

Better Security, Better Care - Managers' discussion tool

Version 4: August 2026

This discussion tool is designed to help you have discussions with your frontline staff to check their knowledge and provide evidence of their competence in data security and protection to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#).

The tool is broken down into four colour-coded sections covering the four learning outcomes for frontline social care staff:

1. Understand the importance of data security and protection in care organisations and what you need to do to keep data safe
2. Be able to follow the laws and rules that keep personal information safe
3. Be aware of the risks to keeping data safe and know how to avoid them, including:
 - I. being aware of scams
 - II. safe use of digital devices
 - III. safe keeping of paper records
4. Recognise when data has been lost, shared, seen, or used without approval and know what to do if it happens

Each section includes guidance notes to help you understand the topic, links to further resources, questions for you to ask to prompt discussion with your staff, and a multiple choice quiz (and the answers!) that you can give your staff to test their knowledge or assess their learning needs.

Use the tool flexibly to suit your needs. For example, play a short video and lead a discussion using the prompts within the tool or work through the multiple choice quiz either individually, in pairs or in small groups.

You can cover the whole tool in one go or work on one section at a time.

The **quiz** is also available to download as a separate document so that your staff can answer all the questions in one go.

Sign and date each section to show that you have discussed that topic with your staff and that you are confident that your staff meet that learning outcome.

Section 1: Understand the importance of data security and protection in care organisations and what you need to do to keep data safe

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Good information supports good care. Everyone who we support should be able to trust that their personal information (especially things like health and care information) is being kept safe. We must follow the UK General Data Protection Regulation (GDPR), the Data Protection Act and the common law duty of confidentiality. There are also the Caldicott Principles and National Data Guardian Standards for Health and Social Care. Personal data is anything that might identify someone. It is people's information and it should be treated with respect, for example only shared with people who need to know it. It's important their information is used only in ways people would reasonably expect and that it stays safe. Individuals have legal rights over their personal information and we must follow the law. We all have a duty to look after people's personal or confidential data safely and securely AND to share it in the right ways with others who need to see it.	What is personal data? Why is it important to keep personal information safe and keep it confidential? What might happen if information is not kept safe? What sorts of information should we not share with others? What do we have to do to look after information?

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Staff training resources See Staff Guidance on Data Sharing which contains case studies to work through.	Do you know what needs to be included in a care record, why you are recording this information and how it will be used? Do you tell people this information when you collect their data? Can you remember a time when this hasn't worked as well as it should have? What would you do differently now?

Understand the importance of data security and protection in care organisations and what you need to do to keep data safe

I confirm that I have discussed the importance of data security and protection in care organisations with my staff and am confident that the following people/teams/services understand what they need to do to keep data safe:

Signed: _____ Name: _____ Date: _____

Quiz for frontline staff: Understand the importance of data security and protection in care organisations and what you need to do to keep information safe

Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

Question		Answer options	Comment
1a	We have a legal duty to respect the privacy of the people who use our care services	True False	
1b	Sharing information with the right people can be just as important as not sharing it with the wrong person	True False	

Question		Answer options	Comment
1c	Can someone you support ask to see and have a copy of the personal information that is held about them?	Yes No	
1d	When you collect someone's personal details, should you tell them what will happen to that information and who it will be shared with?	Yes No	
1e	Which of the following are examples of personal data? Choose all correct answers	The health conditions of the people you support The payroll details of your colleagues The name of the nearest opticians to where you work The name and contact details of the next of kin of the people you support	

Question		Answer options	Comment
		The bank details of the people you support A list of the ages of all the people that you have cared for or supported over the last year, without names, addresses or dates of birth	
1f	Under the Data Protection Act an individual member of staff cannot be held responsible for information that goes missing or is seen by the wrong people (This is called a data breach)	True False	

Quiz answers: Understand the importance of data security and protection in care organisations and what you need to do to keep data safe

This quiz will provide evidence to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#). The correct answers are shown below. The pass mark is 80% or 5 out of the 6 questions.

