GDPR: INFORMATION STORAGE PRACTICAL HINTS AND TIPS

Introduction

This note should be read in conjunction with the GDPR Webinar and FAQs available at [insert link].

Electronic Files: what is encryption?

Encryption is the process of scrambling the contents of electronic files stored on a computer in such a way so that only those who are authorised can read them. The computer files are encrypted with software that uses a complex password as a key to unlock the computer and descramble the information into a readable form. As a result, the password must be stored separately from the device.

If congregations are using moveable storage devices such as laptops and/or USB sticks and the device (containing sensitive personal data) is lost or stolen, if the device is encrypted the information is secure and the Information Commissioner is unlikely to issue a monetary penalty. If the device is not encrypted congregations will be taking a risk that a financial penalty may be imposed. Fines imposed under GDPR are significantly higher than the previous regime.

Consideration should be given to encryption of church office computers and indeed the personal computers of office bearers who are storing sensitive personal data at home. Congregations should assess the necessity of this and their own risk in this respect.

Encryption Software: which one to choose?

Windows computers can be encrypted using the following software:

- Microsoft BitLocker: available in Windows 7 Enterprise or Windows 8 and Windows 10 Professional or Enterprise
- Symantec Endpoint Encryption
- McAfee Total Protection (the FileLock feature)
- Kaspersky Total Security

The Church of Scotland IT Department use Microsoft BitLocker. The IT Department cannot therefore advise how easy or difficult it is to use the other products; how they impact on the performance of the computers once the software is installed; or indeed how easy or difficult it is to install and configure the particular software.

If congregations have a member who is especially IT literate it may be felt sufficient to have them assist with the encryption process. It is estimated that an annual cost of around £50 per device for the software package is reasonable. For those less confident, a local IT company will be able to assist but they may charge a call out fee.

Password Protection of Documents

In addition to the encryption of hard-drives and moveable storage etc., it is recommended that congregations password protect word and excel documents that contain sensitive personal data.

The password protection feature for documents built into the Microsoft Office Suite 2007 (and newer) is sufficient to protect documents but, where possible, additional measures should be used (such as the use of encrypted storage).

Encrypted USB drives

Most manufactures offer an encrypted version USB stick at relatively low cost.

Manual/Paper File Storage

The GDPR must not be used as an excuse to stop storing paper records! However, do bear in mind that lockable storage is appropriate for most congregational records - and the key should not be left in the cabinet!

Where possible, past Board/Session minutes should not be being stored in an Elder's home/loft. Not only is this creating an additional data protection burden on them, there could be a significant fire risk and also the possibility of the whereabouts of the records being forgotten over time. Such documents should be in lockable fire retardant storage in the church office/vestry. Do bear in mind once minutes and other records of future historical interest are more than 50 years old, they should be transmitted on to the Principal Clerk's department. They will then be passed to the National Archives and released after approximately 100 years for research purposes.

Summary

Congregations should assess which devices they have that ought to be encrypted. Indeed, for small quantities of personal data, it may be that using password protection and encrypted USB drives is adequate from a security point of view. However, if USB drives alone are being used, bear in mind that they are small, easily mislaid and therefore a back-up on an encrypted device ought to be made. Also, do remember to store manual records securely.