Guidance Note on Preparing for the General Date Protection Regulations (GDPR)

1. This note is based upon guidance from the Information Commissioner's Office (ICO) entitled 'Preparing for the General Date Protection Regulations (GDPR)– 12 steps to take now'.

Awareness

2. According to the ICO, the first step is awareness and ensuring that decision makers and key people in the organisation are aware that the law is changing to the GDPR. If you haven't already, you need to get this on your organisation's agenda now.

Information

3. The second step relates to knowing the information that held. This involves documenting:

    - The personal data held
    - Where it came from
    - Who it's shared with

4. This second step underpins many of the other steps and so it would appear that the most immediate action point is to undertake an information audit (see attached).

Privacy Notices and Lawful basis for processing data

5. Under the GDPR there are some additional points to add to your privacy notices ahead of GDPR implementation. These include:

    - Explaining the lawful basis for processing the data
    - Data retention periods
    - An individual's right to complain to the ICO is they think there is a problem with the way the data is being handled.

6. Clearly, the information audit needs to be undertaken first to analyse the types of personal data held in order to determine the lawful basis for processing.

Individual rights and Subject Access Requests

7. Individual rights under the GDPR are similar to those under the Data Protection Act but some are enhanced. For example, the right to have

personal data deleted. You should therefore review your Data Protection Policy to ensure you would be able to meet such a request.

8. There are also some amendments to the rules on Subject Access requests and in particular the timeframe for complying.

Consent

9. One of the biggest changes under the GDPR relates to the way in which consent is sought, recorded and managed. It must be freely give, specific, informed and unambiguous. There must be a positive opt-in and it cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions.

10. You are NOT required to gain fresh consent for any existing consents unless reliance upon individual consent is the lawful basis for processing.

Data breaches

11. There are also some changes to the reporting of data breaches. Certain types of data breaches will need to be reported to the ICO where a breach is likely to result in a risk to the rights and freedoms of individuals such as:

    - Discrimination
    - Damage to reputation
    - Financial loss
    - Loss of confidentiality
    - Other significant economic or social disadvantage

12. This will first require an understanding of the information you process and as such this area cannot be reviewed until after the information audit.

ACTION PLAN

ACTION	BY WHOM	BY WHEN
Information audit	All	ASAP
Identify lawful basis for processing		After Information Audit – before GDPR implementation 25.05.18
Review Privacy Notices		After Information Audit - before GDPR implementation 25.05.18
Review Data Protection Policy to ensure you have a procedure in place to respond to a request for the deletion of personal data.		Before GDPR implementation 25.05.18
Review Data Protection Policy to cover new rules on Subject access requests e.g. 1 month to comply rather than current 40 days		Before GDPR implementation 25.05.18
Review your processes for obtaining consent		Before GDPR implementation 25.05.18
Review your processes in the event of data breach		After Information Audit - before GDPR implementation 25.05.18
Consider whether data security is as robust in relation to trustees as for employees		Before GDPR implementation 25.05.18

INFORMATION AUDIT

What data do you collect? **E.g.** Name, email address, social media posts, location, IP address	
Where do you store the data? **E.g.** Emails, documents, databases, backups, email lists	
Who has access to the data/ who do you share the data with **E.g.** Staff / trustees / other N.B For each of these people, analyse data usage, storage, security	
How do you protect and document the data you have? **E.g.** Passwords, limited access, databases	
How long do you plan to keep the data for? Three Years, Five Years etc…	
Do you have a function/ reason for every piece of data you collect?	
What is the process if someone asks to be removed from your records?	