DSPT: ENTRY LEVEL WORKBOOK

Care Provider:

Registered Manager:

Table of Contents

An introduction to the workbook

Welcome to your Entry Level **'Data Security and Protection Toolkit'** workbook!

- This workbook outlines the **14 steps** you must complete for the **'Entry Level Assessment'.** This has been created for social care providers and publishing it allows you to sign up to and benefit from NHSmail.

- Each evidence item is clearly laid out in the workbook, with a 'notes' section for you to write down any questions you have along the way. These can be discussed during the webinars we will be running after the workshop. There is additional space for notes at the end of each section too!

- Before you start, think about what you may have already done or created regarding data protection. **This may include staff training, updating policies or keeping track of your data processes.** Don't worry if you have not done any of these already, it's just worth checking.

- Throughout the DSP Toolkit you will be asked to submit 'evidence', this will be asked for in the following formats:
  - Uploading a document
  - Entering text directly to the website
  - Ticking a checkbox

- Useful **templates** are available to help you complete each evidence item. You will need to edit these so that they are specific to your organisation. We recommend you store all of the templates and finished policies in a secure and easily accessible location for future use. Store these digitally or physically, whichever works best for you and your colleagues.

Note: When you are working through the evidence items on Data Protection, Data Quality and Data Security, you can create just one policy to cover all of these!

Data Security and Protection Toolkit: A Walkthrough

01 Registering

1. Go to: https://www.dsptoolkit.nhs.uk/Account/Register
2. You will need an email address and your site's ODS Code (Organisation Code). If you don't know this code you can find it on the ODS portal: https://odsportal.hscic.gov.uk/Organisation/Search If you are still having trouble, please contact exeter.helpdesk@nhs.net
3. If you are registering your organisation for the first time, you will become the administrator. You will be responsible for completing your organisation's profile and adding any other users.

02 Completing your profile

1. Go to: https://www.dsptoolkit.nhs.uk/Account/Login
2. The first time you sign in, click on the "*Forgot your Password*" button. This will allow you to set your administrator password.
3. Click on "*Continue to Questions*" on the following screen.
4. If you need guidance on completing the organisation profile questions, this is covered on the next page.

03 Provide Evidence

1. To publish at **"Entry Level"** on the DSPT, you must complete the 14 evidence items detailed in this workbook.
2. There is no specific order required to complete these. The system will autosave at regular intervals.
3. The remainder of the workbook will help you identify what should be provided for each evidence item.
4. Once you have added the evidence, click save on the dialogue box. This will mark the section as complete.

04 Publish your Entry Level DSPT

1. Click "*Publish Entry Level Assessment*" on the right
2. Click "*Continue*"
3. Click "*Publish*"
4. You will receive an email confirming that you have published!

Completing your Organisation Profile

01 Sector Information

1. First you need to choose your organisation type- you can only choose one.
2. 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.
3. Click **"Continue"**

02 Key Roles

Next, you will be asked to fill in who has the following roles in your organisation:

1. Caldicott Guardian
2. Senior Information Risk Owner
3. Information Governance Lead
4. Data Protection Officer

You do **not** have to enter any details in these sections. If you click **"Continue"** you will move on to the next page. These roles are not common in small social care providers.

03 Mail System/Cyber Essentials

You will be asked if your organisation:

