Completing the DSPT

DSPT
Better security.
Better care.

Digital Social Care

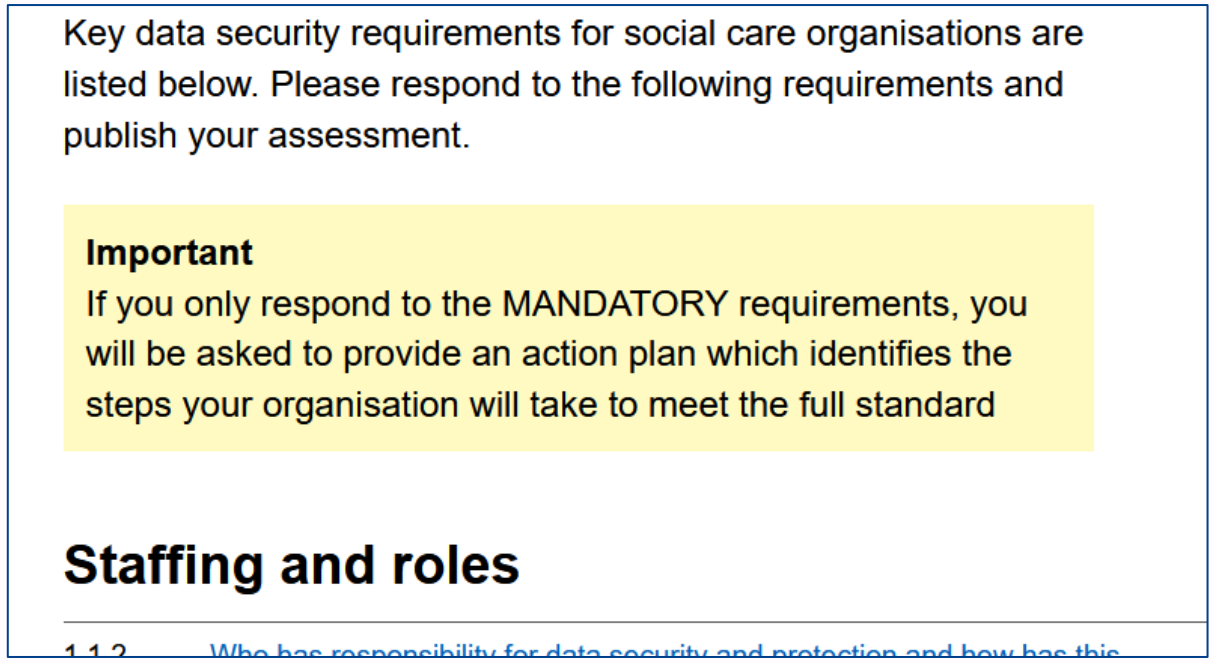
Varsha Modhwadia
Digital Project Manager
Lincolnshire Care Association

Lincolnshire Care Association | Lincolnshire Care Association

Completing the Toolkit

DSPT
Better security.
Better care.

Mandatory Questions are needed to complete to Approaching Standards Level. We will be completing all the questions to get to Standards Met. Once you publish at Standards Met you will not need to upload an Action Pan



Key data security requirements for social care organisations are listed below. Please respond to the following requirements and publish your assessment.

Important
If you only respond to the MANDATORY requirements, you will be asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

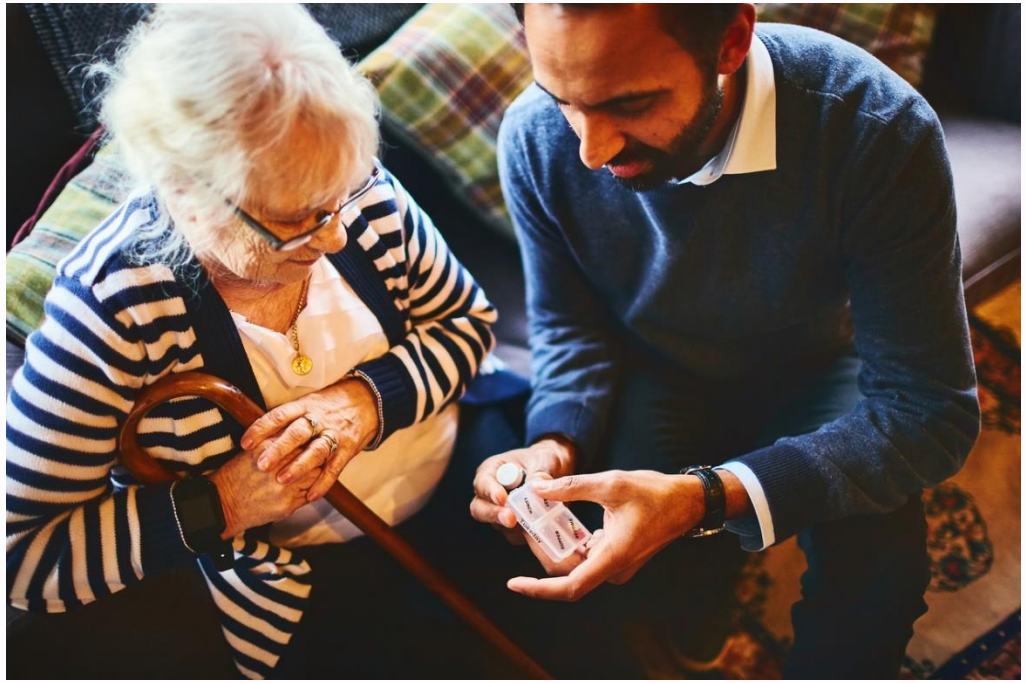
1.1.2 Who has responsibility for data security and protection and how has this

