Better Security, Better Care

Data Security and Protection Toolkit (DSPT) Action Plan – Data Security

Evidence item	Question	Tooltip	Action
1.6.2	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.	
1.6.3	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.	

Evidence item	Question	Tooltip	Action
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. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to the Information Commissioner's Office (ICO). If you are not sure whether or not to inform the ICO of a breach, this	

Evidence item	Question	Tooltip	Action
		toolkit’s incident reporting tool and guide can help you to decide.	
6.1.4	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.	
6.1.5	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. More information is available from the Information Commissioner’s Office https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/	
7.1.2	Does your organisation have a business	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	

Evidence item	Question	Tooltip	Action
	continuity plan that covers data and cyber security?	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). An example business continuity plan is available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/templatepolicies/	
7.2.1	How does your organisation test the data and cyber security aspects of its business continuity plan?	Describe how your organisation tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be since 1st April 2020. Guidance for testing your business continuity plan for the data and cyber security aspects is available from Digital Social Care. https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/	