GDPR Update from the Diocesan Registrar

After years of waiting, the GDPR finally came into effect on 25 May 2018.
In our last Newsletter we mentioned the Church of England's National Stewardship and Resources guidance which suggested that parishes ought to prepare for GDPR by:

- gathering consent for marketing or fundraising communications;
- looking into and understand the new data processing condition available under the GDPR for internal church management. This allows religious (and other) bodies to process data without specific consent as long as it relates only to members or former members and provided there is no disclosure to a third party without consent; and
- developing a privacy notice and ensure they have procedures in place to manage requests from people about their personal data under the GDPR.

Once these are comfortably in hand, we suggest parishes consider the new requirements for demonstrating accountability as a data controller. If not already completed, parishes are well advised to complete a data mapping exercise which records the following information:

- Categories of data subjects the parish has; (for example, congregation members, those who hire the facilities, attendees of Sunday school);
- What types of personal data the parish holds about those data subjects (for example name, dates of birth, address, email address etc)
- Where this information has come from (for example, provided by the individual or a third party for example a booking website)
- All the purposes the parish uses this personal data for (for example, to send email invitations and reminders to parish events)
- Which person within the parish is responsible for this data (for example the chair of the PCC. Please note that we strongly advise that one person is identified with the overall responsibility of ensuring compliance with the GDPR)
- Who has access to the personal data and how access is controlled (for example, the chair has access and shares on a need to know basis with others when necessary);
- How long the data is kept for;
- What security measures are in place to keep it safe (for example, locked cabinets, encryption);
- Whether it will be transferred out of the European Economic Area (unlikely unless you are using cloud storage);
- Which lawful basis you are relying on to process the data (there are 6 under GDPR).

Data Controllers must be able to show that they comply with the GDPR principles by providing evidence. For example, where you process on the basis of consent, you should document how consent was given.