Lincolnshire Care Association | Lincolnshire Care Association

Agenda

DSPT
Better security.
Better care.

- The Standards
- Completing the Toolkit
  - Staffing and Roles
  - Policies and Procedures
  - Data Security
  - IT Systems and Procedures
- Publish the Toolkit
- Next Steps

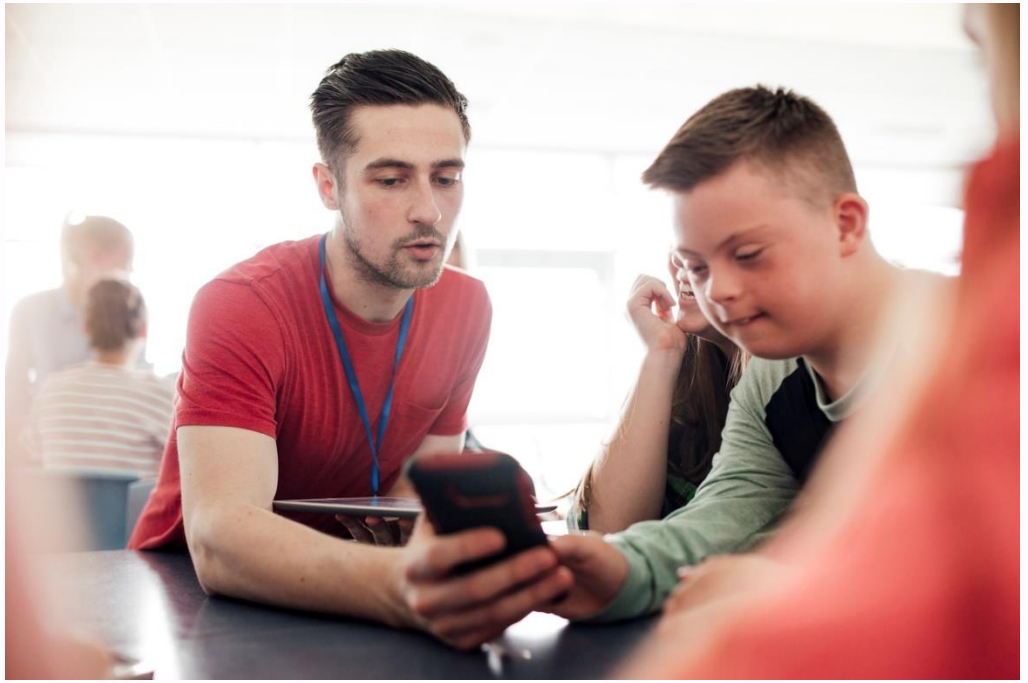


Lincolnshire Care Association | Lincolnshire Care Association

The Standards

DSPT
Better security.
Better care.

- Approaching Standards
- Standards Met
- Standards Exceeded



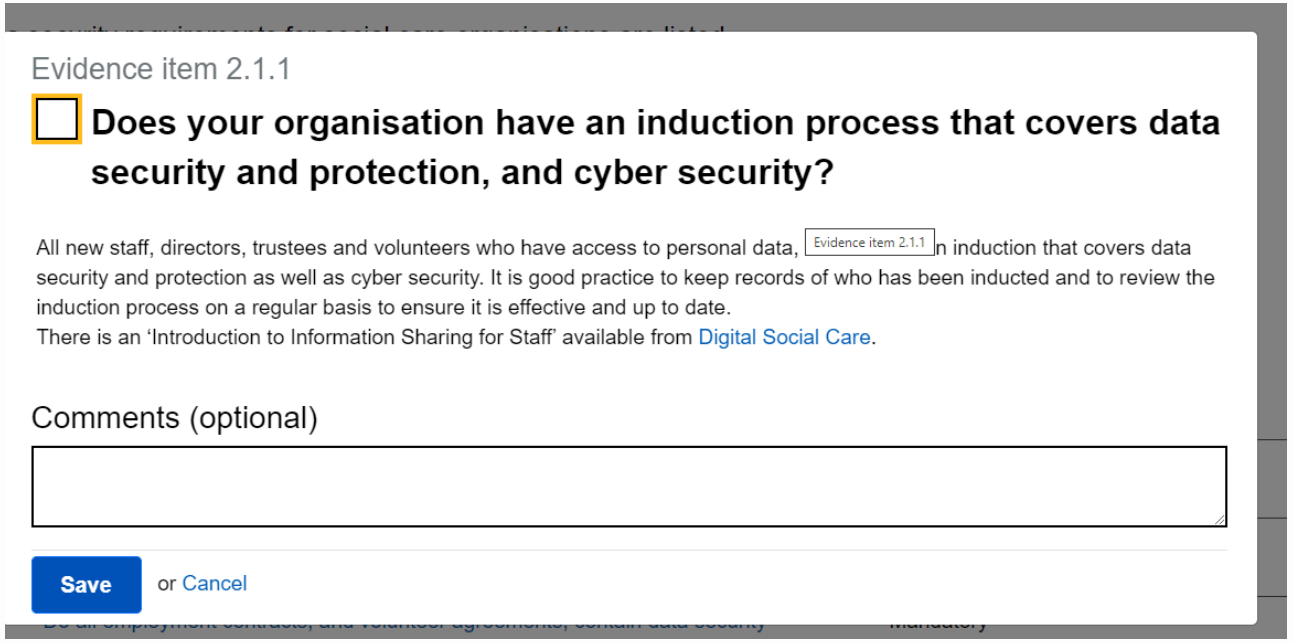
Lincolnshire Care Association | Lincolnshire Care Association