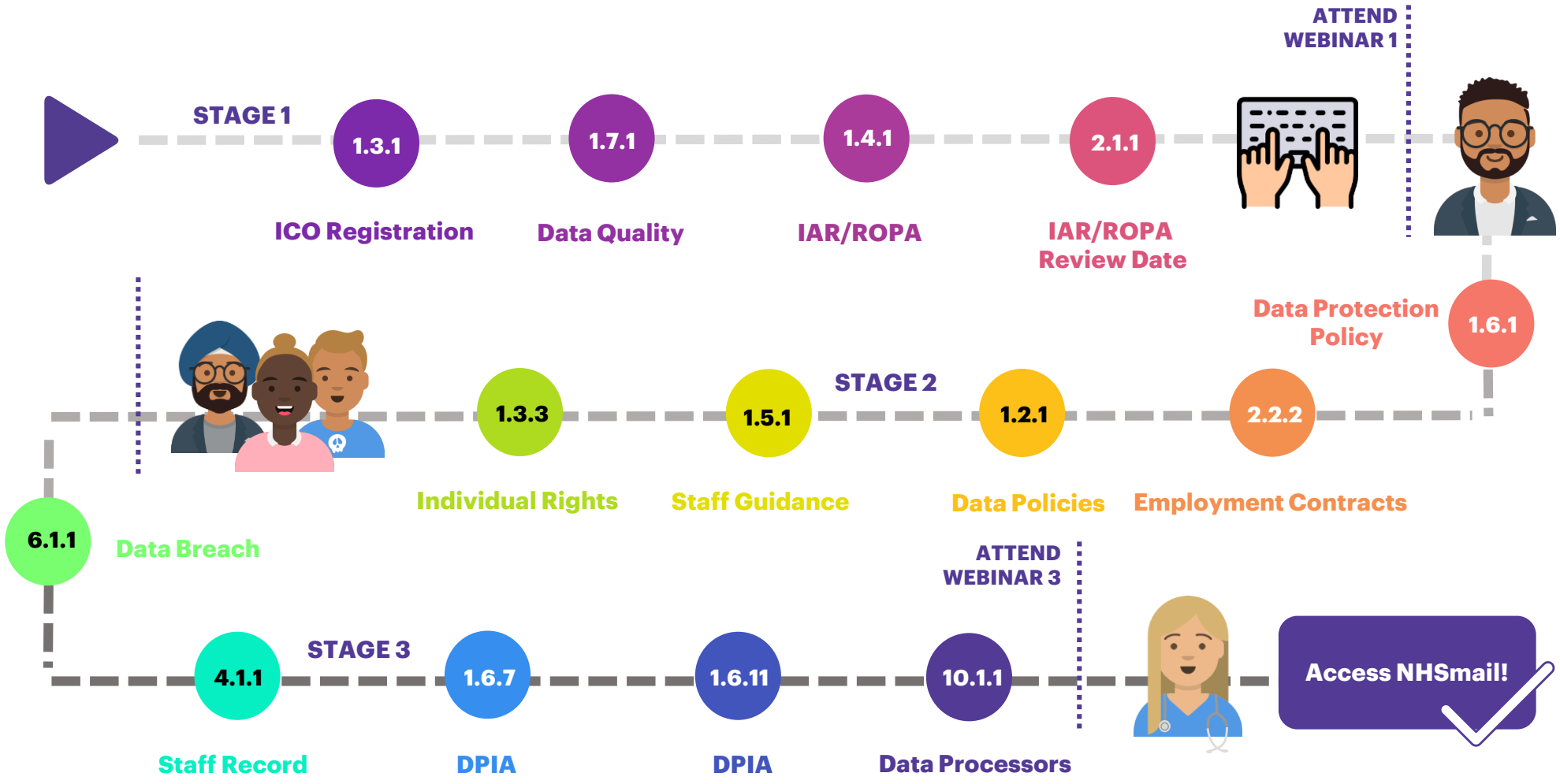
1. Has an NHSmail account: select **"No"**
2. Has a Cyber Essentials Plus certification: If you are uncertain, select **"Not Sure"**
3. Click **"Continue"**

04 Submit your Profile

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

DSPT Entry Level Assessment – What do I have to do?

For **"Entry Level"** we recommend completing the 14 evidence points in the following order. Once these steps are completed, you will be able to sign up for NHSmail. If you have specific questions after each stage, we recommend attending a webinar.



