Miscellaneous A-Z (this document is being continually revised! Last edit: 15-Mar-18)

- **Annual Reports** – if the custom on your circuit has been to print names with addresses, birthdays, phone numbers and/or financial giving, you must have explicit written consent to continue doing so. You should consider anonymising any giving details (for example by using FWO envelope numbers) to ensure such sensitive information isn't discovered by non-members.
- **CCTV** – if you use CCTV you must be registered with the Commissioner and have a policy in place regarding how long images are kept, with whom they might be shared, etc.
- **Cloud Sharing** – all of the 'big' cloud services (eg Amazon, Apple, Box, BT, Dropbox, Google, Microsoft...) hold your data on servers either in the EU or a country with adequate protection and security protocols. If the personal data you hold is backed-up or synchronised to the cloud please check with your provider to ensure their standards match the EU's 'GDPR' requirements. It is probably safer when you need to share personal data electronically, to do it using the cloud rather than e-mail. *Ministers, staff and circuit officials with MCI Office365 accounts should always use the MCI Onedrive, Sharepoint and other services for added security.*
- **Computers** – should always be password-protected, and locked when stepping away from them; laptops in particular should be stored in the boot of a car when travelling or parked.
- **Consent Expiry** – you need to decide how long the consent you have recorded will last; eg if you don't hear from or see a person for five years, have they effectively withdrawn their consent to be contacted? This presumes that you have either an electronic or paper record of consent to begin with – so keep these carefully!
- **Cradle Roll** – if your church displays a cradle roll poster that contains the full name and date of birth for children you should move it to somewhere that only members can view it, eg vestry or a Sunday School room.
- **Data Controllers** – as the Methodist Church in Ireland does not employ someone as a Data Protection Officer, who can actively ensure that individual societies are following their data protection policies, we consider the Data Controller to be at Circuit level. Therefore it is the responsibility of Circuit Executives to maintain policy and train data processors.
- **E-mail Accounts** – Methodist ministers and staff should avoid using joint e-mail accounts with family members, and where available should use a full 'IrishMethodist.org' Office365 account; keeping personal and sensitive information within the Methodist Church in Ireland's e-mail and folder system reduces the risk of an unauthorised person accessing it.
- **E-mails to multiple recipients** – always use the 'BCC' option for a list of e-mail addresses when sending to many people who aren't engaging in a conversation; to do otherwise reveals the addresses of people to everyone else.
- **First Contact** – often 'first contact' between minister/lay pastor and new members of a church involves the staff member (for want of a better word) saying, "Can I have your number and address so we can stay in touch?" As long as those details are kept distinct, separate from other lists (for instance as a contact in their mobile phone address book, or a standalone note), data protection rules don't yet apply. However, once pastoral care is being offered and their details are included in the congregational list or membership register, explicit consent to process those details is required.
- **Leaders** – when a member of the church becomes a leader they will need to be given a privacy notice that explains how their contact details might be used, such as being published on the church website or in the announcement sheet/annual report, *or passed on to Connexional leaders*. Once they leave office the publication of those details should stop.
- **Legitimate Interests** – a case can certainly be made for the use of legitimate interests as the legal basis for processing data (rather than consent), but there are more strict rules around sensitive data and children's information. Any church or department preferring to not use Consent for some purposes will need to have a

written 'Legitimate Interests Assessment' showing why they selected this route – asking if the use is genuine? necessary? invasive?; the need for transparency remains, so privacy notices are especially important.

- **Mailing Lists** – when members or congregational list people give their details to the church, the privacy notice on the form should specify that the church will keep in touch by post, e-mail and phone to keep them informed about the congregation's life together and the causes they support (eg Connexional appeals).
- **Memory Sticks** – are particularly vulnerable to being mislaid or stolen; ensure any sensitive documents, or the entire pen-drive, are encrypted. At time of writing, a 4GB encrypted USB drive (where you set a password at first use) costs ~£7 (eg http://bit.ly/encryptedUSB4).
- **Pastoral Notes** – the notes made about an individual by a person with pastoral responsibility, whether or not they are employed, come under the Data Protection rules. They must therefore be made available to that individual should they ask to see them, and facts corrected or deleted if requested. NB – an *opinion* can't be amended or deleted, but an individual could object if the opinion was based on inadequate or incorrect information. Therefore pastoral notes about a person must include information about the person whose opinion it is, the circumstances it is based on, and any evidence to support the outcome of the opinion. Such notes must be checked periodically to ensure information about an individual is accurate.
- **Passwords** – three or more random words joined together makes a password that's easier for you to remember but long enough to make cracking it extremely complex (eg bluelasagnestars).
- **Personal Data** – is defined as information that relates to a living individual who can be identified by that data, including opinions about them. *Sensitive* personal data needs to be treated even more carefully, and includes: the racial or ethnic origin of the data subject, their political opinions, their religious beliefs, membership of a trade union, their physical or mental health, their sexual life, and anything related to the commission or alleged commission by them of any offence.
- **Phones and Tablets** – ensure these portable devices are locked with a pin/password/etc if they could allow access to other people's data (eg a cloud backup app, e-mail app). Be aware of 'find my device' services built-in to the operating system that can both locate and erase content if necessary, eg Apple's Find My iPhone [www.icloud.com/find] and Android's Find My Device [www.android.com/find].
- **Prayer Chains** – you cannot transmit personal data to a group of people via text message, e-mail or other messaging service without the subject's permission; therefore it is key to get consent for such activity. However, verbal consent is enough as long as you record that you have received such consent, e.g. "Michael, is it ok if I send a message to our folks asking them to pray for your sick wife?" – then send the message along the lines of, "Michael has asked us to pray for..." or "Michael has given me permission to inform you that..."
- **Public Viewing of Registers** – some churches are known to put their marriage and/or baptismal registers on public display during special anniversaries. If the records relate to people who are still alive, information including a woman's date of birth, home town and maiden name could be easily photographed and misused for identity fraud or account hacking. Instead, why not consider a redacted list that could be put on display, with names of couples married and the year in which it happened?
- **Registration with the Information Commissioner's Office (NI) or the Data Protection Commissioner (RoI)** – the previous system of 'notifying' the ICO that you are a Data Processor lapses on 31 March 2018. From 1 April, all data processors must pay a fee to ICO unless exempt: we understand that churches will be in the exempt category. The situation in RoI will be clarified soon. Whether or not you pay a fee you must still comply with GDPR.
- **Software** – any software, spreadsheet or document containing personal data must be password-protected or encrypted.
- **Websites and Social Media** – contact details, images and video of church members should only be published online if express consent is given.
- **Wi-Fi** – your home and/or office router should have a secure password, as individuals who can guess it could potentially gain access to your computer's documents.