Question		Answer	Explanation
1a	We have a legal duty to respect the privacy of the people who use our care services	True	We all have a legal duty and a personal responsibility to respect the privacy of the people we support. This is the same as your employer who has a legal duty and responsibility to respect your privacy as a member of staff. This includes not looking at or sharing confidential information about a person unless it is needed for their care and is covered by your organisation's policies and procedures.
1b	Sharing information with the right people can be just as important as not sharing it with the wrong person	True	If you don't share correct and up to date information with the right people, this could badly affect the care provided to someone. Confidential information can be shared with the right people. For example, you should share information about the people you support with other health and care professionals if it is needed for their care.

Question		Answer	Explanation
1c	Can someone you support ask to see and have a copy of the personal information that is held about them?	Yes	Data protection law gives individuals rights over their information. People have the right to see the personal data recorded about them. This is known as a subject access request. You should be careful about what comments or opinions you record about someone, because they may see that information in the future.
1d	When you collect someone's personal details, should you tell them what will happen to that information and who it will be shared with?	Yes	People should be told how their personal data will be used and looked after. Under data protection law individuals have the right to know what personal information is being collected about them, for what reason, how long it will be kept for, and who it will be shared with.
1e	Which of the following are examples of personal data?	The health conditions of the people you support The payroll details of your colleagues ~~The name of the nearest opticians to where you work~~	Personal data is any information that identifies an individual, for example their name and contact details. Some personal data is more sensitive, like someone's health, and you should take extra care with this information. Information about an organisation, such as the name of a business, is not personal data. Nor is information where the details that would identify individuals have been removed.

Question		Answer	Explanation
		The name and contact details of the next of kin of the people you support The bank details of the people you support ~~A list of the ages of all the people that you have cared for or supported over the last year, without names, addresses or dates of birth~~	
1f	Under the Data Protection Act an individual member of staff cannot be held responsible for information that goes missing or is seen by the wrong people (This is called a data breach)	False	Employees can be taken to court for breaking data protection laws. People have been fined for causing data breaches, but this happened because they did not follow their organisation's data security policies.

Section 2: Be able to follow the laws and rules that keep personal information safe

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
The information about an individual's care and support must be treated as confidential and only shared with people who need to know it. It is OK to share with care workers who are providing care to the individual and with, for example, social workers or health workers who are involved in their care. Sharing information with the right people can be just as important as not sharing it with the wrong person. Part of keeping data safe is to record it properly, so it's important that care records are accurate and up to date. They must always be kept up to date, complete, correct and easy to understand to support good care. There are some simple steps you can take to follow the Data Protection Act/GDPR and the common law duty of confidentiality. We must take care to keep and share information carefully to avoid the wrong people seeing confidential information: • Think about who can overhear information when you're talking • Check if the person you are speaking to over the telephone is not pretending to be someone else • Use secure email or password protect files if you are sending confidential information by email • Log off computers or out of systems when you are finished. Lock the screen if you are away from the device even if only for a short period of time • Only use systems and apps that are approved for you to use	What information do we hold on individuals who receive care and support, and staff? How can we make sure we keep this information safe? For example, are you aware of who is around you when looking at or talking about someone's personal data? Who should be able to see people's care records? Why is it important to record information as soon as possible? Do you save records in the right place so that they are easy to find? What systems or apps do you use when working with confidential information? What are safe ways to share information?

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
• Only look at records for work reasons • Share information but only the details that are needed • Take care of paper records • Get rid of old paper and digital records in the right ways and at the right times	What should you do with old paper records? What about digital records that are no longer needed? Do you know the different places where they might be?
Staff training resources There is downloadable Staff Guidance on Data Quality & Record Keeping on the Digital Care Hub website	Do you understand the risks to keeping information safe if you are working from home? Can you remember a time when this hasn't worked as well as it should have? What would you do differently now?

I confirm that I have discussed the laws and rules that keep personal information safe with my staff and am confident that the following people/teams/services understand what they need to do to keep personal information safe:

Signed: _____ Name: _____ Date: _____

Quiz for frontline staff: Be able to follow the laws and rules that keep personal information safe

Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

Question		Answer options	Comment
2a	When should information be recorded? Choose one	As soon as possible, whilst the event is still fresh in your mind Within a couple of weeks When there is time to do it	
2b	Who should be able to see people's care records, including confidential information about their care? Choose one	All the staff, we need to know what's going on Only the senior staff and managers, so that it's kept safe Only those staff and managers involved in their care should look at their records	

Question	Answer options	Comment
2c If you have previously obtained someone's consent to see and use their information, you do not have to get their consent again if you wish to use it again for the same purpose	True False	
2d How could you safely share confidential information with another person? Choose all correct answers	You take the person to a safe space where you can talk privately You put the information on social media You send the information by secure email for example NHSmail You password protect the information and then email it to the person	
2e Which of these people would need to know about an individual's care and support needs? Choose all correct. answers	A care worker who provides care to the individual The individual's neighbour A social worker supporting the individual	

Question		Answer options	Comment
		The individual's family and friends	
2f	You are in the supermarket when you overhear two other members of staff talking about someone you provide support for. What should you do? Choose one	Join in. They may have information you need to know Go to your line manager and ask for them to be fired Speak to them and say that this behaviour breaches confidentiality	
2g	Free online tools may store or reuse the information you put in	True False	
2h	Which of these is a safe way to get rid of old paper records? Choose one	Shred them Put them in the recycling bin Burn them	

Quiz answers: Be able to follow the laws and rules that keep personal information safe

This quiz will provide evidence to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#). The correct answers are shown below. The pass mark is 80% or 5 out of the 6 questions.

Question	Answer options	Comment
2a When should information be recorded?	As soon as possible, whilst the event is still fresh in your mind	Record information as soon as possible while the details are still clear in your mind. Record high-risk information straight away.
2b Who should be able to see people's care records, including confidential information about their care?	Only those staff and managers involved in their care should look at their records	People will not expect anyone to look at their care record unless that member of staff is involved in their care.
2c If you have previously obtained someone's consent to see and use their information, you do not have to get their consent again if you wish to use it again for the same purpose	True	You don't need to get consent each time you use or share personal information for the same reason. But this is only if you have already told the person - they should know what is happening and be ok with that.

Question		Answer options	Comment
2d	How could you safely share confidential information with another person?	You take the person to a safe space where you can talk privately ~~You put the information on social media~~ You send the information by secure email for example NHSmail You password protect the information and then email it to the person	All of these are safe ways to share information except for putting information on social media.
2e	Which of these people would need to know about an individual's care and support needs?	A care worker who provides care to the individual ~~The individual's neighbour~~ A social worker supporting the individual ~~The individual's family and friends~~	The information about an individual's care and support must be treated as confidential and only shared with people who need to know it. It is OK to share with care workers who are providing care to the individual. It's also ok to share with others, for example social workers or health workers, who are involved in their care.

Question	Answer options	Comment
2f You are in the supermarket when you overhear two other members of staff talking about someone you provide support for. What should you do?	Speak to them and say that this behaviour breaches confidentiality	People expect their personal information to be shared with the staff who need it to provide care. However, they would not expect it to be talked about in public places where others can hear it, as this would not protect their privacy.
2g Free online tools may store or reuse the information you put in	True	Using free online tools such as Chat GPT can help to speed up tasks. But you do not know how the tool is using the information you put in or where it is kept. This means: • Personal information could be seen or used by the wrong people. • Information might be shared or kept in unsafe ways and be seen by anyone. • Tools can make mistakes, which could affect decisions about people.
2h Which of these is a safe way to get rid of old paper records?	Shred them	Paper records should be put in the confidential waste or securely shredded. Burning paper isn't safe. Anyone could find them if they were put in the recycling bin.

