Better Security Better Care

DSPT

Bedfordshire Care Group

Central Bedfordshire

Completing the

Data Security Protection Toolkit

(DSPT)

21/22 Toolkit Year

Better Security Better Care
DSPT

The Data Security Protection Toolkit (DSPT) is an online data protection assessment.

It is a compulsory requirement to successfully complete the DSPT if you have an NHS Mail Account, you have access to any NHS digital records or you contract with the NHS.

All CQC registered care providers will need to complete this data protection assessment (regardless of whether or not you have an existing NHS Mail Account).

The DSPT is an extremely useful tool because it covers all areas of GDPR compliance that you as a Care Provider are required to implement, such as having up to date policies and ICO registration, ensuring you are operating within the law.
Once you have completed the DSPT you can potentially have access to these other NHS services:

- **NHS Mail -** A secure email system to safely swap medical and residents' data with both the health service and local authorities
- **Proxy Access -** with proxy access you can order medication on behalf of your service users
- **Shared Care Record -** This allows Care Providers and the NHS to see each other's patient records transforming how you deliver care
- **Digital Red Bag -** Improves information sharing between care homes, ambulance services, hospital staff, residents, and their family members

It includes Microsoft Teams video conferencing which is being used by doctors to do virtual consultations when they are unable to visit the home.
DSPT compliance can also potentially give you access to NHS records, and this is being rolled out across the country.
It includes Microsoft Teams video conferencing which is being used by doctors to do virtual consultations when they are unable to visit the home.

Better Security Better Care

DSPT

DSPT
Better security.
Better care.

Bedfordshire Care Group

Central Bedfordshire

DSPT compliance can also potentially give you access to NHS records, and this is being rolled out across the country

Better Security Better Care
DSPT

DSPT
Better security.
Better care.

Bedfordshire Care Group

Central Bedfordshire

Before You Start

Register to use the DSPT

If you haven’t done so already, this is easy to do.

You will need an email address (we suggest you use a generic one rather than a personal or individual address that is easily accessible by staff within the care business).

Your ODS Code. You can look this up by visiting the ODS portal
Then register at https://www.dsptoolkit.nhs.uk/

To help you complete the DSPT we have produced a checklist of the policies and procedures you need in place before you start. Examples of these can all be downloaded from our website https://www.digitalsocialcare.co.uk/resources/

Your ICO Registration Number Data Protection Policy

Data Privacy Policy

Data Register

Training Needs Analysis

National Data Opt Out Policies

Spot Check Audit Checklist

Unsupported Software Register* If needed

If you are happy you have these then you should be ready to begin the toolkit

Bedfordshire Care Group

Central Bedfordshire

Before You Start

Policies and Procedures

You need to have various policies and procedures in place to successfully complete the DSPT and to demonstrate you are compliant with elements of data protection law. These are highlighted on the checklist on the previous page, but we will explain in more detail what is required in each document here

Data Privacy Policy

Your data privacy policy is an overarching document which sets out how you collect personal data, what it is used for and how long it is retained. It must also stipulate how individuals can view or challenge the use of this

data. This policy must be easily accessible and produced on demand. It may consist of several documents or a single document. Most organisations publish this on their website (often as a permanent link in the page footer), it may also be included in your service user contracts. There are many standard templates available that are GDPR compliant. **You can see the associations privacy policy at here**. **You will need to state that you have a policy and specify where it is held.**

Staff Data Policy

Staff must be aware of the safe and secure use of data and their individual responsibilities pertaining to its use and access. This should be included in your standard staff procedures and manuals. All staff must be made aware of your policies and their responsibilities on induction and reviewed regularly. You can see an example policy here . **You will need to state that you have a policy and specify where it is held.**

Data Register

This is a list of all the data you hold, where it is held and whether or not this is shared with other organisations. The Data Register is made up of several different documents. It is entirely up to you if you maintain a single register or have them as separate documents. These are:

- **Information Asset Register: This is a document including details of the type, location, software, owner, support and maintenance arrangements, quantity of data and how critical they are to the organisation. You will need to state that you have a policy and specify where it is held.**
- **Retention Register.** A document stating how long data is held and when it is due for destruction/disposal
- **List of Suppliers and any data sharing arrangements (if applicable)**: You must be able to provide a list of your current suppliers with whom you share data or who process personal data of your service users or staff. It must also include the nature of the data processing and when the contract expires (e.g. outsourced payroll). **If you do not have any such arrangements, you can state not applicable in the Toolkit. If you do, you will need to state that you have a register and specify where it is held.**

Staff Bring Your Own Device Policy (BYOD)

If you allow staff to use their own phones/mobile devices you must have a policy outlining how this works and how it is managed. You do not need this policy if staff do not use their own devices

Additional Information Needed for Standards Met

To complete the Toolkit to Standards Met you will also need the following:

- A Training Needs Analysis of Data Protection/Security needs
- Systems Administers need to sign an agreement holding them to higher standards

- A document highlighting any unsupported software you use and the business need and risk (if you have unsupported software)

  Examples of all these documents can be found on our website at www.digitalsocialcare.co.uk If you are happy, you have these then you should be ready to begin the toolkit

Bedfordshire Care Group

Central Bedfordshire

Organisational Profile

When you first sign into the toolkit and before you can answer the questions, you must complete your organizational profile.

