Data Protection

Whilst the digital age has created many advances in the world of communication, it has also brought some challenges. Increased availability of information has meant we have to work significantly harder to protect personal data. Indeed, theft of information is now the modern-day burglary, with seven tenths of frauds being cyber-related. The Regulator, the Information Commissioner's Office ('ICO') has also seen an increase in its monitoring and enforcement powers which include the ability to issue enforcement notices, criminal sanctions and fines of up to £500,000. Charities are not immune, with several instances of high profile enforcement having been implemented. For a charity, the risk of not only a financial penalty but of the reputational damage resulting from a publicised breach of the Data Protection Act 1998 is significant.

A breach could occur through, for example, the theft of a laptop, the loss of an unencrypted electronic device or the mistaken transfer of data, if the information lost, stolen or transferred contains personal data.

The charity trustees of a congregation are ultimately responsible for compliance in this area.

The Regime

EU Data Protection Directive 95/46/EEC was designed to protect the privacy of all personal data collected for or about citizens of the EU especially as it relates to processing, using or exchanging such data. The UK implements that Directive through the Data Protection Act 1998. The Directive is being replaced by a new General Data Protection Regulation which will come into force across the EU in May 2018 and updated advice and guidance will be issued over the next year so as to facilitate ongoing compliance with the law in this area.

A Church of Scotland congregation is a 'Data Processor' in terms of the Act. As such, congregations process 'Sensitive Personal Data' about individuals connected with the congregation, referred to in the legislation as 'Data Subjects'. The data is 'Sensitive' as it is indicative of a person's religious beliefs. In addition, congregations may also be holding financial data and health/other information from a pastoral care perspective.

Anyone who processes personal information must comply with the eight data protection principles contained within the Act. Information must:

- Be processed fairly and lawfully
- Be obtained for specific and lawful purposes
- Be kept accurate and up to date
- Be adequate, relevant and not excessive
- Not be kept for longer than is necessary
- Be processed in accordance with the rights of data subjects
- Be kept secure to prevent unauthorised processing and accidental loss, damage or destruction
- Not be transferred to any country outside the EEA unless certain considerations apply

The Way Forward

It is likely that your Presbytery Clerk, as Data Controller for the congregations within the Presbytery bounds, will ask each congregation to appoint an individual as the Data Protection Representative. It is therefore suggested that congregations appoint an office bearer to implement the following:

1. Implement a Data Protection Policy

This is a straightforward task as a style is contained in the Data Protection Pack for Congregations. However, it is not sufficient to simply reproduce the style and then file it away. As with all policies, it must be acted upon. Office bearers must familiarise themselves with the published policy and implement its procedures and ensure that others are doing so.

2. Consent for Personal Data

The Data Protection Act allows congregations to process data without explicit consent provided that the information is not shared with third parties and that the data protection principles are complied with so far as the storage, security, accuracy and relevancy of such information is concerned. It is, however, good practice to make it clear to members that their personal details are held, and continue to be securely held, by the congregation in connection with the purposes of the Church of Scotland.

Members can at the same time be reminded that they can opt-out of their data being held and that they should provide the congregation with any updated personal information (new addresses/contact numbers etc.). This could perhaps be brought to members' attention by way of notices in the Church/the Church bulletin/website etc. Members might also be reminded to provide any updates to their details in order to ensure they are up to date. Information should not be shared with any parties unconnected with the Church and data should not be stored or transferred out with the EEA. Further information can be found in the Data Protection Pack for Congregations.

3. Information Security Risk Assessment

It is likely that you will be asked by Presbytery Clerk to undertake a risk assessment of all buildings where personal data is stored. A style is available in the Data Protection Pack for Congregations. This should highlight any areas of risk. It is also likely that you will need to confirm to your Presbytery Clerk through the Roles and Records System/local Church Review that you are complying with Data Protection law.

4. Information Security & Encryption

It is likely that there will be a Presbytery decision requiring that data being held or stored electronically be protected by encryption. Encryption is a form of complex password protection that scrambles information on a device and requires a password to unlock the information. There is not much difference between the cost of an encrypted USB device and one that is not. However, using an encrypted device may avoid a monetary penalty from the ICO if that device is lost or stolen. Do also bear in mind that information security applies equally to manual records. Paper records containing personal data should be securely stored in lockable, fire-resistant storage with the key stored separately and securely. Information Security Hints and Tips are contained within the Data Protection Pack for Congregations.

5. Subject Access Request

If you receive a request from an individual looking to obtain a copy of the information stored about them, please let your Presbytery Clerk know immediately as there are important time limits that must be complied with. Advice should also be sought from the Law Department.

6. Training

It is important that data protection does not fall off your radar. All office bearers and those handling personal data should watch the Law Department's training 'webinar' on the subject. It can be accessed from the Data Protection Pack for Congregations with the password: *cos2014.* When a new office bearer is appointed they should attend this training. It would also be good practice to have your office bearers and any 'home workers' (those working on church business using their home computers) sign up to the eight data protection principles.

7. If There Is a Breach…?

If the worst happens and there is a breach please contact the Law Department using the Breach Notification form contained in the Data Protection Pack for Congregations. The Law Department will be able to assess whether the breach requires to be reported to the ICO. They may be able to assist with containing the breach and correcting things for the future.

Further reading and resources

The Law Circulars section of the Church of Scotland -
www.churchofscotland.org.uk/resources/subjects/law_circulars#data_protection