Section 3: Be aware of the risks to keeping data safe and know how to avoid them

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Scams Scams are when someone uses tricks to manipulate people to gain access to your building, information or money. It could happen in person, on email, on social media or over the phone. It can appear real, but it's actually a scam. Sometimes it's called 'phishing'. Phishing attempts might try to trick you into sharing sensitive information. They might try to get you to click on a link that goes to a scam website or download an attachment that puts a virus on your device. Learn the warning signs, trust your judgment, and speak up if something doesn't seem right. Look out for: • Unexpected phone calls from the bank or a supplier • Unusual requests • Trying to rush you • Trying to make you trust them because the person seems important • Messages not addressed to you personally • Emails or links that are not what they seem Delete suspicious emails and do not click on links or open attachments in these emails before you delete. Do not reply to them even if they seem to come from a company or person you may know. Replying can tell the sender that your address is a real one.	In what ways could we be scammed? What should you look out for? What is a phishing email? What steps can you take to check that an email is real? What should you do if you think that an email might be a scam? Can you remember a time when this hasn't worked as well as it should have? What would you do differently now?

Staff training resources There is an interactive government eLearning training package on cyber security on the National Cyber Security Centre website: Top Tips for Staff (which takes about 15 minutes)	
Safe use of digital devices Keeping your computer, tablet or mobile phone safe will help you to stay safe online and be better protected if it gets lost or is stolen. Good practice includes: Using strong passwords and not sharing passwords Adding layers of security to make it even harder to access an account such as using two-factor authentication (2FA) Locking devices for example with a password, fingerprint or PIN number Putting antivirus software on computers Downloading and installing the latest software and app updates for your devices	What devices do you use for work or to talk about work? Are they protected by a password, or PIN or another way? Do you lock them when you are not using them? Can you think of some passwords that you shouldn't use? For example 'password1' Think up some examples of strong passwords. Do you re-use your passwords or use easy to guess information in your passwords? If so what will you do to make them stronger?
Staff training resources There is government advice on how to stay safe online: Top tips for staying secure online	Have we got our computers/phones set to automatically update newer versions of software?

Safe keeping of paper records

Taking simple safety steps will lower the risk that personal or confidential paper records are lost, stolen or seen by the wrong people. Confidential data should not be left out where people who are not allowed to can see it. Things like lockable doors, windows, filing cabinets or secure areas can help. It is especially important to take extra care if paper records are taken out of the building, for example for hospital appointments or visits to people's homes. Leaving papers in cars, for example, can be risky.

We also have to be careful when getting rid of any personal or sensitive information. Paper documents should be shredded.

How can paper records be kept secure?

Do you always put away care or other records when you've finished using them?

What sort of documents are ok to throw in the bin? What need to be shredded?

Can you remember a time when this hasn't worked as well as it should have? What would you do differently now?

I confirm that I have discussed the risks to keeping data safe with my staff and am confident that the following people/teams/services are aware of relevant data security risks and know how to avoid them:

Signed: _____

Name: _____

Date: _____

Quiz for frontline staff: Be aware of the risks to keeping data safe and know how to avoid them

Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

Question		Answer options	Comment
3a	Which of these is a strong password and harder for a hacker to guess? Choose one	123456 qwerty Password1 monkeysponCh2air	
3b	You have created a strong password for your email account, should you use the same strong password for the information system you use at work?	Yes No	
3c	You receive an email which you are not expecting that says it is from CQC. The email asks you to save	Open the document before you save it just to be sure it is not a scam	

Question		Answer options	Comment
	the attachment quickly for best results and then open it. What should you do? Choose one	Save the document and then open it as CQC correspondence is very important Report it to your manager and delete it without opening the attachment	
3d	Which of the following are ways you could protect your mobile phone from being used without your permission? Choose all correct answers	PIN Password Facetime Fingerprint WhatsApp Biometric facial recognition	
3e	Which of the following are ways that you could protect paper records from being seen by people who shouldn't have access to them? Choose all correct answers	Lock them in a filing cabinet when not in use Keep confidential files with you rather than leaving them in a car if you are driving between visits/offices	

