GDPR / Data Protection Act (DPA 2018) Questionnaire

Preparation			Delete as appropriate	Comments
01	Where do I start?	Have you prepared a flow chart to guide you through the steps to compliance?	Yes/ No	
02	Glossary and Further Information	Do you understand the terminology used within the Data Protection Act 2018?	Yes/ No	
03	Data Mapping	Have you mapped all the personal data you process and store?	Yes/ No	
04	Legitimate Interests: 3-part balance test	Do you understand how to establish whether 'legitimate interests' is the most appropriate lawful basis (for certain processing activities)?	Yes/ No	
05	Legitimate Interests Assessment (LIA)	Do you have a template to aid your decision when balancing the interest of a data subject, against your charity's legitimate business interests?	Yes/ No	
General				
06	CCTV Policy	Does your organisation have CCTV for crime prevention purposes; if so, do you have a policy?	Yes/ No	
07	Cookie Policy	Do you have a Cookie policy for your website (if relevant)?	Yes/ No	
08	Data Controller to Processor Contract	Do you have a template or know how to prepare a Contract between a Data Controller and a Data Processor?	Yes/ No	
09	Data Controller to Processor Contract – Guidance Notes	Do you understand how to prepare a contract between a Data Controller and a Data Processor?	Yes/ No	
10	DPIA Checklist – is it necessary?	Can you identify whether completing a Data Protection Impact Assessment is necessary?	Yes/ No	
11	DPIA Template	Do you have a Data Protection Impact Assessment template?	Yes/ No	
12	Data Protection Policy	Do you have a policy aimed at all staff and/ or charity representatives who process personal data on your behalf?	Yes/ No	
13	Data Retention Policy & Schedule	Do you know how long you store files and documentation for, in line with the storage limitation principle?	Yes/ No	
14	Information Asset Inventory & Risk Assessment Template	Have you completed an inventory of all personal data assets, with associated risk assessment etc.?	Yes/ No	
15	Information Security Policy	Do you have a policy stating the measures you have in place to protect the confidentiality, integrity and availability of personal data, processed electronically and physically?	Yes/ No	

16	Privacy Notice for Members/ Customers	Do you have a Privacy Notice for Members/ Customers?	Yes/ No	
17	Privacy Notice for Employees	Do you have a Privacy Notice for Employees?	Yes/ No	
18	Privacy Notice for Job Applicants	Do you have a Privacy Notice for Job Applicants (ideally placed on application form)?	Yes/ No	
19	Staff Training Matrix	Do you keep a record of staff data protection (and other) training?	Yes/ No	
20	User Access Log	Do you keep a log of which staff have access to each electronic and physical system?	Yes/ No	
Subject Access Requests				
21	Subject Access Request Policy	Do you have a policy which outlines how to identify SARs, who has responsibility, etc.?	Yes/ No	
22	SAR Register	Do you have a log of all Subject Access Requests?	Yes/ No	
23	SAR Checklist/ Procedure	Do you know how to respond to a SAR?	Yes/ No	
24	SAR Letter of Acknowledgement	Do you know how to prepare a letter formally acknowledging a subject access request?	Yes/ No	
25	SAR – Verbal Verification of ID	Do you have a script for phone calls, to verify the identity of a data subject requesting a copy of their personal data?	Yes/ No	
26	SAR – Written Verification of ID	Do you have a template of a letter requesting ID, to verify identity of a data subject requesting a copy of their personal data?	Yes/ No	
27	SAR Data Map	Do you Map where all personal data is stored, based on data subject categories, and refer to this to locate data to send in response to SAR?	Yes/ No	
28	SAR Letter Advising Subject of Extension	Do you have a template of a letter to a data subject informing them that an extension of an additional 2 months to respond is required?	Yes/ No	
29	SAR Letter responding to subject with data	Do you have a template of a letter to a data subject, with requested data enclosed, or to invite to view on site?	Yes/ No	
35	SAR Letter Advising Subject of Fee	Do you have a template of a letter to a data subject informing them that you need to charge a reasonable fee due to the cost of providing the information requested?	Yes/ No	

Data Breach				
30	Data Breach Policy	Do you know what to do if a data breach is suspected or actualised?	Yes/ No	
31	Data Breaches – what you need to know	Do you know what constitutes a data breach under the GDPR?	Yes/ No	
32	Data Breach Procedure for Notification to ICO	Does the DPO/ DP Representative know the steps to follow to record a data breach, how to establish whether it requires notifying the ICO, and the procedures for doing so?	Yes/ No	
33	Data Breach Notification Procedure to Data Subject	Does the DPO/ DP Representative know the Steps to follow to record a data breach, how to establish whether it requires notifying the Data Subject, and the procedures for doing so?	Yes/ No	
34	Data Breach Register	Do you keep a numbered log recording all Data Breaches that you become aware of, and whether they require notification to ICO and Data Subject/s?	Yes/ No	