



DATA RETENTION ADVICE

The online safeguarding manual discusses Data Protection and the associated principles to consider when handling sensitive information in some detail within Standard 5. We also recommend that you read the information from the Information Commissioner's Office which sets out 8 principles regarding collecting, retaining and disposing of data. (Data Protection Principles, ICO). In brief, they are as follows:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Here we offer some guidance on one of those principles which is a common enquiry we receive on our Helpline with regard data retention. This includes:

1. Why retain information
2. How long to retain it

3. How to retain it - secure storage
4. How to keep a record of retention
5. How to dispose of unwanted information

1. Why retain this information?

On the Helpline, we receive frequent calls with regards to data retention. This InFocus is to assist you to answer the questions as recommended by the 'General Data Protection Regulations' that came into effect on 25th May 2018. This has now been incorporated into the latest update to data protection legislation i.e. the Data Protection Act (DPA) 2018.

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Along with the Data Protection Act, 2018 the following regulations and laws may also impact the work of several charitable organisations:

- Keeping Children Safe in Education, 2015
- The Charities Act, 2011
- Freedom of Information Act, 2000
- Fundraising Regulator's Fundraising Code
- Limitations Act, 1980

2. Duration of retention

Retention of safeguarding information is crucial to maintaining a transparent approach on the part of the organisation, both to assist in any future investigations and also to protect reputation. Local authorities usually retain their records for a period of 75 years and in some cases the term permanently maybe considered. With regards to all other information and data of a non-safeguarding nature, you should demonstrate evidence of giving adequate reasons to retain and safe keep such relevant information. A variety of reasons can be given for retaining any document, but the need is to have a measured approach. The default standard retention period for most organisations is 6 years plus the current year to allow for a review and/or disposal to be carried out within that year. Possible retention periods to consider are, immediately after creation, after 6 months, after 1 year, after 2 years, after 6 years, after 10 years etc. There are however some statutory retention periods that one would need to carefully consider, which are impacted by legislations and guidance such as the Limitations Act, 1980, Keeping children safe in education etc.

For example Keeping Children safe in Education 2015, gives the following advice on retention of records of allegations:

Details of allegations that are found to have been malicious should be removed from personnel records. However, for all other allegations, it is important that a clear and comprehensive summary of the allegation, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on the confidential personnel file of the accused, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference, where appropriate. It will provide clarification in cases where future DBS checks reveal information from the police about an allegation that did not result in a criminal conviction and it will help to prevent unnecessary re-investigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer.*

* at thirtyone:eight we are mindful of the fact that not all allegations regarded as malicious should easily be dismissed and that a vulnerable person or child may in fact be trying to convey a message about an event. We usually use the word 'unfounded' to convey this as a more accurate term. Some of the past case reviews have found that allegations which were dismissed have now returned to be re examined and some have reached a different conclusion than previously

However please also check with your denomination's protocols if they issue longer retention periods, particularly in the light of the investigations by the Independent Inquiry into Child Sexual Abuse (IICSA).

3. Storage

Any personal and sensitive information needs to be kept securely.

1. A locked filing cabinet in a place where access is limited to known/designated people.

2. Alternatively, documents can be scanned onto a computer where the information is password protected, backed up, where the password is regularly changed and where access is limited to known people.
3. The computer should not be a personal computer.
4. Where the information is needed for an event (for example a list of health information for young people at a camp), this should be kept in a secure place by the camp leader or designated person.


The CPSU (Child Protection in Sport Units) also offer additional advice on this which includes:

1. Maintain a log of individuals who access the unit and enter details of the files used.
2. Maintain separate files for concerns, allegations and referrals relating to individuals.
3. Make appropriate arrangements for safe exchange of keys in the event of a transfer of responsibilities/role.
4. Careful consideration of this facility in the event that the organisation/service is closing down.

4. Record of retention

A retention schedule is usually helpful in such situations. The ICO defines a Retention Schedule as 'a tool used to ensure the retention of business information for as long as it is needed'. The ICO advice that a retention schedule should be kept up-to-date in the light of the changing needs of the organisation, new legislation and regulation, risks involved etc.

Link: Records Management in Charities

As an organisation you may want to consider developing an Information Asset Register that captures details of all the data you hold within your organisation.

Form: Information Asset Register

Some useful principles to keep in mind when looking at data retention are:

- Does the data have any historic value (heritage) associated with the organisation?
- Does it have any safeguarding value? (i.e. potentially assist in future investigations/enquiries)
- Has explicit consent been given for retaining the information (particularly personal/sensitive data i.e. names, addresses, photographs or any other identifying information)?
- If the data has been identified for longer term retention, can it be transferred into a different format i.e. paper files to electronic copies.

- Do you need to seek legal advice or speak to your insurance company regarding data retention?
- Does your denomination have any specific guidance/policy on the matter? (for example the Church of England and the Methodist Church have detailed guidance on this subject which can be accessed [here](#))

5. Destruction and Disposal

The Child Protection in Sport Unit (CPSU) offer some good advice which is as follows:

- Documents are shredded or incinerated in the presence of a member of organisation or handed to a firm that specialises in destruction of confidential material
- Destruction of both electronic and paper copies should be carried out at the same time
- If not shredded immediately, all confidential records must be held in a secured plastic bag, labelled as confidential and locked in a cupboard or other secure place.
- When a part of an organisation (e.g. a club, team, project etc.) is closed down, the organisation must make arrangements for ongoing management of records relating to that club/team/project including the review, retention and disposal of records. (CPSU Briefings, 2013)