You must first state what type of business you are (Social Care)

It will then ask you for details of the following roles

- Caldicott Guardian

- SIRO

- IG Lead

- Data Protection Office

These can all be left blank as the first question of the toolkit will ask you to name who is responsible for

data protection in your company

You will then be asked if NHS Mail is used by your company

And whether or not you have Cyber Essentials Plus Certification (this is not mandatory, so it is OK to answer no or not sure). If you have Cyber Essentials Plus, upload a copy of your certificate. Many questions on the DSPT are covered by Cyber Essentials Plus so it will prepopulate some of the questions in advance.

You will be given a summary of the information you have entered to double check. If you are happy, you can press continue and begin the assessment questions.

The toolkit itself is split into 4 sections of questions:

- **Staffing and Roles**

- **Policies and Procedures**

- **Data Security**

- **IT Systems and Procedures**

The toolkit also has different levels of completion

Approaching Standards - These are the questions marked Mandatory. Approaching Standards is the mini- mum level required to access NHS Mail. You cannot publish at Approaching Standards until you have published an action plan on how you are going to address the issues stopping you reaching Standards Met.

Standards Met - This is met by completing all 43 questions on the toolkit. Standards Met potentially gives you access to facilities like Share Care Records and shows that you take your data protection seriously.

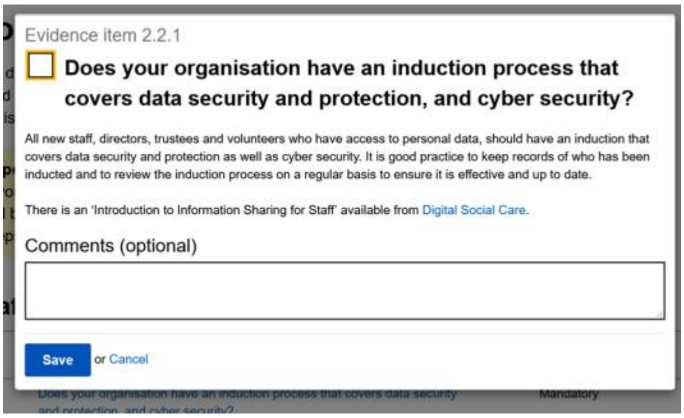
The Toolkit does not need to be completed in one sitting. You can dip in and out.

Better Security Better Care DSPT

Bedfordshire Care Group

Central Bedfordshire

The toolkit has 3 different types of question



Evidence item 2.2.1

□ **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.

There is an 'Introduction to Information Sharing for Staff' available from Digital Social Care.

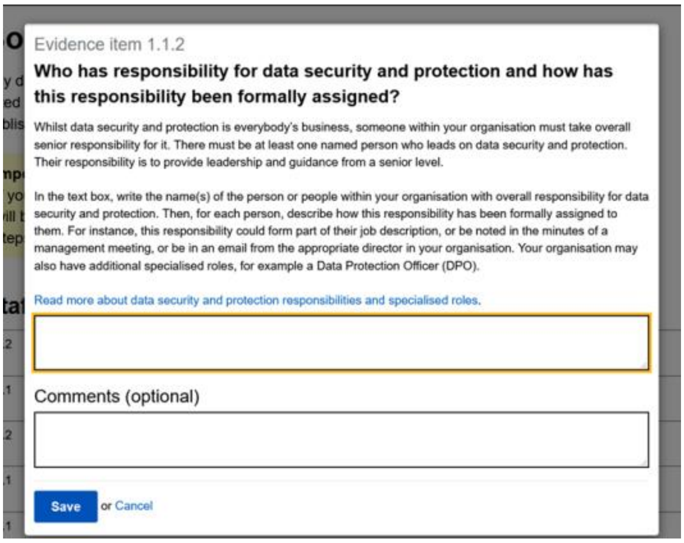
Comments (optional)

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

Tick Boxes

Essentially a Yes/No question

Comments are always optional unless the question requires a 'Not Applicable' answer



Evidence item 1.1.2

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.