Timeline


Get Started Workshop
2 Weeks
4/14 evidence items completed!
Webinar 1
Webinar 2
2 Weeks
9/14 evidence items completed!
1 Week
Webinar 3
Completion workshop!
1-2 Weeks
All Entry Level evidence items completed!
NHSmail!
START

The layout of your workbook

The title of the evidence item, as it appears in the DSPT

Evidence code – the number of the evidence point as it appears in the DSPT

X

Title

Simplified title of the evidence point

Overview

Brief overview of what this evidence item is all about

To do

The actions you need to undertake for each evidence item

- https://ico.org.uk/registration/new

Notes

A section to fill with notes to help you along the way

Use these to help you keep track of where you're up to

To open links in the workbook left click on the underlined text. Alternatively, just type the link in to your internet browser

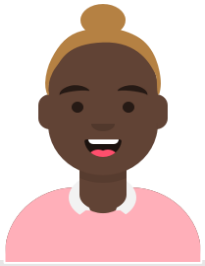
*Please note that if the link contains block capitals you will need to put capital letters in the browser

**Some links may download files automatically

What is your Information Commissioner's Office (ICO) Registration Number?

1.3.1

Register with the ICO



Overview

The Information Commissioner's Office (ICO) is the regulatory body for data protection.

Every organisation holding personal information is legally obliged to register with the ICO and pay a small registration fee (most care providers will already be registered).

If you are part of a larger group, head office are likely to be registered so you may need to contact them to check.

To do

- If you are not registered, register by following this link: https://ico.org.uk/registration/new
- If you think you are registered, but are unsure of your ICO number, you can search the ICO register for your ICO number via the following link: https://ico.org.uk/esdwebpages/search
- To complete this evidence point enter your ICO registration number.

Notes

Is there a policy and staff guidance on data quality?

1.7.1

Data Quality Policy

Overview

Social care providers are required to keep records that are accurate, up to date and audited.
Data records must be regularly checked to make sure data quality is maintained.
Staff must make sure data records meet the following criteria:

- **Authentic** – Data is what it claims to be.
- **Reliable** –Records are accurate, complete and up to date.
- **Integrity** – Changes are clearly marked and the person who made the change is clearly identified.
- **Useable** – Records are kept in an easily accessible place.

To do

- Use the template below to create a data quality policy that is specific for your organisation and make sure your staff are familiar with this (via training).
- **Data Quality Policy Template:** http://bit.ly/DSPTpolicies
- Store this policy safely: either in a folder in your filing cabinet or in a specific location on your computer.
- To complete this evidence point, **tick the box** to confirm you have a policy and staff guidance on data quality.

Notes

Provide details of the record or register that details each use or sharing of personal information, including the legal basis.

1.4.1

IAR/ ROPA

Overview

Care providers are legally obliged to keep a record of all personal data they hold for staff and residents and the legal basis for doing so. This does not mean you must record every single time an individual's data is used or shared.

We recommend that you keep two registers:

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

To do

- You must create these two records and include all confidential data processed by your organisation.
- Templates of both an IAR and ROPA are available for you to use. These contain examples of the types of personal data your organisation may collect and legal reasons for processing it.
- Labelled versions of these templates are attached to this workbook.
- **Templates and additional guidance:** http://bit.ly/DSPTdataprocessing
  - How to document your data processing guidance
  - IAR Template
  - ROPA Template
- To complete this evidence point, **upload the documents** to the DSPT site, or note down where you store the documents.

Notes

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

2.1.2

IAR Last Review Date

Overview

The document created to maintain a list of systems/information assets holding or sharing personal confidential information in the previous evidence item (1.4.1) is called an 'Information Asset Register'.

The list should be reviewed and updated periodically.

To do

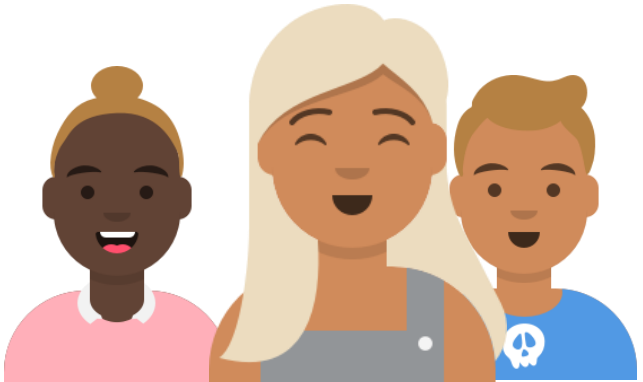
- Create an IAR or similar document if you do not already have one – This is covered on the previous page (evidence point 1.4.1).
- Make sure that your IAR is up to date and reviewed periodically.
- **Enter the date** of the last time you reviewed your IAR to complete this evidence point. If you created your IAR for the first time to complete your DSPT submission, then the date you created the document will be the one that you enter.

Notes

If you have any questions on these 4 evidence points, attend Webinar 1!

Email Contact:

Send any questions prior to the webinar to the email address above!



Notes

Notes

Is there an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements?

1.6.1

Data Protection Policy

Overview

Your procedures and systems should be created with data security in mind. Think of ways your procedures could be made more secure. It's not just about keeping a resident's information safe, it's also about ensuring the appropriate people can access it when they need to.

Procedures should aim to ensure that only the minimum necessary personal data is processed and that pseudonymisation is used where possible.

Pseudonymisation is the act of removing enough data from records to ensure that the individual cannot be identified without additional information from another source. If you replace patient names with unique codes when calling social services or similar, you are already doing this!

To do

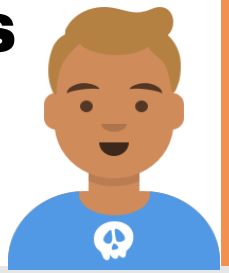
- To ensure this evidence point is met you need to make sure you have the relevant procedure in place and that staff members have been given enough guidance on the matter.
- **Data protection policy template:** http://bit.ly/DSPTpolicies
- Select the **tick box** to confirm that you have this policy in place to complete this evidence point.

Notes

Do all employment contracts contain data security requirements?

2.2.2

Employment Contracts



Overview

All employment contracts must contain an explicit clause which outlines employee responsibility for data security, which involves ensuring the confidentially, integrity and availability of data.

- **Confidentiality** - data is not disclosed to people that do not have the right to see it.
- **Integrity** - all data is accurate and unchanged – for example in a care plan.
- **Availability** - data must be accessible to those authorised to see it.

To do

- Review your staff contracts to determine whether they need updating to include a clause on confidentiality.
- **Confidentiality clause template:** http://bit.ly/DSPTstaffguidance
- It is important for you to explain to your staff the implications of not following data protection policies (possible disciplinary action).
- To complete this evidence point, select the **tick box** to confirm all employment contracts cover data security and confidentiality.

Notes

Are there approved data security and protection policies in place that follow relevant guidance?

1.2.1

Data Policies

Overview

Policies are one of the foundations of having a strong framework in place for data security and protection.

Policies will vary based on the size and complexity of your organisation. Some will have one policy covering all areas, whilst others may have multiple policies supported by standards and procedures.

There is not a set number of policies required, but it is important that your organisation's policies are effective, acknowledged and understood.

To do

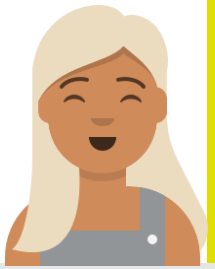
- Confirm you have Board approved policies in place for:
  - Data Protection
  - Data Quality
  - Records Management
  - Data Security
  - Network Security (This is not required for smaller organisations – instead record in your Data Quality policy a procedure detailing how **automatic updates** are completed on your computers and make sure your **WiFi password** is changed from the default).
- Please see our free, editable **template** policies and procedures if you need help: http://bit.ly/DSPTpolicies
- Select the **tick box** once your organisation has these policies in place to complete this evidence point.

Notes

Is there approved staff guidance on confidentiality and data protection issues?