Question		Answer options	Comment
		Have a clear desk policy so that no paperwork is left out for others to see when you finish work Make sure that all staff and visitors wear a security badge/identity badge	
3f	You have been sent a message from a colleague asking you to follow a link to a website where you can make money quickly. What should you do? Choose one	Reply to them and ask for more information Select the link to find out more Phone them or get in touch in another way to see if they sent the message	

Quiz answers: Be aware of the risks to keeping data safe and know how to avoid them

This quiz will provide evidence to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#). The correct answers are shown below. The pass mark is 80% or 5 out of the 6 questions.

Question	Answer	Explanation
3a Which of these is a strong password and harder for a hacker to guess?	monkeyspoonCh2air	The National Cyber Security Centre has guidance on what makes a good password . They recommend using 3 random words . Don't use easy to guess words such as the name of your child, family pet or favourite football team.
3b You have created a strong password for your email account, should you use the same strong password for the information system you use at work?	No	Never use the same password for all your accounts. Don't share your passwords with other people.
3c You receive an email which you are not expecting that says it is from CQC. The email asks you to save the attachment quickly for best results and then open it. What should you do?	Report it to your manager and delete it without opening the attachment	Attachments like this could be a way of putting viruses on your computer or IT system. Do not open attachments, or click on links in emails, that you are not expecting. Always report them.

Question		Answer	Explanation
3d	Which of the following are ways you could protect your mobile phone from being used without your permission?	PIN Password ~~Facetime~~ Fingerprint ~~WhatsApp~~ Biometric facial recognition	This is the most important part about keeping your phone safe. If someone can't get into your device, they can't see your apps or access your emails. PIN number, face or fingerprint matching, patterns and passwords can all be used to lock devices.
3e	Which of the following are ways that you could protect paper records from being seen by people who shouldn't have access to them?	Lock them in a filing cabinet when not in use Keep confidential files with you rather than leaving them in a car if you are driving between visits/offices Have a clear desk policy so that no paperwork is left out for others to see when you finish work	All of these are ways that you can keep paper records safe.

Question		Answer	Explanation
		Make sure that all staff and visitors wear a security badge/identity badge	
3f	You have been sent a message from a colleague asking you to follow a link to a website where you can make money quickly. What should you do?	Phone them or get in touch in another way to see if they sent the message	Someone else may be using their account without them knowing, so it's a good idea to contact them using another way. If things seem too good to be true, they often are.

Section 4: Recognise when data has been lost, shared, seen, or used without approval and know what to do if it happens

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
All social care staff must report any data breach or near misses where information may not be safe. Data breaches could be breaches of: Confidentiality - information should only be seen by those who need to see it Integrity - information is correct and up to date Availability - information is there when it is needed to support care Data breaches and near misses could be digital, such as sending an email to the wrong person. They could be paper, for example if files containing sensitive information have been left out, or the key for the filing cabinet has gone missing, or confidential paperwork is lost or stolen, or care workers talking about a client in a cafe. All staff should be able to recognise the times when information might be put at risk. They should know how to report this. They must also understand why it's important to report near misses or breaches. Encourage staff to flag incidents, as the sooner you report an incident the quicker it can be sorted out and the less harm it will cause.	What types of incidents should you report and how would you report them? Who would you report them to? Why is it important to report an incident as soon as possible? What steps can you take to reduce the risk of a data breach? How might data be lost when it is being sent from one place to another? What might be lost or stolen that would be a worry? How should we safely get rid of old records or other paperwork?

Staff training resources

The Digital Care Hub has downloadable [Staff Guidance on Data Breaches](#) which describes what a data breach is.

