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

Evidence item	Question	Tooltip	Action
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 in https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/ .	

Evidence item	Question	Tooltip	Action
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 https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/	
2.2.2	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. There is an example staff contract clause available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/	
3.1.1	Has a training needs analysis covering data	A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across	

Evidence item	Question	Tooltip	Action
	security and protection, and cyber security, been completed since 1st April 2020?	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. An example training needs analysis is available to download from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/	
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. Digital Social Care provides guidance on training, including sources of free online data and cyber security training:	

Evidence item	Question	Tooltip	Action
		https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/	
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.	
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	