1.5.1

Staff Guidance



Overview

It is important that your staff fully understand their responsibilities when dealing with confidential data.

You will need to have guidance for staff that explains what the policies mean and what you need them to do to help make sure everyone works safely within the law.

To do

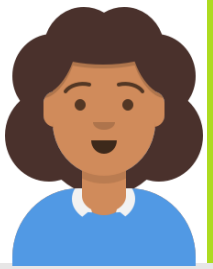
- Decide how to provide this guidance to staff: either via training or updating staff handbooks and contracts.
- Templates and guidance are available for:
  - Staff Data Security and Protection Code of Conduct
  - Guidance on Subject Access Requests and the Rights for Individuals under GDPR
  - Guidance on Data Sharing, Data Quality & Data Breaches
- **Templates and training for staff**: http://bit.ly/DSPTstaffguidance
- **Tick the box** once these are in place to complete this evidence point.

Notes

How have individuals been informed about their rights and how to exercise them?

1.3.3

Individual Rights



Overview

It is a **legal requirement** that you let individuals know:

- **What information** is collected about them
- **How** this is **stored**
- **Why** you store this information
- **Who** you **share** this information with
- **How long** you keep it for
- Their **individual rights**

This applies to patients, staff and also visitors to your care home, such as relatives.

To do

- One way to ensure you are complying with these legal requirements is by making a privacy notice.
- This privacy notice can be displayed on a page on your website, in a poster in your waiting room or a leaflet that you hand out. Whatever style you think will be most accessible for individuals that come into contact with your organisation.
- There is a privacy notice template available, which will need to be edited so that it is specific to your organisation.
- **Privacy notice template and example leaflet**: http://bit.ly/DSPTdataprocessing
- **Tick the box** once these are in place to complete this evidence point.

Notes

If you have any questions on these 5 evidence points, attend Webinar 2!

Email Contact:

Send any questions prior to the webinar to the email address above!

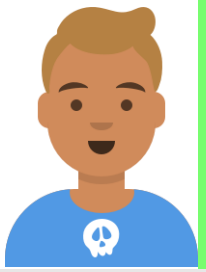
Notes

Notes

Is there a data security and protection breach reporting system in place?

6.1.1

Data Breach Reporting



Overview

All staff are responsible for noticing and reporting data breaches. Staff should report data breaches to the data protection champion who is responsible for investigating the breach further and filling out a record of the data breach.

Examples of incidents include emailing confidential data to the wrong person or losing a USB memory stick that holds sensitive data. Furthermore, if a manager were to lose the key to a filing cabinet holding personal data, this would also be a breach as access to essential information is disrupted.

It is essential that there is a system in place for reporting these breaches.

To do

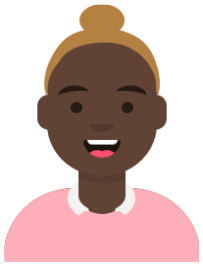
- Create a data breach reporting system. This is similar to fostering a Health & Safety culture through accident books. Accidents happen so it's safer to have measures in place. If in doubt, always report and investigate then you can confirm or withdraw your report. There is a template for recording data breaches available below.
- **Recording Data Breaches Template:** http://bit.ly/DSPTpolicies
- Once the data breach is logged, the ICO must be informed within 72 hours. If the data breach could affect an individual's rights you must inform the individual as well.
- Note – there is a tool on the DSPT for reporting data breaches. Once the tool has been used, all relevant bodies like the ICO will be notified.
- To read more, further detail is available on page 20 of **the Entry Level Guidance:** http://bit.ly/EntryLevelGuidance
- This evidence point is about **creating a procedure** that can be used in case a breach occurs. **Tick the box** to confirm you have this in place.

Notes

Does your organisation maintain a record of all staff and their roles?

4.1.1

Staff Record



Overview

It is important to maintain a record of all current staff and their roles. This can help keep your data secure by only allowing employees with the correct clearance access to information.

This record might be linked to your existing payroll or rostering system.

