The Church of Scotland Presbytery of Glasgow ("the Presbytery")
Data security breach management policy

This policy covers all congregations within the Presbytery.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

If it appears that a data security breach has occurred, a report must immediately be made to the Presbytery Clerk. The following breach management plan will then be implemented.

1. **Containment and recovery**

1.1 The Presbytery Clerk as Data Protection Compliance Officer will take the lead in responding to the breach, and in investigating the nature and cause of the breach and the extent of the harm that could result. He or she may elect to carry out all necessary investigation him or herself or alternatively may appoint someone else to do so. As a first step, the Clerk will establish who needs to be made aware of the breach and will inform them of what they are expected to do to assist in the containment exercise. This could be, for example, finding a lost document or piece of equipment.

1.2 Steps will be taken to establish whether there is anything which can be done to recover any losses and limit the potential damage arising from the breach. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that people recognise when someone tries to use stolen data to access accounts.

1.3 The Clerk will determine the identity of the data controller for the purposes of the breach, bearing in mind that there may be more than one data controller where shared services are involved. If it appears that the breach has been caused by another data controller, or by the data processor, the terms of the contract with that third party will be checked with a view to determining whether a claim may lie for breach of a specific obligation, breach of confidence or a failure to take reasonable skill and care; and whether the breach gives rise to a right to terminate the contract.

1.4 An immediate report of the breach must be made by the Clerk to the Solicitor of the Church.

1.5 Consideration should be given to whether or not it is appropriate to inform the police.

2. Assessing the risks

2.1 Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Before deciding on what steps are necessary beyond immediate containment, the Clerk will assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

2.2 The following points will be borne in mind when making this assessment:

- What type of data is involved?
- How sensitive is it? Some data is sensitive because of its very personal nature (e.g. information about health) while other data is sensitive because of what might happen if it is misused (e.g. bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the biggest risks will accrue from the loss of large amounts of data but this is an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, volunteers or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, the appropriate actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a loss of public confidence or reputation?
- If individuals' bank details have been lost, the banks themselves could be contacted for advice on anything they can do to help prevent fraudulent use.

3. Notification of breaches

3.1 Informing people and organisations of the data security breach can be an important element in a breach management strategy, but this is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

3.2 All decisions on notification will be taken by the Solicitor of the Church, in discussion with the Clerk. The Solicitor will be responsible for notifiying the Information Commissioner's Office ("ICO") where this is appropriate. The Clerk will be responsible for notifying affected individuals, where appropriate.

3.2 If it is likely that there will be a risk to people's rights and freedoms, the breach must be reported to the ICO. If such a risk is unlikely then it does not have to be reported. If a decision is taken not to report the breach, this decision and the reasons for it must be documented. Notifiable breaches must be reported to the ICO without undue delay, but **not later than 72 hours** after we become aware of it. If we take longer than this, we must give reasons for the delay.

3.3 If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be informed without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means that the threshold for informing individuals is higher than for notifying the ICO. It will be necessary to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, the risk is higher. In such cases, we must promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them.

3.4 The following considerations will be taken into account in assessing the likelihood and severity of the risks and deciding whether to notify:

- The type of breach
- The nature, sensitivity and volume of the data involved
- Ease of identification of individuals
- Severity of consequences
- The number of affected individuals
- Are there any legal or contractual requirements to do so, for example if a regulatory body is involved (is a report of a serious incident to OSCR required?)

- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act so as to mitigate risks, for example by cancelling a credit card or changing a password?
- Special characteristics of the individual
- How notification can be made appropriate for particular groups of individuals, for example vulnerable adults
- Is there a danger of 'over notifying'? Not every incident will warrant notification and notifying a large number of people about an issue affecting only a small number may well cause disproportionate enquiries and work

3.5 Bear in mind that it may also be appropriate to notify insurers of potential claims.

3.6 Consideration will also be given to what should be said to any person or body to whom notification is made, and how that message is to be communicated. This will depend to a large extent on the nature of the breach but the following points will be taken into account:

- There are a number of different ways to notify those affected. The most appropriate one will be used, bearing in mind the security of the medium as well as the urgency of the situation
- Notification will include a description of how and when the breach occurred; what data was involved; and what has already been done to respond to the risks posed by the breach
- When notifying individuals specific and clear advice will be given on the steps they can take to protect themselves and also what the Church is willing to do to help them
- Information will be provided about how individuals can obtain further information or ask questions about what has occurred

4. Evaluation and response

4.1 It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the Presbytery's response to it. If it is established that existing procedures could lead to another breach, improvements to those procedures will be identified. Questions to be asked will include:-

- Was the data protection policy, and in particular its security provisions, followed?

- Does action need to be taken to raise security compliance standards?
- What are the weak points in existing security measures?
- Should disciplinary steps be taken against any staff members?

- Have adequate training and guidance been provided?
- Are adequate contractual safeguards in place?
- Where do the biggest risks lie? Risks will arise when sharing data with or disclosing to others. Are the methods of transmission secure? Is only the minimum amount of data necessary being disclosed or shared?

5. Recording breaches

5.1 All breaches must be recorded, regardless of whether or not they need to be reported to the ICO.

5.2 The facts relating to the breach, its effects and the remedial action taken must all be recorded. Consideration should be given to whether or not the breach was a result of human error or a systemic issue and how a recurrence might be prevented, whether through better processes, further training or other corrective steps.

March 2018