Completing the Toolkit

DSPT
Better security.
Better care.

Questions will follow these formats

- Tick Boxes (yes/no with comments – majority of questions)



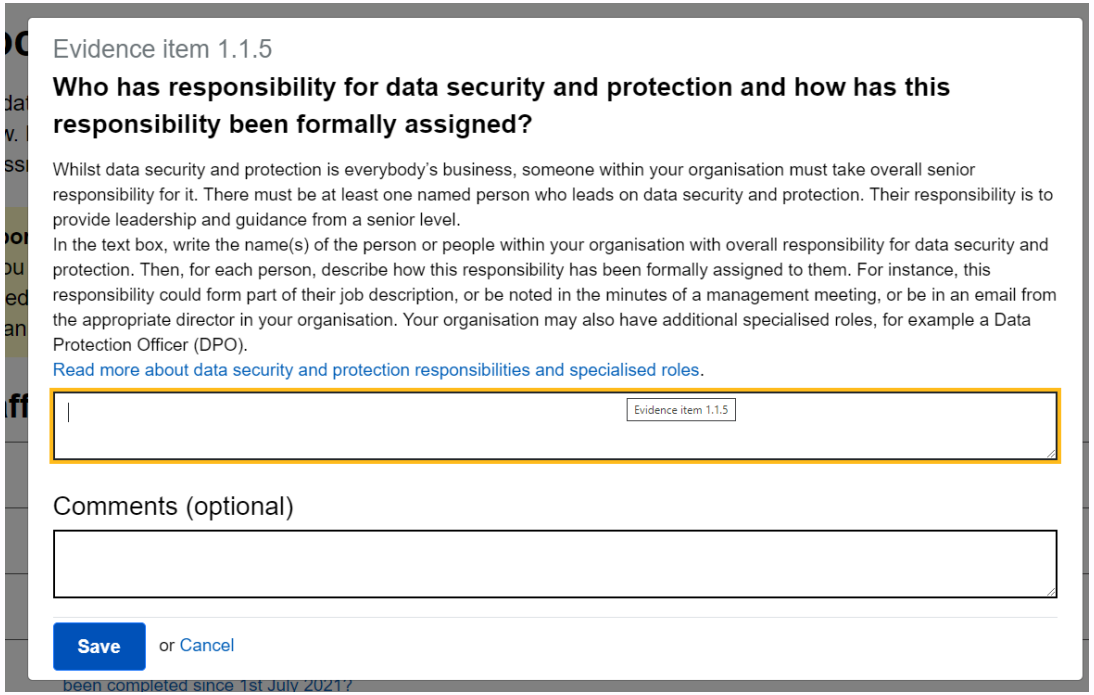
Lincolnshire Care Association | Lincolnshire Care Association

Completing the Toolkit

DSPT
Better security.
Better care.

Questions will follow these formats

- Text Box (need to make a statement)