To do

- Create a list of all staff and their roles. This should be up to date and include when staff started their role, any role changes, as well as if and when staff leave the organisation.

- If you have an up to date record then you can **tick the box** to complete this evidence point.

Notes

Is there a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance?

1.6.5

DPIAs: Part 1

Overview

Data Protection Impact Assessments (DPIAs) are essentially a risk assessment specifically focused on data protection and privacy. You should conduct a DPIA for any system or process that uses or shares personal data. It is good practice to complete a DPIA when you introduce a new system which could impact individuals' data rights.

You only need to carry out a DPIA for "large" data processing systems. If you decide not to perform a DPIA for a system, you must note down why you made this choice.

Care planning systems and CCTV cameras are likely to require a DPIA.

To do

- Decide who would be responsible for completing a DPIA and ensure that individuals understand the purpose of completing one. In smaller organisations this might be only one person.
- Have a procedure on how and when to complete a DPIA for each system that processes, stores or shares confidential data.
- A DPIA template and additional guidance can be found on the ICO website.
- **DPIA template**: http://bit.ly/DPIATemplate
- **Further guidance**: http://bit.ly/DPIAguide
- **Tick the box** to complete this evidence point, confirming you have a procedure for completing DPIAs in place.

Notes

Is a Data Protection Impact Assessment carried out before high risk processing commences?

1.6.6

DPIAs: Part 2

Overview

Once you have completed 1.6.5 you should be familiar with DPIAs, and have them in place for systems currently running in your home where necessary.

You are required to complete a DPIA for all new processing activities that are likely to result in a high risk to individuals. It is therefore good practice to complete a DPIA for any major project which requires processing personal data.

To do

- Ensure that you have completed any necessary DPIAs for your current systems – including your existing care planning system.
- Confirm that your organisation will add any new software you come across to your IAR
- Confirm that any new processing activity (e.g. adopting an e-care system) will be added to the ROPA.
- If you assess any of these additions to be high risk you will need to carry out a DPIA before you start using the process.
- **DPIA template**: http://bit.ly/DPIATemplate
- **Further guidance**: http://bit.ly/DPIAguide

- **Tick the box** if you can confirm this to complete the evidence item!

Notes

Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration?

10.1.1

List of Suppliers

Overview

You must keep a record of all third parties (suppliers) that handle personal information, the services and products they provide and details of the contract in place.

These third parties are called "**data processors**" because they 'process' the data you give them. For example, a Person Centred Software, offers a system called Mobile Care Monitoring- you must note down this company as a "data processor".

To do

- Make a list of all your suppliers. This should include providers of software or data handling services, but also those people that you contract or come to deliver services in your home (e.g. hairdressers and window cleaners.)
- Talk with them to understand what information they hold about your residents/staff, if they are GDPR compliant, and that they understand their contractual responsibilities to protect privacy.
- If you are unsure who handles personal information for your care home, ask your finance team as they may have a list of the suppliers that they pay.
- **Upload this document** or note down its location to complete this evidence point.

Notes

If you have any questions on these 5 evidence points, attend Webinar 3!

Email Contact:

Send any questions prior to the webinar to the email address above!

Notes

Notes

Adding New Users to your DSPT submission

- To add more users to your organisation to help you through the DSPT: Sign in to the DSPT and click on the *"admin"* tab in the top right of your screen. This will reveal a drop down menu. Select "*user list*".

- Once on the user list page, you can add more users. There are 3 types of users:
  1. **Administrator member** – access to view and edit everything.
  2. **Auditor** – access to view (but not edit) everything, they can reset their own password and update their personal details on the system.
  3. **Member** – access to view everything, can edit evidence points but not the organisation profile. They can reset their own password and update their own personal details.

