GDPR Top Ten Tips

1. GDPR doesn't only apply to data held electronically it also applies to data held in hardcopy form.

2. Only collect the information that you need. If you cannot demonstrate a legitimate reason why you need an individual's personal data then don't obtain it. You cannot be held responsible for data that you don't possess.

3. Undertake a comprehensive data audit of all the data in your possession. Until you know what data you have and where it is, GDPR compliance is impossible.

4. Keep your privacy policies under review. Make sure you tell people what their information is needed for, what it will be used for and what rights they have. Each Congregational Committee should have appointed a Data Protection Lead. Unless someone takes the lead on data protection there is a real risk of non-compliance.

5. Consider the impact of a breach. If you have personal data that could, if lost or misappropriated, cause harm or loss to the individuals concerned then pay particular attention to that data as to its security from collection through to disposal.

6. In the event of a breach follow the procedures set out in your Breach Policy Document.

7. Communication and training are essential. Although there are many instances of data being stolen by hackers or through data theft the majority of data breaches are still due to human error – data left unattended, given out inappropriately, disposed of in an unsecure manner etc.

8. Keep your personal data secure and keep it only for as long as you need it. Lock it away, restrict access to it, don't leave it unattended. If held electronically, use password protection and ensure antivirus protection is kept up to date.

9. When publishing information, where possible and appropriate, make individuals anonymous or use pseudonyms to protect and minimise the risks associated with processing personal data (see further information on this overleaf).

10. Apply a common sense approach. Don't use the data in a way that would surprise the person e.g. by passing it on without authority or using it for another purpose.

Anonymisation

Anonymous information - information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The GDPR does not apply to anonymised information.

Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.

Pseudonymisation

Pseudonymisation, which is not the same as anonymisation, is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual"