Establishing Good Data Protection Practice in Your Church Checklist[1]

REMEMBER - Data Protection legislation applies to both paper and electronic records and includes photos and videos as well as documents.

1. Confirm who is the Data Controller for your church. In most cases this is likely to be the eldership.
2. Make sure that the Data Controller(s) understands what constitutes personal data. (Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession.)
3. Make sure that the Data Controller(s) understand what constitutes SPECIAL CATEGORY (sensitive) personal data (ie data which contains information about: racial/ethnic origin; political opinions; religious or philosophical beliefs; TU membership; genetic/biometric for identification; health; sex life and sexual orientation. Special Category data can only be processed with explicit consent.
4. Compile a full list of all the types of personal data the Church collects and holds.
5. For each type of information determine where and how it Is held.
6. Ensure that the data is held securely. Take steps to ensure that personal data is not disclosed to others without that person's permission — this includes: birthdays; addresses; telephone numbers; email addresses; matters relating a person's health.
7. For each type of information determine how long it should be held and be able to justify your decisions.
8. Dispose securely of any data which is no longer useful.
9. For each type of information establish a routine for the permanent and secure disposal of time-expired data.
10. Determine who will deal with Subject Access Requests (SAR). Usually the Church Secretary.
11. Make sure that the Church Secretary or other relevant person(s) know that there is a statutory limit (30 days) within which to comply with a Subject Access Request.
12. Complete and publish your church's Privacy Statement.
13. Make sure that the Privacy Statement is posted in a prominent position and that members, friends and adherents are aware of its existence and that copies are available for them to take away.
14. Bring the Privacy Statement to the notice of members at a Church Meeting and review regularly its effectiveness - suggest at Annual Church Meeting.
15. Monitor, review and amend as necessary.

[1] The United Reformed Church, GDPR Checklist vi —1 February 2018

NSPCI Data Protection Policy 2018

The General Data Protection Regulation (GDPR) takes effect across Europe from 25 May 2018. It replaces the existing law on data protection and gives individuals more rights and protection in how their personal data is used by organisations.

There must be a valid lawful basis in order to process personal data. There are six available lawful bases for processing. Which basis is most appropriate will depend on your purpose and relationship with the individual. The majority of data held by the Denomination should be held under the basis of consent, such as a permission slip for photography during youth activities, or legal obligation, e.g a safeguarding referral.

Personal data is information about a living person which is capable of identifying them. This that includes, address, telephone number, email address, age, birthday, names of family members.

The Information Commissioner's Office (ICO) provides for special conditions for not for profit organisations. This includes an exemption from registering with the ICO where data is processed only for the purposes of: establishing or maintaining membership; supporting a not-for-profit body or association; or providing or administering activities for either the members or those who have regular contact with it. The information must not be kept after the relationship between the individual and the organisation ends, unless it is necessary for the purposes described above.

Sensitive personal data can only be processed with explicit consent. This includes data contains information about: racial/ethnic origin; political opinions; religious or philosophical beliefs; TU membership; genetic/biometric for identification; health; sex life and sexual orientation.

Where gathering information regarding health, including allergies or medical conditions, you should always seek explicit permission.

Where information is held in electronic form it may be necessary to register with the ICO. Where data is held in hard copy this is not necessary. All data must be held securely in a locked cupboard to which there is no general access.

The basic premise of the GDPR is that people are entitled to know what data is being held by organisations, for what purpose and how long. Where organisations hold data they should make clear how they intend to store, manage and use this. This can be covered in a short sentence on a permission slip seeking permission to photograph.

Personal data should not be shared without consent however if you are keeping records for child protection reasons, you don't necessarily need to get consent from the adults and/or children concerned. More information is available from the NSPCC at https://safeguardingtool.nspcc.org.uk/documents/171/Child_protection_records_retention_and_storage.pdf. If you are in doubt as to whether you need to inform a child or adult that

data has been shared after a concern is raised you should make the referral first and discuss notification with the agency you are dealing with e.g Police or social services.

Congregations should appoint a Data Controller who will record what type of information is held by the Congregation and ensure it is used only for the exempted purposes above. This should not be an onerous role and can be shared by more than one person.

Under GDPR a person has the right to ask organisations to set out what information they hold about them. Congregations should decide who will deal with Subject Access Requests (SAR). There is a statutory limit (30 days) within which to comply with a Subject Access Request. When a request is received the Congregation should respond setting out what information they hold and for what purpose.

Further information on the GDPR can be found on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Hints and Tips — Good Data Protection Practice[2]

- Respect everyone's privacy.
- Data should only be used and stored electronically for Church matters, administration and the specific purpose the information was collected for: not shared without permission outside the Church.
- Ensure that paper records are kept in a locked cupboard.
- Do not disclose any personal information about an individual without first obtaining that person's consent—that includes, address, telephone number, email address, age, birthday, names of family members.'
- Consider data security when sending e-mails regarding Church matters from a personal e-mail address. You may wish to set up a congregational or office bearer email addresses using a provider like Gmail e.g. ***secretary.congregation@gmail.com*** or ***congregation.nspci@gmail.com***
- When emailing groups of people always put their email addresses In the 'bcc' row rather than the 'To' row. This prevents an individual's email address being visible to all the recipients
- If you are sharing birthday information (age or date) about an individual with others always ask for the individual's permission first. Ideally this should be in writing.
- When mentioning pastoral concerns or praying for identifiable individuals take reasonable steps to ensure that the individual (and anyone else who may be directly or indirectly involved) is willing for this to happen.
- When minuting pastoral concerns, refrain from mentioning names and the nature of the concern.
- Prayer lists should be confidentially destroyed immediately after they have been used.

---

[2] Based on information produced by United Reformed Church, Hints and tips Good Data Protection Practice vl - I February 2015

- Personal data held on laptops, data sticks and other portable electronic devices should be encrypted. If data is held in electronic form then the Congregation may need to register with the ICO.
- If using cloud storage ensure that the servers are located within the European Economic Area (PEA) and take reasonable steps to ensure security.
- When collecting an e-mail always ask for consent from the owner of the e-mail: do not assume consent if the e-mail address is supplied by a third party. e.g "*These e-mail addresses will only be used for issues related to Congregation for purpose of …… This information will not be shared with third parties. Should you wish to remove your email address from this list please let us know*"
- Order your records —minimise what you keep.
- Check that existing and former officers/elders/committee members are not retaining their own copies of personal data in paper form or electronically. Seek their confirmation that all such data has been returned or destroyed.

Sample forms of words

1. Photography

Dear Parent/Carer

During the course of the year, we may sometimes wish to take photographs or video recordings of children within this group or on trips, either for our own records, for use as part of our learning, for inclusion in Denominational publications or for inclusion on our website. Children may also be photographed when attending events or activities organised by the Sunday School and Youth Committee of the NSPCI.

To comply with the Data Protection Act 1998 and the new General Data Protection Regulation (May 2018), we need to ask your permission to do this. In view of this, please read the Statement below and complete and return this form by_____**.**

> We may use your child's photograph in congregational or denominational publications.
> We may use your child's image on our website.
> We may record your child's image on video.
> These recordings or photographs may be used as part of Sunday School learning and work and entered into Sunday School exams.
> Your child's image may appear in the media.
> Your child's first name may appear with the image in the media.

I/We **do/do not*** give consent (please sign) .....
*delete as applicable
Relationship to child …….

Address ……..

……..

Telephone number ……..

Date ……

2. Health/Allergies

Dear Parent/Carer

At the start of each year we wish to ensure that we are aware of any allergy or medical issues which affect those children and young people with whom we work. This information will be held securely for the sole purpose of ensuring we are aware of any risks to the children and young people we engage with.

To comply with the Data Protection Act 1998 and the new General Data Protection Regulation (May 2018), we need to ask your permission to do this.

Please complete and return this form informing us of any medical issues which you think we should be aware of by_____**.**

I/We **do/do not*** give consent (please sign) .....
*delete as applicable

Relationship to child …….

Details of allergies or medical conditions……..……..

……

……

Address ……..

……..

Telephone number ……..

Date ……

3. Contact details

We hold contact details of our members and those we have regular contact with in order to establish and maintain membership; support our work and to provide or administer activities.

To comply with the Data Protection Act 1998 and the new General Data Protection Regulation (May 2018), we need to ask your permission to do this. These contact details will only be used for issues set out above.

Should you no longer wish to be contacted by us please let us know and we will remove your data from our records.

I **do/do not*** give consent (please sign) .....
*delete as applicable

Email/Address ……..

……..

Telephone number ……..

Date ……