Lincolnshire Care Association | Lincolnshire Care Association

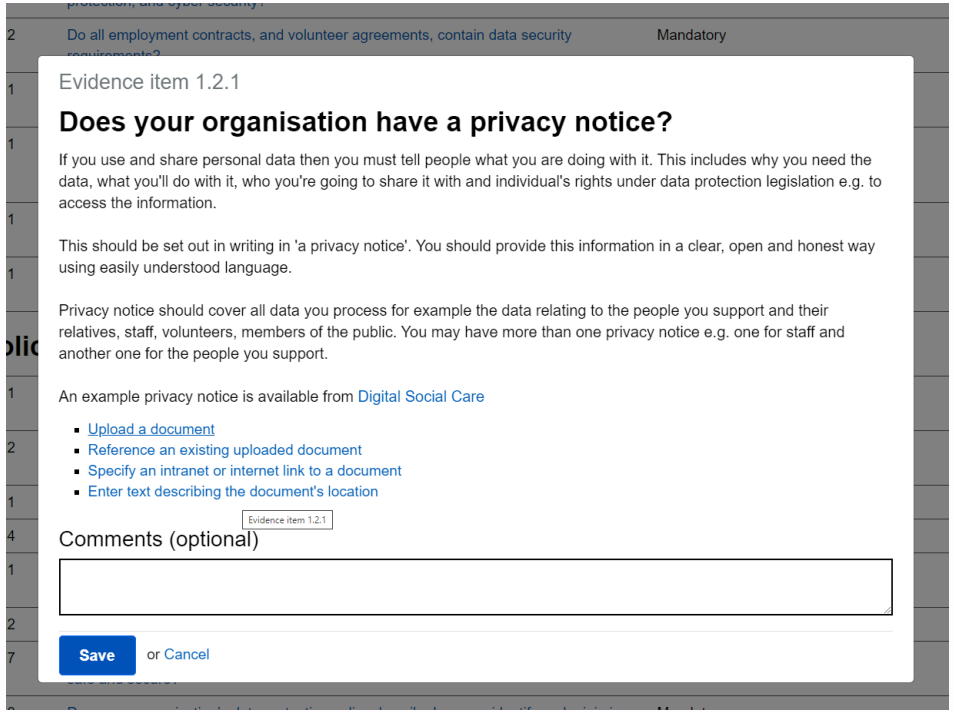
Completing the Toolkit

DSPT
Better security.
Better care.

Questions will follow these formats

- Document (need to upload a document)*

*You can choose to make a statement where the document is kept or copy the document into the text box



Lincolnshire Care Association | Lincolnshire Care Association

Completing the Toolkit

DSPT
Better security.
Better care.

- **The DSPT is a declaration of your data protection compliance**
- **If you are unsure of any questions today do not answer them**
- **You can answer them in the future**

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

1.1.5

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

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

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

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.1.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	
3.2.1	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?	
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?	
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory

Policies and procedures

1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory
1.1.2	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Mandatory

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

ganisation will take to meet the full standard

aff

5

1

2

1

1

1

olic

1

2

Does your organisation have an up to date list of the ways in which it holds and shares

Mandatory

Evidence item 1.1.5

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

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

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

Read more about data security and protection responsibilities and specialised roles.

John Smith MD

Comments (optional)

Save or Cancel

Evidence item 1.1.5

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.5	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	**COMPLETED**
2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory	
2.1.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory	
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?		
3.2.1	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?		
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?		
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory	

Policies and procedures

1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory	
1.1.2	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Mandatory	
	...ve a privacy notice?	Mandatory	

ent/EvidenceItem?evidenceId=13&assertionNumber=1.1.1&organisationCod...

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

2.1.1

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

All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

2.1.2

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

Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

3.1.1

Has a training needs analysis covering data security and protection, and cyber security, been completed since 30 June 2021?

A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation. Your organisation's training needs analysis should identify the level of training or awareness raising required by your staff, directors, trustees and volunteers if you have them. It should be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

3.2.1

Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 30 June 2021?

All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need.

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

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

3.4.1

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

It is likely that the person or people within your organisation who are responsible for data security and protection will need additional and more in depth training than the majority of your staff. Your organisation's training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Staffing and Roles

DSPT
Better security.
Better care.

4.1.1

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

Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.1.1

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

Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should register as a matter of urgency

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.1.2

Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing

Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st April 2020. Upload the document(s) or link to the document or specify where it is

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.2.1

Does your organisation have a privacy notice?

Your organisation must set out in clear and easily understood language what it does with the personal data it processes regarding the people it supports, staff and volunteers, and members of the public, for example relatives or other professionals etc. This is called a privacy notice and there may be more than one privacy notice e.g. one notice for staff and one for the people you support. Your organisation's privacy notice(s) should be made available to these people and inform them about their rights under data protection legislation and how to exercise them. It is good practice to publish your privacy notice on your website if you have one.

.

Policies and Procedures

DSPT
Better security.
Better care.

1.2.4

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

The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic.

As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out.

All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 30 September 2021.
More detailed guidance that gives advice about compliance with the national data opt-out policy is available from NHS Digital and Digital Social Care.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.3.1

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

Confirm that your organisation has a policy or policies in place to cover:

- data protection
- data quality
- record keeping
- data security
- where relevant, network security

The policy or policies should be reviewed and approved by the management team or equivalent within the last 12 months. There is no set number of how many policies your organisation has to have on these topics as the different sizes and complexity of organisations means that some will have one all-encompassing policy, whilst others may have multiple policies.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.3.2

Does your organisation carry out regular data protection spot checks?

Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.3.7

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

Your policy should describe how your organisation keeps personal data as safe as possible. It should set out, for example: how you might use codes instead of names when sharing data with others; how you might secure or encrypt messages so that only authorised people can read them. This is called 'data protection by design'.

Your policy should also set out, for example: how you only collect the minimum amount of data that you need, how you limit access to only those who need to know, keep the data for as short a time as possible, and how you let people know what you do with their data. This is called 'data protection by default'.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.3.8

Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?

Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes.

This type of risk assessment is called a Data Protection Impact Assessment (DPIA).

Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO) Guidance.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.4.1

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

Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance,

staffing and care records. The timetable, or schedule as it sometimes called, should be based on statutory requirements or other guidance)

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.4.2

If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed since 1st April 2020? This contract should meet the requirements set out in data protection regulations.

It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks.

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

If you do not use third parties to destroy records or equipment, then tick and write “Not applicable” in the comments box

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

1.4.3

If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?

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

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Policies and Procedures

DSPT
Better security.
Better care.

10.1.2

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

Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided.

If you have no such suppliers, then 'tick' and write “Not applicable” in the comments box.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

DSPT
Better security.
Better care.

1.3.12

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

Paper records may be taken out of your organisation's building(s), for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when 'on the move'?

If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

DSPT
Better security.
Better care.

1.3.13

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

Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your organisation's sites.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

5.1.1

If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?

Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place.

If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

6.1.1

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

All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation.

There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner's Office ICO. If you are not sure whether or not to inform the Information Commissioner's Office of a breach, the toolkit's incident reporting tool and guide can help you to decide.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

6.1.3

If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?

In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

Approaching Standards

Data Security

6.1.4

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

If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible.

If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

DSPT
Better security.
Better care.

7.1.2

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

Your organisation's business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire).

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

Data Security

DSPT
Better security.
Better care.

7.2.1

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

Describe how your organisation tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be since 1st April 2020.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

1.3.11

If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?

The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, write “Not applicable” in “Enter text describing document location”.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

1.3.14

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

Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.

If your organisation does not use any mobile phones, write "Not applicable" in the text box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

4.1.2

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

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

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

4.2.4

Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?

When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

4.5.4

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

If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

6.2.1

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

This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

6.3.2

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

Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write “Not applicable” in the comments box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

7.3.1

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

It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them.

You may need to ask your IT supplier to assist with answering this question.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

7.3.2

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

Contacts include phone number as well as email.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

7.3.4

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

It is important that your organisation's backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

8.1.4

Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?

Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example.

If your organisation does not use any IT systems or software, then tick and write “Not applicable” in the comments box. For guidance (including information on how to check which software

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

8.2.1

If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.

This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable.

If your answer to the previous question was yes, write “Not applicable” in “Enter text describing document location”.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

8.3.5

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

It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box.

Approaching Standards

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

9.1.1

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

Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this

question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

9.5.2

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

Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question.

If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable“ in the comments box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

IT Systems and Devices

DSPT
Better security.
Better care.

10.2.1

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

Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example.

If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.

Standards Met

Lincolnshire Care Association | Lincolnshire Care Association

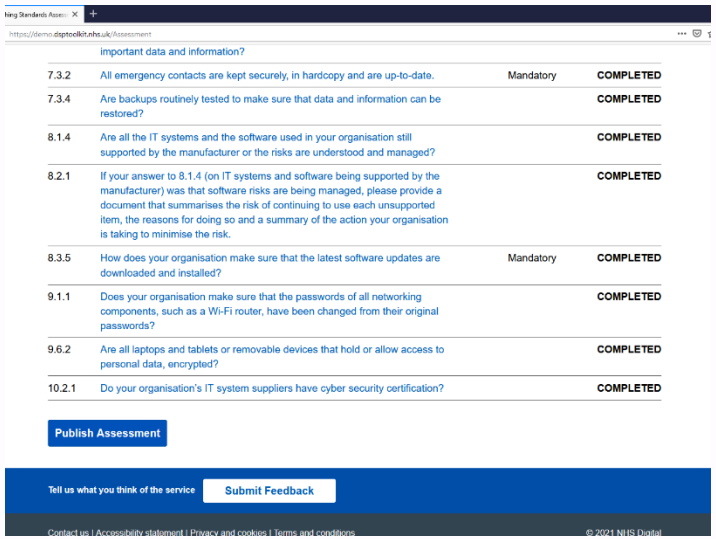
Publish the Toolkit

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Publish the Toolkit

DSPT
Better security.
Better care.

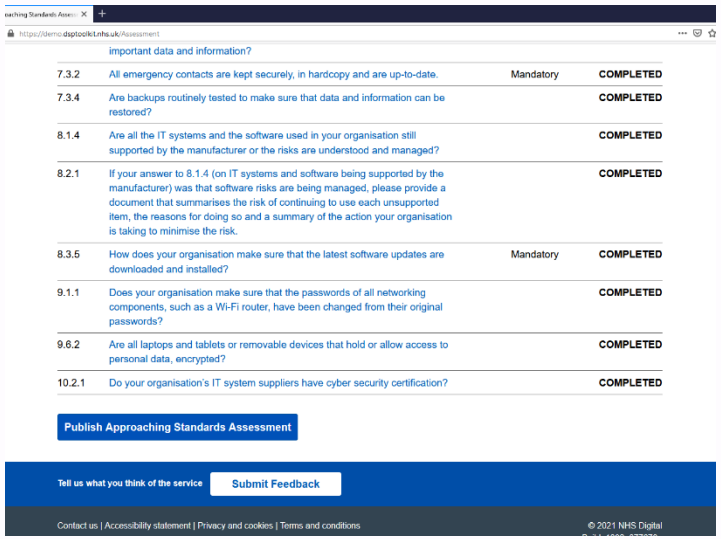


	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	COMPLETED
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		COMPLETED
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		COMPLETED
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		COMPLETED
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	COMPLETED
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		COMPLETED
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		COMPLETED
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		COMPLETED