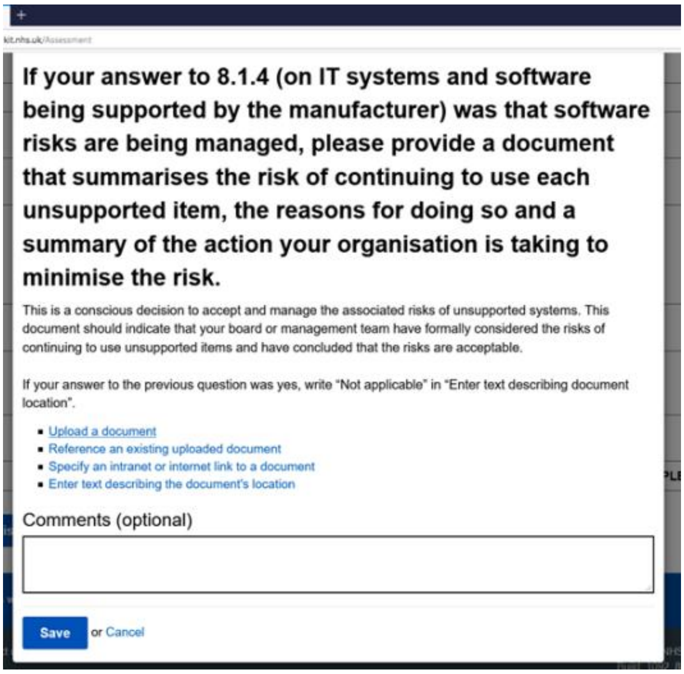
In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job 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.

Comments (optional)

These require a written answer of some sort. Make sure you write your answer in the top box. If you answer accidentally in the comments box, the toolkit will class the question as unanswered

Comments are always optional unless the question requires a ‘Not Applicable’ answer



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".

- Upload a document
- Reference an existing uploaded document
- Specify an intranet or internet link to a document
- Enter text describing the document's location

Comments (optional)

These require a document to be uploaded

However, you can click on the fourth option (Enter Text Describing the Documents location) and state where the document is located rather than upload it (e.g. on a computer in the manager's office or on a website) Comments are always optional unless the question requires a 'Not Applicable' answer

Better Security Better Care

DSPT

Bedfordshire Care Group

Central Bedfordshire

Staffing and Roles

Questions in this section:

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

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

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

3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st April 2020?

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 April 2020?

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?

Better Security Better Care
DSPT

DSPT
Better security.
Better care.

Bedfordshire Care Group

Central Bedfordshire

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)

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.

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.

3.1.1 Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st April 2020?

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.

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 April 2020?

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.

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).

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.

Policies and Procedures

Questions in this section:

1.1.1. What is your organisation’s Information Commissioner’s Office (ICO) registration number?
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?

1.2.1. Does your organisation have a privacy notice?

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

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

1.3.2. Does your organisation carry out regular data protection spot checks?

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

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?

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

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 30 June 2021? This contract should meet the requirements set out in data protection regulations.

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?

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?

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

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

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.

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

From 31st March 2022, all regulated social care providers in England will need to comply with the national data opt-out. Digital Social Care will publish detailed guidance and useful resources. For organisations who publish prior can respond "not applicable" to this question. For all other organisations, we are waiting for sign off on guidance from NHSX and will be publishing this in due course. See Digital Social Care for updates

Bedfordshire Care Group

Central Bedfordshire

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.

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.

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’.

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.

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)

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

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.

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.

Better Security Better Care
DSPT

Bedfordshire Care Group

Central Bedfordshire

Data Security

Questions in this section:

1.3.12 How does your organisation make sure that paper records are

safe when taken out of the building?

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

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?

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

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?

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

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

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

Data Security

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.

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.

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.

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.

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.

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.

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).

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 30 June 2021

IT Systems and Procedures

Questions in this section:

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?

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

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

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?

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

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

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

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

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

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

Bedfordshire Care Group

Central Bedfordshire

IT Systems and Procedures

Questions in this section:

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?

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?

9.5.2 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?

Better Security Better Care
DSPT

DSPT
Better security.
Better care.

IT Systems and Procedures

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”.

1.3.13 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.

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.

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.

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.

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.

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.

Better Security Better Care

DSPT

DSPT
Better security.
Better care.

Bedfordshire
Care Group

Central
Bedfordshire

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.

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

Contacts include phone number as well as email

It is good practice to keep an additional copy of the staff emergency contacts that is not on any of your systems. Hard copy is best. Maybe also keep a second copy off site (business owners' home would be an example)

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

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.

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”.

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.

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.

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.

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.

