having one or two sites, no dedicated staff in roles such as IT or HR 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. https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/ 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.

1.2.1 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 framework in place for data security and protection.

	The different sizes and complexity of organisations means 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 have to have on these topics, but it is important the policies are effective, acknowledged and understood.
What to do	Confirm that you have policies in place that explain your organisation's plan or principles 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.

1.2.3 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 Senior Information Risk Owner (SIRO) or someone in the equivalent role. A 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. 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.
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.

1.3.1 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. (There is advice on whether you need a DPO in section 1.1.6) Provide your ICO registration number to complete this evidence item.

1.3.3 How have individuals been informed about their rights and how to exercise them?	
Overview	GDPR contains stringent transparency requirements so that people are properly informed of 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 a privacy statement.

	As an extension of this privacy notice, 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	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. 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. There is a template leaflet to give to your service users here. Remember that the information has to be provided in a clear, concise and easily understandable manner.

	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.

1.4.1 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) – 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) – Records 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 information governance. Until data flows have been captured and mapped, they cannot be effectively risk assessed and secured against known risks.

What to do	In order to complete your ROPA you should 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 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 your organisation in the free text box.

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 • 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.

1.6.1 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 should be designed to take account of data protection and security issues from when they are first implemented. Your data protection by design procedures should aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent and (where possible) allows individuals to monitor what is being done with their data. These procedures should 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.

1.6.7 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 used in adult social care, but 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 categories 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, you should 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 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.

1.6.11 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. Select the tick box to confirm that all high-risk data processing has undergone a DPIA before starting to complete this evidence item. If you do not need to perform a DPIA, check the tick box to confirm and comment "n/a" in the comment box.

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.

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 an information asset register (IAR) – this is also mentioned in 1.4.1. If you have not completed the DSPT before, you might not have an IAR yet. An IAR should include a record of digital **and** hard copy records, who is responsible for ensuring the safety of the record, and what safety measures are in place. For example, you might look at your archived care records and decide that it makes most sense for your registered manager to be responsible for these records and that the safety procedures in place are that they are locked in a filing cabinet in a room which is locked when not in use. You should review this list periodically (at least annually) and amend if there are changes.
What to do	As a first step visit the section on our website titled "How to record what data we share and why do we need to do it?". This contains guidance on how to go about creating an IAR. There is also a template IAR which you can choose to use. Provide the date of the last time you reviewed your IAR, or its creation date, 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 a 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. You should 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.

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 role changes of staff, 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	You should maintain a list of all staff and their roles. This should be up to date and reflect when staff are recruited, their role change(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.

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, 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. Integrity: 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, that is a data security incident. If the incident 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 data breaches, i.e. any failure to meet the requirements of the Data Protection Act. This includes but is not limited to any unlawful disclosure or misuse of personal data, e.g. 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 also available 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. They will then investigate further. Your reporting system might be like your existing incident reporting in other business areas. There is a DSPT incident reporting tool you can use. You do not have to use this tool unless the ICO need to be informed of the data breach, but it can be good to get into the habit of using it. 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.

<table>
<tr><th colspan="2">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.</th></tr>
<tr><td>Overview</td><td>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 you give to 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.</td></tr>
<tr><td>What to do</td><td>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. If you would prefer you can use the template below:

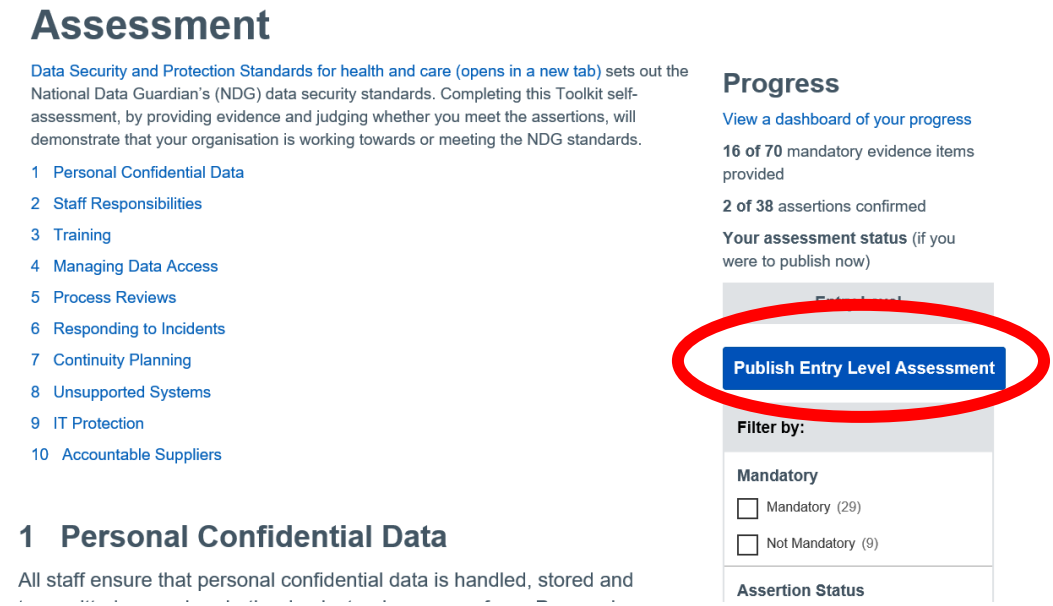
<table>
<tr><th>Supplier</th><th>Products</th><th>Services</th><th>Contract</th><th>Start/end date</th></tr>
<tr><td>Care Planning System</td><td>Care Planning Product</td><td>Cloud based care planning system</td><td>C:\\Contract \IT\CPS</td><td>dd/mm/yy – dd/mm/yy</td></tr>
<tr><td>eRoster</td><td>eRoster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