- The **administrator member** should be the manager and possibly the Data Champion where this is a different person. This is advised as the administrator will have access and editing rights for everything.
- If you have **a local champion** (someone in the region who can help you with the DSPT) it might be a good idea to add them as an **auditor**. They can check the evidence you have uploaded is correct and keep track of your progress without having to travel to your home.
- If you are part of a care home group who deal with all security policy and contracts centrally, but completing the DSPT yourself with permission, it would be a good idea to **add someone from head office as a member**. This will allow them to upload evidence items such as parts of the data security policy to the DSPT! They will also be able to change policies for all care homes that are part of the group at once, saving you all time!

How to sign up for NHSmail

Congratulations! Now that you have submitted your Entry Level assessment of the DSPT, **you are able to sign up for and start using NHSmail.** The steps below will show you how to get going with NHSmail.
Additional support is available from https://support.nhs.net

You will need:

- **CQC Location ID**
- **CDC Contact ID**

1. Visit **https://support.nhs.net** in your web browser.

   Select **'Join NHSmail'** at the bottom of the page.

2. Select **'Registering a Social Care organisation e.g. a Care Provider or Care Home Service'**
   Click on the '**Online Registration Portal**' link under National Administration Service (NAS), or go directly to this web page: **https://portal.nhs.net/Registration#/careprovider**

3. You will be directed to a questionnaire:
   - **Do you already have an NHSmail account?** Select 'No'
   - **Have you completed the DSPT to entry level or higher?** If you have, select 'Yes'
   - **Have you received an email or letter with a One-Time Passcode within the past 2 weeks?** Select 'No' if you haven't requested this. You do not need this to sign up.
   - **Do you know your CQC Contact ID/Manager's ID?** You can find these numbers on your CQC certificates, or by contacting the CQC if you are unsure.

4. Enter your care home's postcode and select the name from the drop-down list.

   On the next page enter the CQC Location ID and CQC Contact ID (sometimes known as Manager's ID).

   These should be on your CQC certificates.

5. On the next page, enter your town name. This will form part of the shared mailbox email address.

6. Now, enter details for each staff member who will need an NHSmail account. Up to 10 accounts can be created initially.

   A current email address is needed to receive a link to log-in for the first time and a mobile number to send the first password to. If this number is personal, it can be hidden after receiving your password.

7. As you add users, at the top of the page, select **'Add access to shared mailbox account'** to give staff access to the shared email account.

8. Once completed, select **' Go'.** When the request has been sent, your staff members will start to receive their details by email and text.

How to set up your NHSmail account

Now you have received a text and an email from NHSmail telling you that you have a new email account... This is how to set up your account and get started!
Additional support is available from https://support.nhs.net

1. Click on the link which you will have received in a "Welcome to NHSmail" email.

   This email will contain your new NHSmail email address, and the details for your shared mailbox if relevant.

2. This will re-direct you to the NHSmail log in page.

   Log in using your new @nhs.net email address and the temporary password sent to your mobile phone.
   When logging in, tick **'This is a private computer'** if this is true to be able to download files.

   You will be asked to change your password and create a new one.

3. Once logged in, complete your profile on the My Profile tab:

   Check your mobile phone number (you can choose to hide this)

   Check your role: e.g. Registered Nurse

   Save your updated profile.

4. Create your security questions:

   On the portal, select **'My Profile'**

   Select **'Security Questions'**

   Choose three security questions to answer. Both questions **and** answers should be within 5-12 characters.

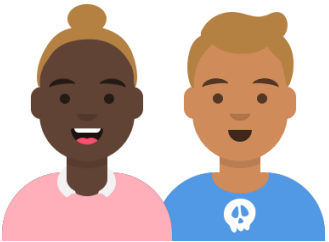
   Save your updated profile.

5. You will be asked to sign back in again, and accept the "Acceptable Use policy". **This step must be completed before you are able to send emails from your new account.**

6. You can now log into your account to send and receive emails!

   You can access your emails by going to **https://email.nhs.net** in your internet browser.

7. When you log in for the first time, click on your name in the top right corner and then **'Open another mailbox'** to switch to the shared mailbox. You should use this to send emails about resident's care, rather than your individual account.