Better Security Better Care
DSPT

Bedfordshire Care Group

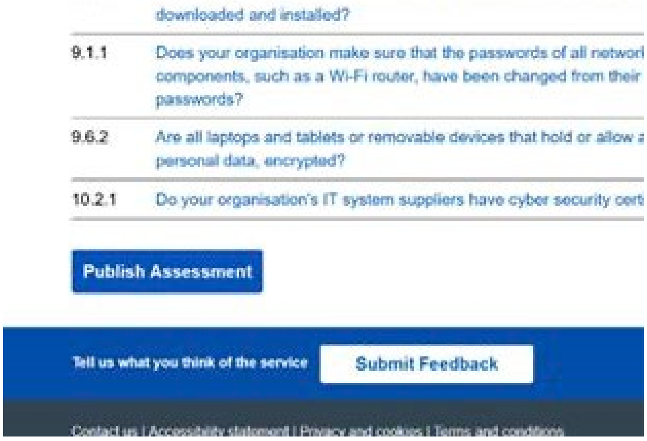
Central Bedfordshire

Publish Your Toolkit

Once you have completed the toolkit questions you will see one of 3 screens:

Publish Assessment:

You have entered all the necessary questions to reach Standards Met - You can click the blue button and publish your answers



	downloaded and installed?
9.1.1	Does your organisation make sure that the passwords of all networ components, such as a Wi-Fi router, have been changed from their passwords?
9.6.2	Are all laptops and tablets or removable devices that hold or allow a personal data, encrypted?
10.2.1	Do your organisation's IT system suppliers have cyber security cert

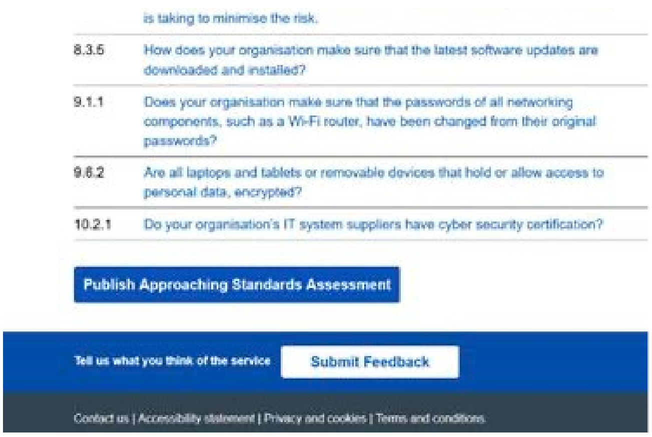
Publish Assessment
Tell us what you think of the service
Submit Feedback
Contact us | Accessibility statement | Privacy and cookies | Terms and conditions

Publish Approaching Standards Assessment:

You have entered all the Mandatory questions to reach Approaching Standards. You must also complete an action plan on how you will address the missing questions to reach Standards Met. For this reason, we recommend you answer as many of the questions as you can as this will reduce your action plan. When you click the blue button, it will prompt you to download and complete and action plan template

Publish Approaching Standards Assessment:

You have entered all the Mandatory questions to reach Approaching Standards. You must also complete an action plan on how you will address the missing questions to reach Standards Met. For this reason, we recommend you answer as many of the questions as you can as this will reduce your action plan. When you click the blue button, it will prompt you to download and complete and action plan template



	is taking to minimise the risk.
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?
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?

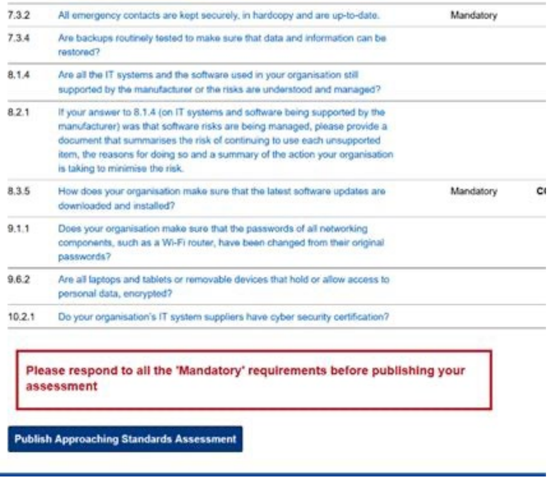
Publish Approaching Standards Assessment
Tell us what you think of the service
Submit Feedback
Contact us | Accessibility statement | Privacy and cookies | Terms and conditions

Bedfordshire Care Group

Central Bedfordshire

If you see this red warning box it means you have not completed at least all of the mandatory questions and cannot therefore publish

If you think you have completed all the questions then go back and recheck your answers, making sure you have not mistakenly answered a question by typing in the Comments Box



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	C
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

Contact Us

We are happy to help with any queries directly relating to the toolkit. You can get in touch using the details below.

Guidance

Before you contact us, have you tried the Online Help?

Contact details

Email: SCHHServicedevelopment@centralbedfordshire.gov.uk
Please provide your ODS code or address when raising queries via email.