St Andrew's

United Reformed Church, Cheam

To know Christ and to make Christ known

Data protection policy

1 Introduction

St Andrew's and various of its officers will necessarily hold information or data which is in some sense 'sensitive' and particular information about individuals. The church and any of those holding such data have a legal duty to protect it. In some cases, the loss of such information could lead to a criminal penalty if it was held to have been insufficiently protected.

It is therefore essential that all St Andrew's staff and volunteers who may handle such data read, understand and adhere to this policy. If you have any questions as to how it applies to you, you should raise this with the church's Data Protection Officer or the Church Secretary.

2 What is sensitive data?

2.1 Personally identifiable data

The UK Data Protection Act (DPA) covers data or information which relates to and can be identified as relating to particular living individuals. This includes addresses, phone numbers, email addresses, dates of birth, salaries and so on as well as less structured information such as employment records or medical records. In the church context, membership data and data relating to baptisms, marriages and funerals is also covered.

Data which is part of the public record is not sensitive. This includes the contents of probated wills or anything which has been legally made publicly available.

The DPA has two main provisions. The first lays down eight principles, which state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

The second provision says that the person to which data relates must be given a copy of the data on request and given a chance to correct anything which is wrong.

The DPA is administered by the Information Commissioner's Office (ICO), and there is a great deal more information on the ICO's website: http://www.ico.gov.uk/.

The ICO offers a checklist for those handling personal data. The following is an extract:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?

2.2 Other data

Other data may also be sensitive, for example for commercial reasons. This will not often impact the church, but we should be aware, for example, that quotations or plans provided by suppliers may be subject to their copyright and should be given reasonable protection.

2.3 Who can hold it?

The simple answer is 'those who have a need to know.' This could be extended to add 'at times and in places where they have that need.'

Sensitive data should not be removed from a place of security unless there is a specific need, so for example, youth leaders may need to carry medical information about young people if they are accompanying an outing, but if practical should not carry it at other times.

3 How do we protect it?

3.1 How securely must it be protected?

The degree of security applied to data is related to its sensitivity. For example, lists of names and addresses are less sensitive than medical or other personal data. A useful question to ask is 'what damage or distress would be caused to the individual if the data fell into the wrong hands?'

Even names, addresses and phone numbers – for example the church membership list – are personal data under the DPA and it is not legal for them to be made available to anyone unless the persons whose names and addresses are listed have given their permission. However, it is not expected that such lists will be held as securely as more sensitive data: for example, it would be reasonable for the Minister or office bearers to carry such a list in an ordinary briefcase.

Permission does not necessarily have to be given explicitly for each disclosure; for example permission to list a person's name in the church directory implies disclosure of the

directory in the normal course of the church's activities – but not, for example, the sale of the directory to a commercial enterprise unless that was made clear at the outset.

3.2 Information held on computers

In general, desktop computers held in rooms or homes that are normally locked when unoccupied are regarded as sufficiently protected against loss of moderately sensitive data provided normal precautions are taken. This includes using a secure password (for example not a word found in a dictionary) for logging on, connecting to the internet with proper security (see below) and turning the machine off when not in use.

Note however that a log-on password for Microsoft Windows only provides weak protection; a knowledgeable computer technician can easily bypass it.

Laptop computers and removable media such as CDs and memory sticks are clearly much more vulnerable to loss, and this policy requires that sensitive data on all such devices must be encrypted, using a secure encryption key. Secure means that the key must not be a dictionary word or an easily guessable phrase, and that it must not be written down where it might reasonably be at risk of theft along with the media concerned.

There are various tools which provide encryption and the Data Protection officer will be happy to advise, but for many purposes the 'Encrypt Files' package, which is free for personal use, will be adequate: see http://www.encryptfiles.net/. Note however that encryption is not an automatic process: files must be explicitly encrypted, then decrypted to use them and re-encrypted once they are no longer in use.

There is of course no harm in encrypting data on desktop computers too.

Please remember that backups of sensitive data need to be protected as securely as the original. Again, encryption is a good solution, and backups on removable media should be locked up.

Lastly, security can be too good. People do forget passwords or encryption keys, and people who know the password are sometimes unavailable when the data is needed. Please ensure that for any information that is protected with a password, at least two people have access to the password.

3.3 Email and the internet

The internet must be regarded as insecure unless precautions are taken.

Sensitive data as described above should only be sent by email if it is password protected, or preferably encrypted. The password or key should be communicated by another means, eg telephone.

Sensitive data should preferably not be held on websites but if it is, should use secure authentication and encryption such as SSH (ie the https protocol).

Any computer containing sensitive information which is connected to the internet should normally be behind a router such that its address is not directly exposed to the internet. Routers must have the configuration screen password changed from the default. Wi-fi networks must use WPA authentication (or better), and the password for the configuration

screen of the access point must be changed from the default. The Data Protection Officer will be happy to advise you if you are in doubt on any of these matters.

3.4 Information held on paper

The DPA also covers most personal data held on paper. Information of low sensitivity must be held in a room or home which is normally locked when unoccupied, and information which is more sensitive must be held in a locked cabinet with keys held only by those with a need to access it.

3.5 Destruction

Information no longer required must be securely disposed of.

The Encrypt Files package mentioned above has the ability to 'shred' computer files so that they are effectively unreadable, and that should be used to destroy entire files.

Surplus CDs should be physically damaged, eg cut or broken in half.

Redundant computers should preferably have their hard disks wiped clean. This can often be achieved by using the feature to allow a complete reinstallation of the operating system. The Data Protection Officer can advise on other means (which are often faster)..

Computers which no longer work pose an interesting challenge, but removing the hard disk and damaging it severely with a hammer will usually suffice. This can also be applied to non-functioning memory keys.

Sensitive paper records should be shredded, preferably using a cross-cut shredder.

4 Incidents

4.1 Reporting

Any loss or theft of sensitive data should be reported as soon as possible to the Minister or the Church Secretary. If the loss resulted from criminal action the police should be informed and a crime number obtained.

The Church Secretary will maintain a register of incidents and will determine what action needs to be taken. This will normally include informing anyone affected by the loss, and making an assessment as to how any similar future loss can be prevented.

December 2009