Publish Assessment

Tell us what you think of the service Submit Feedback

Contact us | Accessibility statement | Privacy and cookies | Terms and conditions © 2021 NHS Digital

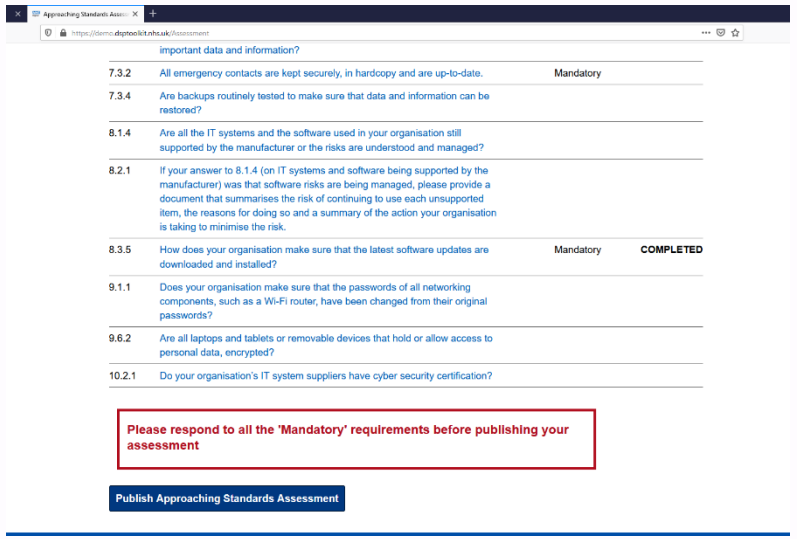


	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	COMPLETED
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		COMPLETED
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		COMPLETED
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		COMPLETED
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	COMPLETED
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		COMPLETED
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		COMPLETED
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		COMPLETED

Publish Approaching Standards Assessment

Tell us what you think of the service Submit Feedback

Contact us | Accessibility statement | Privacy and cookies | Terms and conditions © 2021 NHS Digital



	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	COMPLETED
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		

Please respond to all the 'Mandatory' requirements before publishing your assessment

Publish Approaching Standards Assessment

Lincolnshire Care Association | Lincolnshire Care Association

	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	**COMPLETED**
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		**COMPLETED**
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		**COMPLETED**
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		**COMPLETED**
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	**COMPLETED**
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		**COMPLETED**
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		**COMPLETED**
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		**COMPLETED**

Publish Assessment

Tell us what you think of the service **Submit Feedback**

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

organisation?

Cyber Essentials PLUS

Does your organisation have Cyber Essentials PLUS Certification with a scope covering all health and care data processing awarded during the last 12 months?	No	Change
Cyber Essentials PLUS award date	Not Provided	
Cyber Essentials PLUS Certificate	Not provided	

Publish Assessment

By clicking 'Publish Assessment' you are confirming that your board/senior management have agreed and signed off this assessment. Your assessment will then be published at a summary level on the Data Security and Protection Toolkit. This will be available to the public.

Confirmation of the publication will be sent to you at kb@wmca.care.

