DATA PROTECTION POLICY GUIDELINES

All charities will collect, store and process personal information; usually in relation to staff, trustees, job applicants, volunteers and beneficiaries. The Data Protection legislation requires every data controller (e.g. employer) who processes personal information to register with the Information Commissioner's Office (ICO), however not for profit are exempt).

The General Data Protection Regulations (GDPR) provides a range of rights to Data Subjects and places obligations on those processing data. It also provides for tough penalties for non-compliance.

Because charities often collect such a wide range of information and store and use it in different ways it is important to understand how the Act applies to your organisation specifically. These guidelines are designed to help small charities consider the range of factors that may be relevant when drafting such a policy.

When drafting or updating your Data Protection Policy, the ICO is a good place to start. They publish a wealth of information on their website including:

- A Guide to the General Data Protection Regulation
- A data protection self-assessment
- A quick guide to the Employment Practices Code
- Information specifically for charities
- A privacy toolkit for charities

The following questions/points may also help to guide you on the areas to cover:

- Who does the policy apply to?

GDPR defines the roles of 'Controller' and 'Processor'. The Controller determines how and why personal data is processed and the Processor acts on the controller's behalf. Processors have specific obligations and legal liability if there is a breach.

- Be familiar with the data protection principles and ensure that your policy states what these are. The GDPR principles are similar to those in the DPA, with added detail and a new accountability principle.

- Allocate responsibility for GDPR compliance to a designated individual and consider whether you need to appoint a Data Protection Officer (DPO). A DPO must be appointed if you are a public authority or body, or if you carry out certain types of processing activities.

- You should explain what personal data is and provide examples of the personal data that you may collect. The definition of Personal Data has become more detailed and broader under GDPR. An IP address or CCTV footage can now be personal data. Personal Data is likely to include details of donors, beneficiaries as well as job applicants and people who work for the charity as staff or volunteers (including trustees).

- Personal data and sensitive personal data are different. A definition and examples would help staff to understand the difference and how they are expected to collect, use and store the information. Again, the Information Commissioner website provides useful information.

- Under the DPA you need to state the conditions for processing data (both ordinary and sensitive).

Under GDPR, charities will need to identify and document a lawful basis before personal data can be processed. The lawful basis for processing personal data can determine individuals' rights. For example, relying on 'consent' means the individual will generally have more rights.

• Ensure that your policy explains how your charity demonstrates compliance with the GDPR principles. Specifically, that you have an up-to-date data register that provides details on personal data processed by the organisation, why it is being processed, the categories of individuals and categories of personal data, retention schedules etc…

• Under the DPA, an individual has limited right to request personal data is erased. For example, where processing causes unwarranted and substantial damage or distress. Under GDPR, the right to be forgotten enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

• Retention of data – under what circumstances is data retained and not retained? Your policy should consider what data is destroyed and when. Allocating staff to this via job descriptions will help to ensure it is kept in focus.

• Access to data – those whose personal data you process (applicants, staff, volunteers and beneficiaries), have the right to request that this information is sent to them. Under GDPR access to the information is free of charge and employers have one month in which to comply. Charities may refuse, or levy a reasonable fee, if the request is unfounded or excessive.

• Storage and security – how will data be stored? Who will have access to the data? What will happen if a third party processes data? What steps should staff take to ensure that there is no unauthorised access to the data (for example, drawers must be locked, screens should be locked when staff step away from their desks etc)? What about if/when data is taken off site (for example that only encrypted data sticks must be used, that any manual files are logged out and back in, that leaving files on car seats is considered a security breach and a disciplinary matter etc)?

• Be clear about the process to follow if you discover a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

• Your Data Protection Policy should be consistent with your Privacy Notice, which should be communicated to all those whose personal data you collect and process.