Better Security, Better Care

Managers' discussion tool

Version 2 – July 2022

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 the care system and your personal responsibility to handle data safely
2. Be able to apply relevant data security and protection legislation and principles
3. Be aware of physical and digital threats to data security and know how to avoid them, including:
    i. being alert to social engineering
    ii. safe use of digital devices
    iii. safe keeping of physical records
4. Be able to identify data breaches and incidents and know what to do if one happens

Each section includes guidance notes to help you understand the topic, links to further resources (where they exist), 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 conduct 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 break it down a 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 the care system and your personal responsibility to handle personal data safely

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Good information underpins good care. Everyone who we support should be able to trust that their personal data (confidential and sensitive data in particular) are protected. This is part of our legal obligations under the UK General Data Protection Regulation (GDPR), the Data Protection Act and the common law duty of confidentiality as well as a bedrock of 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 data and it should be treated with respect, for example only shared with people who need to know it. It's important their data is used only in ways people would reasonably expect and that it stays safe. Part of keeping data safe is to record it properly, so it's important that care records are accurate and up to date. Individuals have legal rights with regards to their personal data and we have legal responsibilities or obligations to comply with. We all have a duty to handle people's personal or confidential data in a safe and secure manner AND to share it appropriately with others who need to see it.	What is personal data? Why is it important to keep personal data safe and to maintain confidentiality? What might be the consequences if data is not kept safe? What are our responsibilities about handling data? Do you know what needs to be included in the care record, why you are recording this information and how it will be used? Why is it important to record information as soon as possible? Can you identify a time/a scenario when this hasn't worked as well as it should have? What would you do differently now?
Staff training resources There is information about GDPR and the steps staff need to follow to ensure they remain compliant in the 7 minute training video called **Data protection care services training** on the Digital Social Care website here https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/ (scroll down the page) and there is **Staff Guidance on Data Sharing** available here https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/ which contain case studies to work through.	

I confirm that I have discussed the importance of data security and protection in the care system with my staff and am confident that the following people/teams/services understand their personal responsibility to handle personal data safely:

Signed: _____ Name: _____ Date: _____

Multiple choice quiz for frontline staff

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the Data Security and Protection Toolkit. Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle personal data safely

Question		Answer options	Comment
1a	True or False: We have a legal duty to respect the privacy of the people who use our care services?	True False	
1b	True or False: Sharing information with the right people can be just as important as not disclosing to the wrong person?	True False	
1c	Can someone you support ask to see and have a copy of the personal data that is held about them?	Yes No	

Question		Answer options	Comment
1d	When should information be recorded? Choose the correct answer.	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	
1e	Which of the following are examples of personal data? Choose all correct options.	The health condition(s) 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 The bank details of the people you support An anonymised list of the ages of all the people that you have cared for or supported over the last year	
1f	True or False: Under the Data Protection Act an individual member of staff cannot be held responsible for a data breach?	True False	

Multiple choice quiz for frontline staff ANSWERS

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.

1. Understand the importance of data security and protection in the care system and your personal responsibility to handle personal data safely

Question		Answer	Explanation
1a	True or False: 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, just as your employer has a legal duty and responsibility to respect your privacy as a member of staff. This includes not accessing or sharing confidential information about a person unless it is necessary for their care and in line with your company's policies and procedures.
1b	True or False: Sharing information with the right people can be just as important as not disclosing to the wrong person?	True	If you fail to share accurate, timely 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 necessary for their care.
1c	Can someone you support ask to see and have a copy of the personal data that is held about them?	Yes	Data protection law provides individuals with certain rights. People have the right to see the personal data recorded about them. This is known as a subject access request. It is unwise, therefore, to record comments or other data about individuals which you would not be comfortable with the person seeing.

Question		Answer	Explanation
1d	When should information be recorded? Choose the correct answer.	As soon as possible, whilst the event is still fresh in your mind	Record information whilst the event, care, or other support, is still fresh in your mind. Record high-risk information as a matter of urgency.
1e	Which of the following are examples of personal data? Choose all correct options.	The health condition(s) 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 The bank details of the people you support ~~An anonymised list of the ages of all the people that you have cared for or supported over the last year~~	Personal data is any information that identifies an individual, like their name and contact details for instance. Some personal data is more sensitive, like someone's health condition, and you should take special care with this data. Information about an organisation, such as the name of a business, is not personal data. Nor is anonymised data.
1f	True or False: Under the Data Protection Act an individual member of staff cannot be held responsible for a data breach?	False	Employees can face prosecution for data protection breaches and individuals have been charged and fined for causing data breaches, but in those cases they had not followed their employer's data security policies.

