Storage of data both physical and digital

I realise that since the Safeguarding Review in July 2019 and during the Advanced Safeguarding training that I have presented since then I have given advice and direction surrounding the use of Fireproof Boxes and storage of data. I thought that I would take this opportunity to clarify the position that should be taken –

Fireproof Document Boxes

In policy it provides guidance that fireproof filing cabinet/box should be used to store safeguarding documents. I realise that there may be controversy over the cost of purchasing these and how long the resistance to fire should be. There is no specification provided in policy/guidance just that it should be fireproof.

Based on policy and best practice adopted in other districts, I would now like to give clear direction/guidance to all circuits within the district, each church should have a small box/cabinet that is fireproof. The minister with pastoral charge and the church safeguarding officer should have a key each. This box/cabinet should be kept in the church rather than in the home /manse. (I realise that in some circuits the box/cabinet may have to be shared between churches, for a practical purpose, given that safeguarding officers/ministers may hold responsibility for more than one church).

The Church safe should not be used as others may have access to it and it is most likely to be stolen if there is a burglary.

To avoid the cost involved in the purchase of fireproof boxes/cabinets and the fact that we are in a digital age and ever more moving that way the following is advice/guidance around the storage of digital material which I have sought from the data security expert in the Connexional Team -

Storage of Digital Material

The following measures should be put be in place if material containing special category or criminal data is retained:

- *Access provision should be carefully planned*

  Only those that are required to see and use records should have access to them. A written protocol listing who has access should be drawn up with clear provision for emergency access. Data held on personally owned computers can be lost if unforeseen personal circumstances arise. This should never be the sole source of safeguarding records.

- *Digital files should be subject to regular back-up.*

If the data is stored on a stand-alone computer. The provisions for back-up should be away from this source to ensure that there is another copy if hardware is lost or corrupted beyond recovery. A secure server is the best option for back-up, where available but again access to safeguarding files should be limited to personnel listed in the access protocol.

· *Pen drives or removable media must be encrypted if they are being used to store safeguarding records. However, the risks of loss of such items are higher than less mobile storage so great care should be taken in use.*

· *Software which identifies viruses, malware and phishing must be installed on systems storing safeguarding records. It must be regularly updated and the provision must include a regular scanning facility.*

· *Hard copy material must be stored in lockable cupboards or cabinets. Where available, these should be fire-proof.*

· *If material is scanned for digital retention, care should be taken to ensure that all parts of the document are contained in the scan, particularly the edges of documents. It is important to retain the integrity of the document, in case it is needed for proceedings at a later date.*

· *If plans are made for archiving safeguarding material with another institution, that organisation must be informed of the Methodist Church's requirements relating to retention of safeguarding records to ensure that records are not destroyed in error at a later date.*

· *Passwords must not include personal data which is easily identifiable e.g. a name, address, place or date of birth. Choosing 3 random words for a password can be easily remembered by visualisation of the items together and will create an appropriately secure password. This can be enhanced further by using a capital letter, number and symbol.*

I hope that this adds some clarity in this issue and will permit circuits to find a cost effective way in addressing the issues around the storage of documents/data.

David Cross

Safeguarding Officer