Publish Assessment

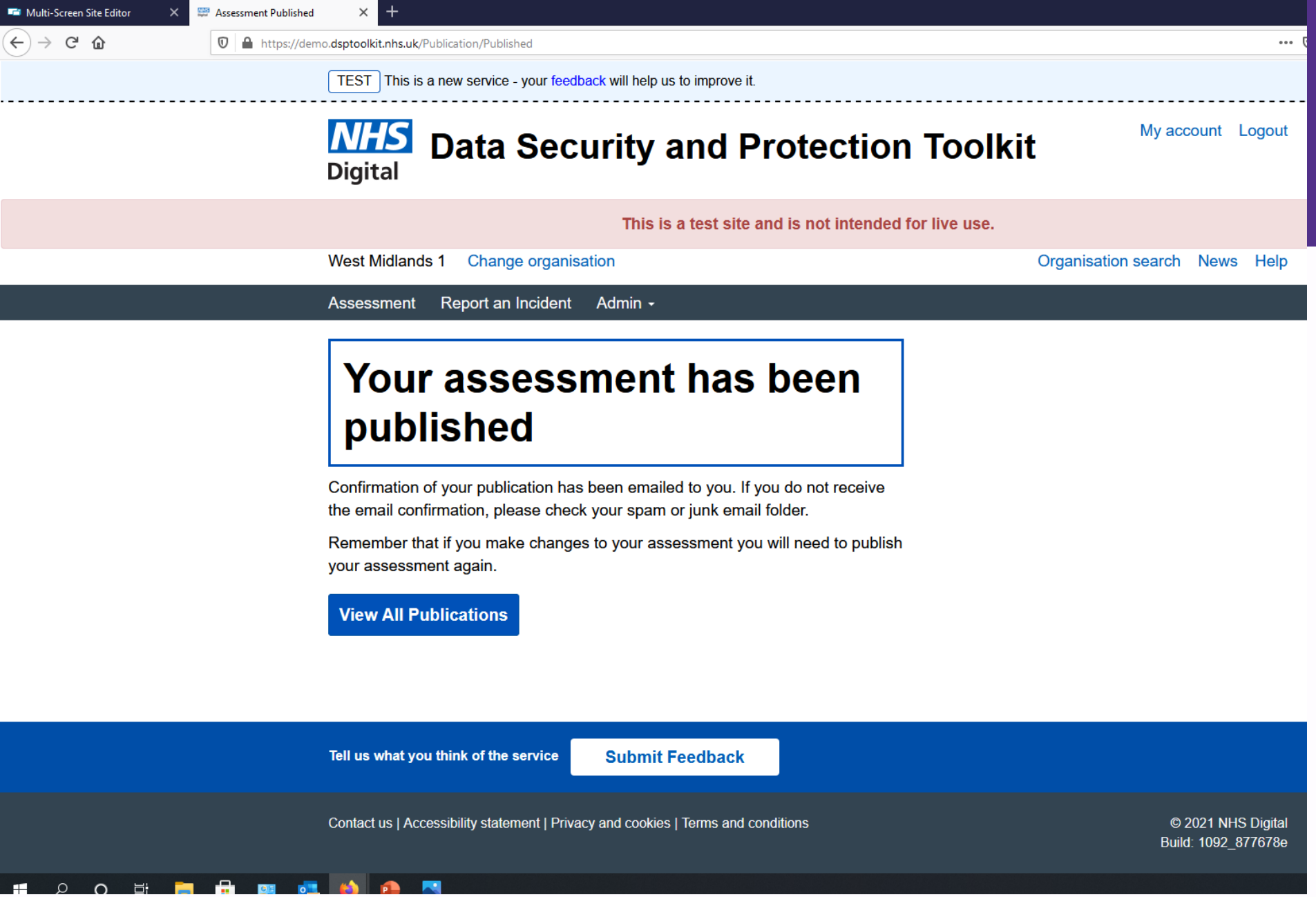
Tell us what you think of the service **Submit Feedback**

Contact us | Accessibility statement | Privacy and cookies | Terms and conditions

Build: 1092_87

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association



DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	**COMPLETED**
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		**COMPLETED**
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		**COMPLETED**
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		**COMPLETED**
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	**COMPLETED**
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		**COMPLETED**
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		**COMPLETED**
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		**COMPLETED**

Publish Approaching Standards Assessment

Tell us what you think of the service **Submit Feedback**

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Multi-Screen Site Editor | Provide Action Plan

https://demo.dsptoolkit.nhs.uk/Assessment/ActionPlan

This is a test site and is not intended for live use.

West Midlands 1 Change organisation Organisation search

Assessment Report an Incident Admin

Assessment

Provide an action plan

Thank you for responding to all the mandatory requirements

- You should now download a blank action plan template, which lists the requirements you have not yet responded to.
- You should then complete this plan and upload a copy here, as proof you are approaching the Data Security and Protection Toolkit standard.
- You will then be able to publish your 'Approaching Standards' assessment.

Upload file

Drag and drop Action Plan or click to browse

Publish Approaching Standards Assessment

Tell us what you think of the service Submit Feedback

javascript:void(0);

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Instructions: This plan lists the requirements your organisation has not yet responded to on the Data Security and Protection Toolkit.
You should complete this action plan outlining the actions you are going to do to meet these requirements, **save a copy** and then upload the file to the Data Security and Protection Toolkit to complete your assessment at Approaching Standards level.
https://www.dsptoolkit.nhs.uk/

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

	important data and information?		
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	
7.3.4	Are backups routinely tested to make sure that data and information can be restored?		
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?		
8.2.1	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.		
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	Mandatory	**COMPLETED**
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?		
9.6.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?		
10.2.1	Do your organisation's IT system suppliers have cyber security certification?		

Please respond to all the 'Mandatory' requirements before publishing your assessment

Publish Approaching Standards Assessment

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

e Editor | Provide Action Plan

https://demo.dsptoolkit.nhs.uk/Assessment/ActionPlan

West Midlands 2 Change organisation Organisation search News

Assessment Report an Incident Admin

Assessment

Provide an action plan

Thank you for responding to all the mandatory requirements

- You should now download a blank action plan template, which lists the requirements you have not yet responded to.
- You should then complete this plan and upload a copy here, as proof you are approaching the Data Security and Protection Toolkit standard.
- You will then be able to publish your 'Approaching Standards' assessment.