Section 2: Be able to apply relevant data security and protection legislation and principles

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 e.g. social workers or health workers who are involved in their care. Sharing information with the right people can be just as important as not disclosing to the wrong person. Care plans are a key record about an individual's needs and choices. They must always be kept up to date, complete, accurate and legible in order to ensure quality and consistency of care. Certain simple actions can ensure that you comply with the principles of the Data Protection Act/GDPR and your common law duty of confidentiality. We must take care to store and share information carefully to avoid unauthorised people accessing confidential information: • Think about who can overhear information being shared verbally • Check if the person you are speaking to over the telephone is genuine • Use secure email or password protect files if emailing confidential data • Log off computers or out of systems when you are finished and lock the screen if you are away from the device even if only for a short period of time • Only look at records for professional reasons • Share information if needed, but only the minimum data necessary • Take care of physical, paper records	What information do we hold on individuals who receive care and support, and staff? How can we make sure we keep this information secure? For example, are you aware of who is round you when accessing and discussing someone's personal data? Who should be able to see people's care records? What sorts of information should we not share with others? What are safe methods of sharing data? Do you save records in the right place so that they are easy to find? Are you aware of the data security and protection issues if you are working from home? Can you identify a time/a scenario when this hasn't worked as well as it should have? What would you do differently now?
Staff training resources There is information about the steps staff can take to keep information up-to-date, accurate and safe in the 11 minute training video called **Data and cyber security care services training** on the Digital Social Care website here https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/ (scroll down the page).	

I confirm that I have discussed data security and protection with my staff and am confident that the following people/teams/services are able to apply relevant legislation and principles:

Signed: _____ Name: _____ Date: _____

Multiple choice quiz for frontline staff

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the Data Security and Protection Toolkit. Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

2. Be able to apply relevant data security and protection legislation and principles

Question		Answer options	Comment
2a	It is good practice to keep duplicate care records in case one is lost or becomes corrupted? Choose all correct options.	Electronic care records should be regularly backed up in-case they are lost or become corrupted. Having duplicate working records can lead to confusion over a person's care. The more records you have for someone the better.	
2b	Who should have access to people's care records, including confidential information about their care? Choose the correct answer.	All the staff, we need to know what's going on Only the senior staff and managers, so that its kept safe Only those staff involved in their care should look at their records	
2c	True or False: If you have previously obtained someone's consent to access 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	

Question		Answer options	Comment
2d	How could you safely share confidential information with another person? Choose all correct options.	You take the person to a private and safe area to discuss the matter 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 options.	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	
2f	You are in the supermarket when you overhear two other members of staff talking about someone you provide care for. What should you do? Choose the correct answer.	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	

Multiple choice quiz for frontline staff ANSWERS

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.

2. Be able to apply relevant data security and protection legislation and principles

Question		Answer options	Comment
2a	It is good practice to keep duplicate care records in case one is lost or becomes corrupted? Choose all correct options.	Electronic care records should be regularly backed up in-case they are lost or become corrupted. Having duplicate working records can lead to confusion over a person's care. ~~The more records you have for someone the better.~~	It is good practice to regularly back-up electronic files in-case of corruption so that you have a recent copy to go back to if needed, it's best if this is an automatic process that happens in the background. In-terms of the working records used to deliver people's daily care, you should check to ensure one doesn't already exist before creating any new records. Duplicate records can lead to confusion about a person's care.
2b	Who should have access to people's care records, including confidential information about their care? Choose the correct answer.	Only those staff 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	True or False: If you have previously obtained someone's consent to access 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 purpose, providing you have previously informed the person - they should know what is happening and have no objections.

Question		Answer options	Comment
2d	How could you safely share confidential information with another person? Choose all correct options.	You take the person to a private and safe area to discuss the matter ~~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 these options are ways that you could use to securely transmit 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? Choose all correct options.	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 and with others, e.g. social workers or health workers, who are involved in their care.
2f	You are in the supermarket when you overhear two other members of staff talking about someone you provide care for. What should you do? Choose the correct answer.	Speak to them and say that this behaviour breaches confidentiality	Whilst people would expect their confidential information to be shared in a way that enables care staff to provide their care, they would not expect it to be discussed in a public place where it can be overheard, this would compromise their privacy.

Section 3: Be aware of physical and digital threats to data security and know how to avoid them

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Social engineering Social engineering is when someone uses tricks to manipulate people to gain access to your building, information or systems, and it could happen in person, on email, on social media or over the phone. It can appear genuine, but it's actually a scam. Sometimes it's referred to as 'phishing'. Phishing attempts might try to trick you into revealing sensitive information or may tempt you to click on a link that goes to a dodgy website or attachment that is infected with a virus. Know the signs, trust your instincts, challenge and report anything suspicious. Look out for: • signs of urgency and importance • messages not addressed to you personally • unexpected contact or strange requests • spelling or grammar errors Delete suspicious emails and do not click on links or open attachments in these emails before you delete. Do not respond to them even if they seem to come from a company or person you may know. Responding can confirm that your address is legitimate to the sender.	In what ways could we be 'socially engineered' or scammed relating to work? What should you look out for to try to be alert to potential attempts to trick us? Describe what a phishing email is? What steps can you take to check that an email is genuine? What should you do if you suspect that an email is not genuine? What should we look out for on a website to check if it is genuine? Can you identify a time/a scenario when this hasn't worked as well as it should have? What would you do differently now?
Staff training resources For more information there is a free interactive, short course **Being Safe Online** (https://www.bt.com/skillsfortomorrow/home-life/being-safe-online) from BT, which covers fraud and scams as well as how to stay safe online more generally (takes about 10-20 minutes, need to register, free of charge). There is also an interactive government eLearning training package on cyber security: **Top Tips for Staff** (which takes about 15 minutes to work through) https://www.ncsc.gov.uk/training/top-tips-for-staff-scorm-v2/scormcontent/index.html#/	

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
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 when using digital devices like computers or smartphones include: • 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 • Installing 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 discuss work related topics? Are they protected by a password, or PIN or another way? Do you lock them when you are not using them? What are examples of commonly used passwords such as 'password1' which you should avoid? 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 improve them? Have we got our computers/phones set to automatically update newer versions of software?
Staff training resources For more information there is a free course **Keep Safe Online** (https://digital.wings.uk.barclays/view-our-digital-courses/keep-safe-online/) from Barclays Digital Wings, which covers passwords, and protecting devices and data as well as fraud and scams (need to register, free of charge). There is also government advice on how to stay safe online (which contains a 2 min video): **Cyber Aware** https://www.ncsc.gov.uk/cyberaware/home	

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
Safe keeping of physical records Taking simple precautions will reduce the risk that personal or confidential paper records are lost, stolen or accessed by people who shouldn't see them. Confidential data should not be left out where unauthorised people can see it and physical controls like lockable doors, windows, filing cabinets or secure areas can help. It is particularly important to take precautions if paper records are taken out of the building, for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. We also have to be careful when disposing of any personal or sensitive information. Paper documents should be securely shredded.	How can physical records be kept secure? Do you always put away care or other records when you've finished using them? What sort of documents is it ok to throw in the bin? What need to be shredded? Can you identify a time/a scenario when this hasn't worked as well as it should have? What would you do differently now?

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

Signed: _____ Name: _____ Date: _____

Multiple choice quiz for frontline staff

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the Data Security and Protection Toolkit. Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

3. Be aware of physical and digital threats to data security and know how to avoid them

Question		Answer options	Comment
3a	Which of these is a strong password and therefore harder for a hacker to crack or guess? Choose the correct answer.	123456 qwerty Password1 monkeyspoonCh2air	
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, it urges you to save the attachment for best results and then open it. What should you do? Choose the correct answer.	Open the document before you save it just to be sure it is not a scam. 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.	

Question		Answer options	Comment
3d	Which of the following are ways you could protect your mobile phone from being used without your permission? Choose all correct options.	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 options.	Locking them in a filing cabinet when not in use Keeping confidential files with you rather than leaving them in a car if you are driving between visits/offices Having a clear desk policy so that no paperwork is left out for others to see when you finish work Ensuring 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 the correct answer.	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	

Multiple choice quiz for frontline staff ANSWERS

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.

3. Be aware of physical and digital threats to data security and know how to avoid them

Question		Answer	Explanation
3a	Which of these is a strong password and therefore harder for a hacker to crack or guess? Choose the correct answer.	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 and don't share your passwords with other people.
3c	You receive an email which you are not expecting that says it is from CQC, it urges you to save the attachment for best results and then open it. What should you do? Choose the correct answer.	Report it to your manager and delete it without opening the attachment.	It should be reported and deleted - sending attachments like this could be a way of installing viruses or ransomware on your computer or IT system. Do not open attachments, or click on links in emails, that you are not expecting.
3d	Which of the following are ways you could protect your mobile phone from being used without your permission? Choose all correct options.	PIN Password ~~Facetime~~	This is the most important element of phone security, if someone can't get into your device they can't see your apps or access your emails. Facial recognition, PIN number, fingerprint recognition, patterns and passwords can all be used to lock devices.

