Better Security, Better Care

Data Security and Protection Toolkit (DSPT) Action Plan –

Policies and Procedures

Evidence item	Question	Tooltip	Action
1.2.1	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.	

Evidence item	Question	Tooltip	Action
		Policy templates are available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/	
1.3.1	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] (https://ico.org.uk/for-organisations/data-protection-fee/). You can check whether you are registered and what your ICO registration number is on the [Information Commissioner's Office website] (https://ico.org.uk/esdwebpages/search)	
1.3.2	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. An example privacy notice is available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/	

Evidence item	Question	Tooltip	Action
1.4.1	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 saved. Example IARs and ROPAs are available from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/	
1.5.2	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,	

Evidence item	Question	Tooltip	Action
		if applicable. There is an example audit checklist that you can download from Digital Social Care https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/	
1.6.1	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'. There is [guidance on data protection by design and by default on the ICO's website] (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/). The Data Protection Policy template that is available from [Digital Social Care] (https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/) covers this subject.	
1.6.5	Does your organisation's data protection policy describe	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	

Evidence item	Question	Tooltip	Action
	how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?	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.	
1.7.2	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	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 organisation. Details are available from the ICO https://ico.org.uk/media/fororganisations/documents/1475/deleting_personal_data.pdf. If you do not use third parties to destroy records or equipment, then	

Evidence item	Question	Tooltip	Action
	protection regulations.	tick and write “Not applicable” in the comments box. Advice on contracts for secure disposal of personal data is available from Digital Social Care https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/	
1.7.3	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. Digital Social Care has a Record Keeping policy that has details on the safe destruction of personal data https://www.digitalsocialcare.co.uk//latest-guidance/template-policies/	
1.7.4	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. (https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016)	

Evidence item	Question	Tooltip	Action
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. A template example is available from Digital Social Care https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/	