Do you know who to speak to if you think there has been a data breach or a near miss?

Can you remember a time when this hasn't worked as well as it should have? What would you do differently now?

I confirm that I have discussed data breaches and incidents with my staff and am confident that the following people/teams/services are able to recognise when data has been lost, shared, seen, or used without approval and know what to do if it happens:

Signed: _____

Name: _____

Date: _____

Quiz for frontline staff: Recognise when data has been lost, shared, seen, or used without approval and know what to do if it happens

Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

Question	Answer options	Comment
4a You see that another member of staff has forgotten to lock their computer. It is showing the care record of someone your organisation supports. This is not the first time. What should you do? Choose one	Use the computer to send some e-mails Nothing. They will only be a moment Lock the computer for them and tell your line manager	
4b What should you do if you make a mistake in a care record? Choose one	Correct it as soon as you realise Ignore it, it doesn't matter	

Question	Answer options	Comment
4c What are the main causes of data breaches in the UK? Choose one	Hackers, scammers or cyber criminals IT equipment or systems failures Human error	
4d You work in a care home and accidentally take the care handover notes home with you at the end of a shift. Is this a data breach?	Yes No	
4e Which of the following are data breaches? Choose all correct answers	Sending an email that contains confidential information to the wrong person Leaving your lunchtime shopping list out on the reception desk Losing the care notes of someone you support A laptop that has copies of people's care or support plans is stolen. It is not encrypted, or the data is not password protected	

Question		Answer options	Comment
		Telling your friends or family members about the health or care needs of someone you support Changing the care notes for someone you support because you realise that you had turned up at the wrong time Receiving a phone call and not checking who you are talking to before telling them confidential information	
4f	Why is it important to report a data breach or data security incident as soon as possible? Choose one	To make sure you don't make the same mistake again To reduce the impact of any potential harm So that other users won't have to report the same incident	

Quiz answers: Recognise when data has been lost, shared, seen, or used without approval and know what to do if it happens

This quiz will provide evidence to meet requirement 3.2.1 of the [Data Security and Protection Toolkit](#). The correct answers are shown below. The pass mark is 80% or 5 out of the 6 questions.

Question	Answer	Explanation
4a You see that another member of staff has forgotten to lock their computer and it is showing the care record of someone your organisation supports. This is not the first time. What should you do?	Lock the computer for them and tell your line manager	It's important to report incidents so that all staff understand the importance of people's personal information being kept confidential. Data breaches and near misses can show where staff need extra training.
4b What should you do if you make a mistake in a care record? Choose one	Correct it as soon as you realise	Records must be correct and up to date. A mistake in a care record could cause harm to the person.

Question	Answer	Explanation
4c What are the main causes of data breaches in the UK?	Human error	Data breaches can be caused by criminals or IT problems, but the main thing to worry about is people. Most data security breaches reported to the Information Commissioner's Office have been due to human error.
4d You work in a care home and accidentally take the care handover notes home with you at the end of a shift. Is this a data breach?	Yes	It is a data breach because the data would not be available for other staff to use when they need it.
4e Which of the following are data breaches?	Sending an email that contains confidential information to the wrong person Leaving your lunchtime shopping list out on the reception desk Losing the care notes of someone you support A laptop that has copies of people's care or support plans is stolen and it	These are all breaches of either the confidentiality, integrity or availability of personal data except for leaving your shopping list out. You should always report any data breaches or near misses, even if you think it's nothing to worry about.

Question	Answer	Explanation
	is not encrypted, or the data is not password protected Telling your friends or family members about the health or care needs of someone you support Changing the care notes for someone you support because you realise that you had turned up at the wrong time Receiving a phone call and not checking who you are talking to before telling them confidential information	
4f Why is it important to report a data breach or data security incident as soon as possible?	To reduce the impact of any potential harm	If you don't report something, you could miss your chance to fix the problem and reduce any harm caused. You should always report anything that seems unusual.