Question		Answer	Explanation
		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 options.	Locking them in a filing cabinet when not in use Keeping confidential files with you rather than leaving them in a car if you are driving between visits/offices Having a clear desk policy so that no paperwork is left out for others to see when you finish work Ensuring that all staff and visitors wear a security badge/identity badge	All these options are ways that you could protect paper-based records.
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 the correct answer.	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 via another means. If things seem too good to be true, they often are.

Section 4: Be able to identify data breaches and incidents and know what to do if one happens

Discussion topics to cover/managers' guidance notes	Questions/discussion prompts
All social care staff have a duty to report any data breaches or incidents where data security might have been compromised. Data breaches could be breaches of: • Confidentiality - information should only be seen by those who need to see it • Integrity - information is accurate and up to date • Availability - information is there when it is needed to support care Data breaches and incidents could be digital, such as sending an email to the wrong person, or non digital, for example if files containing sensitive information have been left lying around, or the key for the filing cabinet has gone missing, or confidential paperwork is lost or stolen, or care workers discussing a client in the pub. All staff must be able to spot common activities where information could be compromised and know how to report incidents. They must also understand why it's important to report incidents or breaches. Encourage staff to flag incidents, as the sooner you report an incident the quicker it can be resolved and the less damage 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 could data be lost in transit? What might be lost or stolen that would be a worry? How should we dispose of records or other paperwork? Do you know who you should speak to if you have concerns about a potential incident or breach? Can you identify a time / a scenario when this hasn't worked as well as it should have? What would you do differently now?
Staff training resources Digital Social Care has downloadable **Staff Guidance on Data Breaches** which defines what a data breach is: https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/	

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 identify data breaches and incidents and know what to do if one happens:

Signed: _____ Name: _____ Date: _____

Multiple choice quiz for frontline staff

This quiz will provide evidence that you have completed data security and protection training that meets requirement 3.2.1 of the Data Security and Protection Toolkit. Circle or tick the correct answers and write any questions in the comment boxes.

Name: _____ Date: _____ Score: _____

4. Be able to identify data breaches and incidents and know what to do if one happens

Question		Answer options	Comment
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? Choose the correct answer.	Use the computer to send some e-mails Nothing. They will only be a moment Lock the computer for them and report the incident to your line manager	
4b	You notice that a fax has arrived on the fax machine with hospital discharge papers; the fax machine is in a public area. What should you do? Choose the correct answer.	Turn the papers upside down so that no one can see them Hand over the papers to your line manager and report the incident to them Read the papers to see who they are talking about	
4c	What are the main causes of data breaches in the UK? Choose the correct answer.	Hackers, scammers or cyber criminals IT equipment or systems failures Human error	

Question		Answer options	Comment
4d	You work in a care home and accidently 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 options.	Sending an email that contains confidential data to the wrong person Overreacting to scare stories about cybercrime Losing the care notes of someone you support A laptop that has copies of people's care or support plans is stolen and it 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? Choose the correct answer.	To reduce the impact of any potential harm	

Multiple choice quiz for frontline staff ANSWERS

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.

4. Be able to identify data breaches and incidents and know what to do if one happens

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? Choose the correct answer.	Lock the computer for them and report the incident to 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 also help to identify staff training needs.
4b	You notice that a fax has arrived on the fax machine with hospital discharge papers; the fax machine is in a public area. What should you do? Choose the correct answer.	Hand over the papers to your line manager and report the incident to them	It's important to limit the use of methods of communication that aren't secure to protect people's rights to confidentiality. Where the use of fax machines is unavoidable other measures should be taken to ensure confidentiality can be maintained such as locating the fax machine in a secure area, adding a PIN or swipe card or ensuring the right person is available to receive documents and requiring a received receipt.
4c	What are the main causes of data breaches in the UK? Choose the correct answer.	Human error	Scammers, cyber criminals, and dodgy IT can all cause data breaches but the main thing to worry about is people. Most data security breaches reported to the Information Commissioner's Officer have been due to human error.

Question		Answer	Explanation
4d	You work in a care home and accidently 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? Choose all correct options.	Sending an email that contains confidential data to the wrong person ~~Overreacting to scare stories about cybercrime~~ Losing the care notes of someone you support A laptop that has copies of people's care or support plans is stolen and it 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	These are all breaches of either the confidentiality, integrity or availability of personal data except for overacting to scare stories. It is better to overreact to cybersecurity dangers than not give it sufficient importance. If in doubt 'call it out'.

Question		Answer	Explanation
4f	Why is it important to report a data breach or data security incident as soon as possible? Choose the correct answer.	To reduce the impact of any potential harm	If you don't report an incident, you could miss your chance to resolve the problem and reduce the potential harm caused. You should always report anything that seems unusual. If in doubt, ‘call it out’.