GDPR Principles

As a church, we come within the definition of *'data controller'*. As such, the Regulations are clear that good documentation is essential to demonstrate compliance with the principles embodies in the Regulations. But this does not have to be onerous. In fact, if we make it onerous, people won't do it! So the church has worked hard to ensure that the following principles are applied while, at the same time, doing so in a manner that church workers will find straight forward. However, perhaps it is right at this point to be clear. If we ask you collect and store data in a particular way, it is for a very good reason. Please do as we request – it is not your gift to do just as you please!

1. *Personal data must be processed lawfully, fairly and transparently.*

2. *Personal data can only be collected for specified, explicit and legitimate purposes.*

3. *Personal data must be adequate, relevant and limited to what is necessary for processing.*

4. *Personal data must be accurate and kept up to date.*

5. *Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.*

6. *Personal data must be processed in a manner that ensures its security.*

Individual Rights

We live in times where people are very quick to tell us that “they know their rights”. As far as data handling is concerned there are eight individual rights, although only six are likely to apply to the church.

1. The Right to be Informed

Everyone who uses the church has a right to know how we handle personal data.

Procedure – Privacy Notice is displayed on an internal notice boards, as well as on our website.

2. The Right of Access

Everyone who uses the church has a right to see whatever data we hold on them.

Procedure – if the data is available, the activity leader should act immediately and take the individual to a quiet corner, where the data can be disclosed. If the data is not available, an appointment should be made for the individual to return to view the data.

3. The Right to Rectification

Everyone who uses the church has a right to have inaccuracies rectified.

Procedure – when in accuracy is identified, the details must be recorded and passed to Church Data Manager (CDM) who will: a) ensure all records are amended and b) confirm that fact to the data subject.

4. The Right to Erasure/The Right to be Forgotten

Everyone who uses the church has a right to ask that their personal data be erased from church records. Where there is no compelling reason not to do so, we will comply with the request.

Procedure – because a number of tests have to be applied before we can grant the request, details should be passed to CDM who will:
a) assess if request can be followed b) if 'yes' will ensure data is erased c) will confirm erasure or otherwise to the data subject.

5. The Right to Restrict Processing

Everyone who uses the church has a right to ask that, other than storing it, we don't use their personal data.

Procedure – This request needs to be handled by CDM as we would wish to use personal data in an emergency. CDM will contact the data subject to discuss the matter further and agree an outcome.

6. The Right to Data Portability

This is unlikely to ever apply to the church.

7. The Right to Object

Everyone who uses the church has a right to object to us collecting their personal data.

Procedure – Such objection should be handled initially by the activity leader and, if the objection still continues, should be escalated to CDM. The CDM will meet with the data subject and agree a way forward.

8. Rights in Relation to Automated Decision Making

This is unlikely to ever apply to the church.

Collecting Personal Data

The church collects personal data from those attending activities of the church so that we can function effectively. In the words of GDPR, we are collecting data for the purposes of “legitimate interests pursued by the church”. Because this is the *lawful basis* under which we collect data, there is no need to obtain specific consent, which means we don’t need another form! However, we still need to be able to tell everyone where and how we will use their data so it is important that the Privacy Policy notice is prominently displayed in the church.

At Latimer Church, we presently collect data as follows:

For the purpose of claiming Gift Aid
o The treasurer will arrange for forms to be signed as appropriate.
o The treasurer will keep the forms in a secure place in his/her home.
o The treasurer will keep details of donations on a password protected computer, stored in his/her home.
o After the donor stops making gifts under the scheme, the church will keep personal data for as long as required by HMRC. Then it will be deleted.

For the purpose of running church activities efficiently (such as Holiday at Home or Toddler group and other children’s work)

o Contact details of attender, or child and parent/carer will be taken at first attendance.
o Contact details will be checked each year.
o Contact details and register of attendance will stored in a secure place in the church.

o Contact details will be archived, for insurance purposes, when a child stops attending.

For the purpose of maintaining the Church Directory

o The responsible person will request contact details from members or regular worshippers.

o An updated version will be issued annually.
o Copies of the Directory will not be kept in church but they can be requested from the responsible person.
o Electronic data used to publish this Directory will be stored on a password protected computer in the home of the responsible person. For contacting members/visitors

o Church officers will keep contact information on password protected computers in their home and/or on password protected mobile devices.

Dealing with a Breach

What is a personal data breach?
ICO define it as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.

Now this could be something that occurs accidentally, like leaving sensitive documents in a taxi, or something that occurs deliberately, like hacking into a computer.

In the church, it is highly unlikely that we would hold data that is particularly sensitive but, using ICO’s definition, *any* data breach is serious. As such all data breaches within the church must be reported to CDM as soon as you are aware of the breach.

The CDM, in conjunction with the Pastor, will determine how to deal with the breach and, will, if appropriate report the breach to ICO.

https://ico.org.uk/for-organisations/report-a-breach/

November 2018