Second Presbyterian Church Comber

DATA BREACH POLICY

Second Presbyterian Church Comber is committed to complying with data protection legislation and will take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of or damage to personal data:

If, despite the technical and organisational measures that we have put in place to protect personal data, a data security breach occurs, it is important to manage and respond to it effectively. A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

- Loss or theft of data or equipment.
- People gaining inappropriate access.
- A deliberate attack on systems.
- Equipment failure.
- Human error.
- Catastrophic events, (for example, fire or flood).
- Malicious acts such as hacking, viruses or deception.

If such an incident occurs it is imperative that we act immediately. The following steps will be taken:

A. Minister, Data Protection Lead, Clerk of Session and Congregational Committee Secretary (the "Security Breach Team") will be informed immediately;

B. An investigation will be undertaken to determine:
   i. The nature and cause of the breach; and
   ii. The extent and nature of harm that has or could arise from the breach.

If there is no risk of harm then no further action is required (for example if papers are temporarily lost due to being incorrectly filed but are then promptly found and no disclosure has occurred or harm likely to occur then no further action is required).

If there is considered to be a risk of harm then the following steps must be undertaken:

1. Information Commissioner's Office must be informed within 72 hours. If we do not have all of the information by then a report should be made within the 72 hours on the basis of what is known while investigations continue.
2. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay. Examples of this could include where there is a high risk of reputational damage, embarrassment or putting the individual's property at risk.
3. If necessary a number of third parties will be informed which may include:
   a. PCI
   b. the Organisation's insurers;
   c. the police;

d. the Congregation's solicitors.

4. Following notification we will continue to liaise and cooperate with ICO.
5. All reasonable steps to mitigate the damage arising from the breach will be taken.

A record of all data protection breaches will be maintained regardless of whether or not notification is required. Detailed records of the investigation will be maintained as well.

Following a breach if necessary it must be considered whether any of the below is required:

- Disciplinary action;
- Legal action;
- Internal review of security procedures.