Retention and Storage of Records and Data

In common with most organisations, parishes need to keep records in order to provide an efficient and effective service in safeguarding vulnerable people. All parishes involved in child and adult protection work have a duty under the Data Protection Act 1998 to:

- Keep information about individuals confidential and in a secure place
- Keep information for specific legal purposes
- Ensure that the information is accurate and up-to-date
- Keep information for no longer than required for legal purposes

Records include all information held either electronically (including e-mail correspondence) or in paper format, which include ‘sensitive personal data’ about an individual.

What counts as ‘Sensitive Personal Data’?

The following may be counted as sensitive personal data, but the list is not exhaustive;

- Personal details (home address, phone number, date of birth, health needs, including that stored on parish databases, and on registration forms for activities)
- Recruitment information for paid or voluntary workers (application forms, references)
- Criminal Record details (Confidential Declaration forms, outcomes of DBS disclosures)
- Employment information for paid and voluntary posts (contracts of employment, appraisal notes, details of disciplinary or grievance cases)
- Photos, video or audio tapes
- Consent forms relating to activities and events
- Signed agreements with offenders
- All logs of events or incidents, including entries in incident and accident books and relating to specific allegations or concerns about a child or vulnerable adult

Storage and Access

Sensitive personal data should never be left unattended where others, who have no right to access it, may find it. Paper records should be kept in a locked cabinet or room with keys available only to those who have a legitimate need to access the information. Electronic records should be password protected or encrypted.
How long should records be kept?

One of the principles of the Data Protection Act is that personal data should not be kept for longer than the purpose it is required for. Guidance outlining how long parish records should be retained can be found on the **Retention of Records Fact Sheet** provided in the section Forms, Factsheets and Templates.

The Diocese as Umbrella Body destroys DBS disclosure certificates 6 months after the data of issue. It is illegal for the parish to retain a copy of a DBS Disclosure if this is shown by the applicant.

Any records which are no longer needed to be retained should be destroyed securely, i.e. by incineration or shredding, in the presence of another adult worker. If not shredded immediately, all confidential records must be held in a secure plastic bag, labelled as confidential and locked in a cupboard or other secure place.

Normally, personal information should not be held for longer than 6 years after the subject’s last contact with the parish. Exceptions to this period will occur when:

- The record needs to be retained because the information is relevant to legal action that has been started
- The record is required to be kept longer by law
- The record is archived for historical purposes (e.g. where the parish was party to legal proceedings or involved in proceedings brought by a local authority)
- The record consists of a sample of records maintained for the purposes of research
- The record relates to individuals and providers of services who have, or whose staff, have been judged unsatisfactory
- The record is held in order to provide, for the subject, aspects of his/her personal history (e.g. where a child might seek access to the file at a later date and the information would not be available elsewhere).

Right of Access to Personal Records

The law requires that any living person who is the subject of personal information held and processed by the organisation may access records containing information about him/her. The general principle is that as much information as possible should be shared with the individual. However, there are some restrictions and conditions attached to the legal right of access, for instance, in the interests of protecting the rights of other individuals to privacy and for the prevention of crime. Therefore all information must be removed which might identify a third party. In addition, information containing serious allegations, such as child abuse is entitled to be held back, if revealing the information would compromise an investigation into those allegations.
Dealing with Requests for Access

A formal request for access to personal records should be made in writing. The maximum period, in which a response must be provided to any request for personal access to records is forty days, however, a response should be given as soon as practically possible. The forty-day period commences at the point a written request has been received, and where any further information necessary to confirm the identity of the person making the request has been obtained.

Access should normally be provided on church premises and the case-file should not be removed from its location.

If any other person is mentioned in the record and disclosure would allow him or her to be identified, the person’s consent must be obtained before disclosure.

Where the church does not hold the personal information requested, the applicant should be informed of this as quickly as possible.

Any notification of refusal to disclose personal data should be given as soon as possible and in writing, even if the decision has also been given in person. The reason for the decision to refuse access should be recorded and explained to the individual unless there is good reason not to do this.

Information to be Disclosed

All data held about the individual requesting access should be disclosed, unless the data is subject to any exemptions. Information disclosed must be that held at the time the request was received. The individual has the right to comment on inaccurate data, and such information should be corrected if it is proved to be wrong. If the individual wishes to query or comment on a judgement or opinion about him/her, a written record of the query/comment should be appended to the original recordings.

In the event of a request to access personal data, which results in uncertainty about what information should be made available, you should contact the Diocesan Safeguarding Advisers for advice.