Glossary

The following terms are used during the workbook, you can find the definitions here.

- **Data Processors –** Any third party that handles personal data associated with your care home. For example, a company who you hire to shred confidential documents.
- **DSPT** – Data Security and Protection Toolkit.
- **Entry Level –** Attained after completing the 14 evidence items detailed in this workbook. Required for NHSmail.
- **Standards met -** Achieved after completing every mandatory item. Other digital tools are available after this step.
- **Evidence Item –** The elements of the DSPT that you need to complete.
- **Assertion –** Subheadings in the form of statements. These are made up of individual evidence items. For "entry level" you do not need to worry about assertions.
- **GDPR** – General Data Protection Regulation – EU law, adopted by the UK, that provides certain legal requirements regarding protection of confidential data.
- **ICO** – Information Commissioner's Office – The regulatory office for all data regulation.
- **Pseudonymisation** – The act of removing enough data from records to ensure that the individual cannot be identified. This is done by using unique identifiers or codes when referring to patients over the phone or other unsecure networks.

Glossary

- **IAR** – Information Asset Register - A register of all important information the organisation keeps, from filed patient information to CCTV records.
- **IGL** - Information Governance Lead – 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.
- **DPIA** – Data Protection Impact Assessment - A process to help you identify and minimise the data protection risks of a project. The ICO provides guidance on this issue.
- **ROPA** – Record of Processing Activities – A detailed list of all instances of data processing and the legal basis for sharing this data.
- **ODS code** – Organisation Code.
- **SIRO** – Senior Information Risk Owner – Someone who understands, assesses and manages information risks. Someone at the highest level. Not essential for completing the DSPT at entry level.
- **DPO** – Data Protection Officer – The DPO advises the organisation on data protection matters, monitors compliance and is the touch point with the ICO (for more info follow this link): http://bit.ly/DPOinformation
- **Caldicott Guardian** – A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. They are not required for smaller organisations or may be included as part of another role. Information on the Caldicott Guardian: http://bit.ly/CaldicottGuardian

Help and Support

- Register for the Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/Account/Register
- FAQs including training tool https://www.dsptoolkit.nhs.uk/News/9
- DSPT support available through Exeter.helpdesk@nhs.net
- Toolkit training and update events https://www.dsptoolkit.nhs.uk/News/10
- Digital Social Care guidance https://www.digitalsocialcare.co.uk/latest-guidance
- ICO DPIA guidance - http://bit.ly/ICODPIAguide

Templates

1.2.1

- Data Security Policy http://bit.ly/DSPTpolicies
- Data Protection Policy http://bit.ly/DSPTpolicies
- Data Quality Policy http://bit.ly/DSPTpolicies
- Network Security Policy http://bit.ly/DSPTpolicies
- Record Keeping Policy http://bit.ly/DSPTpolicies

1.3.3

- Privacy Notice Template http://bit.ly/DSPTdataprocessing

1.4.1

- IAR Template, ROPA Template http://bit.ly/DSPTdataprocessing

1.5.1

- Staff Data Security Code of Conduct http://bit.ly/DSPTstaffguidance
- Guidance on Data Breaches http://bit.ly/DSPTstaffguidance
- Guidance on Data Quality http://bit.ly/DSPTstaffguidance
- Guidance on Data Sharing http://bit.ly/DSPTstaffguidance

1.6.1

- Data Protection Policy http://bit.ly/DSPTpolicies

1.6.5

- DPIA Template http://bit.ly/DPIATemplate

1.7.1

- Data Quality Policy http://bit.ly/DSPTpolicies
- Guidance on Data Quality http://bit.ly/DSPTstaffguidance

2.2.2

- Confidentiality Contract Clause http://bit.ly/DSPTstaffguidance

6.1.1

- Data Breach Reporting Template http://bit.ly/DSPTpolicies
- Guidance on Data Breaches http://bit.ly/DSPTstaffguidance

Notes