Upload file

Document Currently Saved:

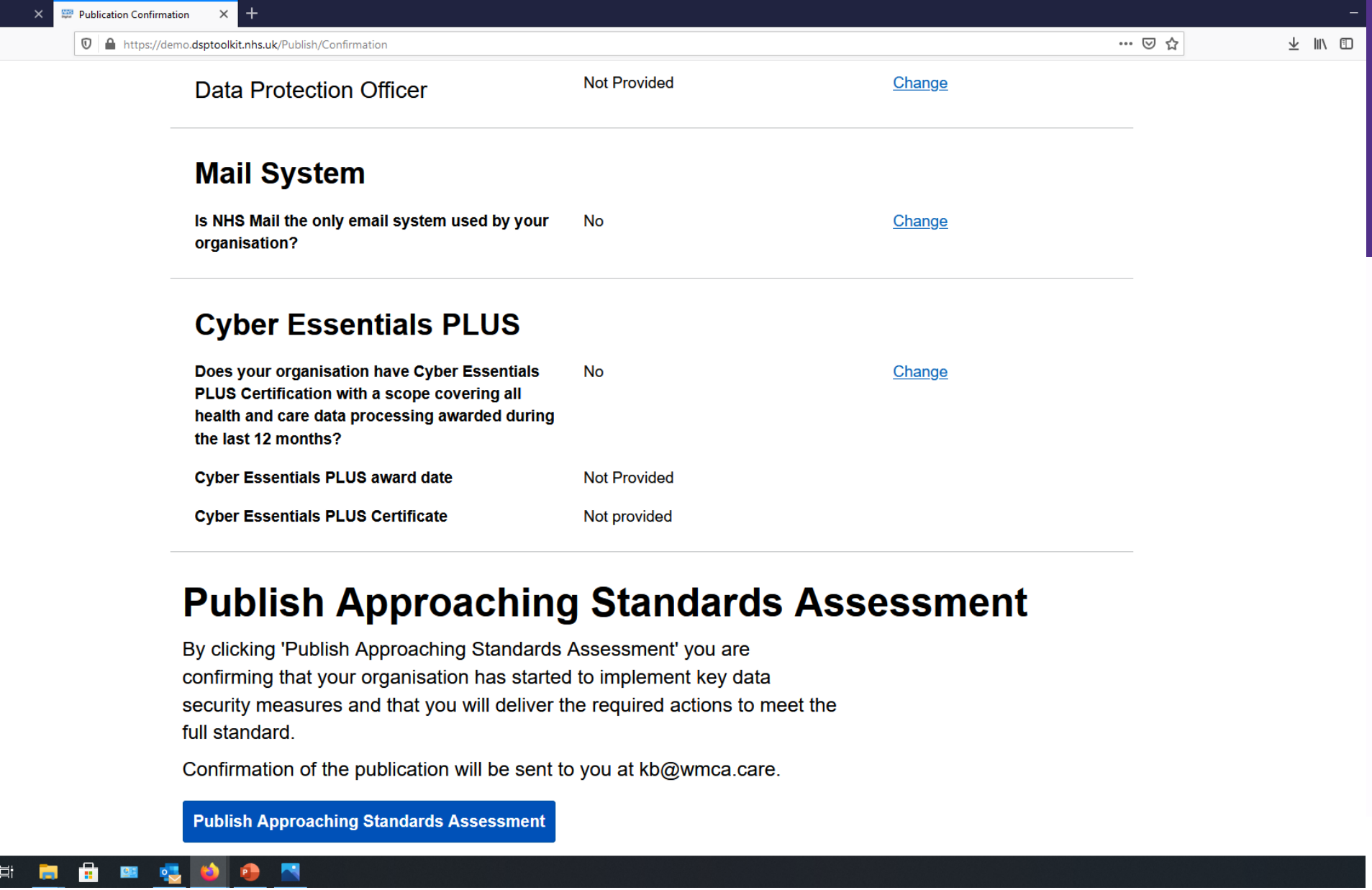
DSPT_Action_plan_WM1_24032021_1627.xlsx	Remove	Replace

Publish Approaching Standards Assessment

Tell us what you think of the service **Submit Feedback**

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association



DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Next Steps

DSPT
Better security.
Better care.

- If you have published at Standards Met today, you're done until the new DSPT year
- If you have published at Approaching Standards that is the minimum for NHS Mail but will not give you access to other systems. You will need to adhere to your action plan – We will be in touch to help
- If you have not published today we can offer you additional support – We will be in touch to discuss

Lincolnshire Care Association | Lincolnshire Care Association

Last Questions

DSPT
Better security.
Better care.

Lincolnshire Care Association | Lincolnshire Care Association

Completing the DSPT
Thank You

DSPT
Better security.
Better care.

Digital Social Care

Varsha Modhwadia – Digital Project Manager
Lincolnshire Care Association
varshamodhwadia@linca.org.uk

Lincolnshire Care Association | Lincolnshire Care Association