Once you have completed this document, upload it or specify where you store it to complete this evidence item.</td></tr>
</table>

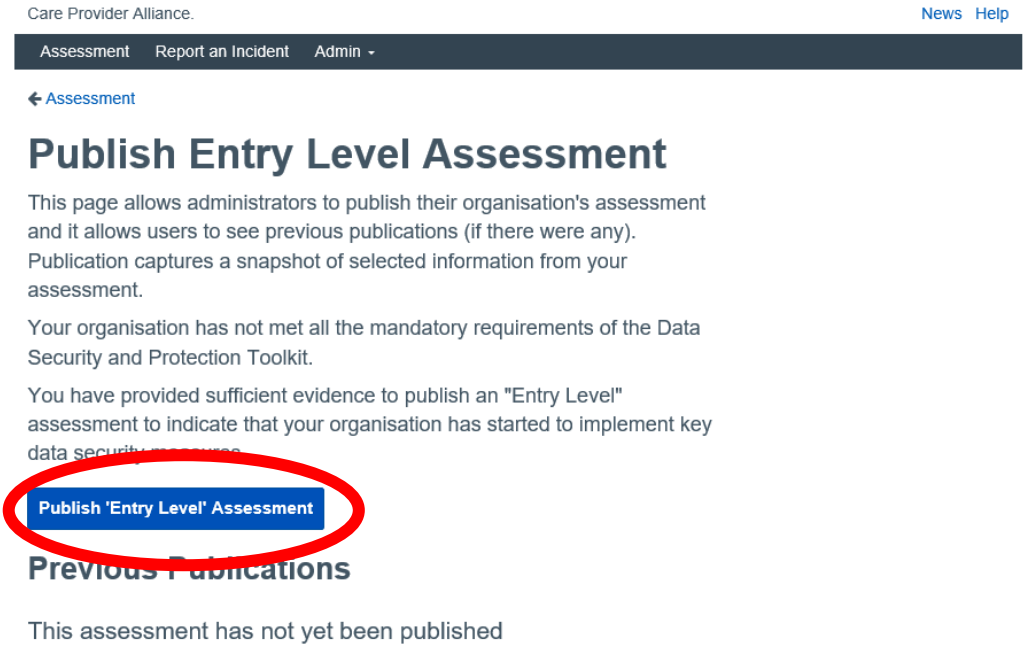
Step Five: Publishing your assessment.

Only Administrator members can publish assessments.

1. Once you have completed all of the 'entry level' requirements, you can publish your assessment. Click on the "*Publish Entry Level Assessment*" button:

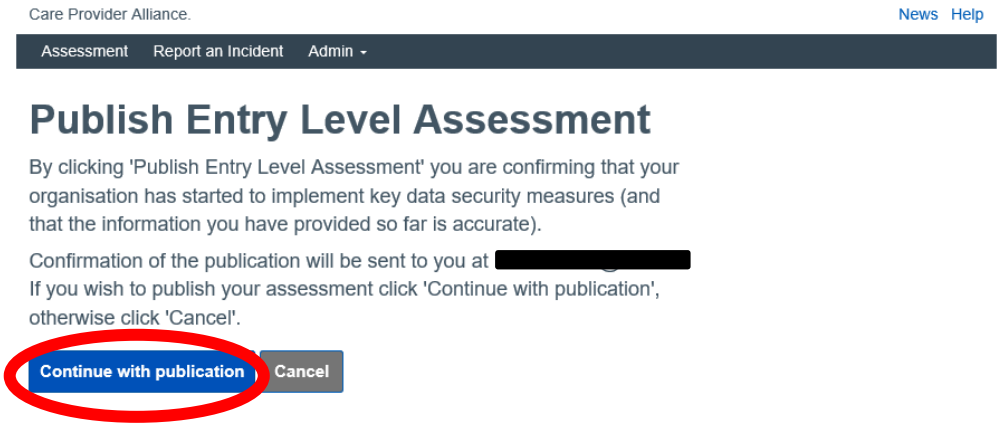


2. You will be reminded that you have not completed all of the requirements for 'standards met'. Click on the *"Publish 'Entry Level' Assessment"* button:



3. The DSPT needs you to confirm that you are happy to continue. Click the "*Continue with publication*" button. Once complete, you will receive an email confirming your submission has been

published:



4. After publication, you can **still continue** to work on your assessment if necessary

   You can make changes or start working towards 'standards met' compliance.

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