

It is in the interests of clients and bureaux that records be kept as long as possible, particularly:

- in cases involving complex advice
- in cases where a client has queried or complained about advice.

Case records: what to keep

It is extremely difficult, and can be impossible, to defend an action for negligent advice where the bureau does not hold a case record.

If a bureau has been negligent but a client does not discover this until later, (s)he has six years in which to bring a claim. (This is subject to a long stop of 15 years in that, irrespective of the client's knowledge, proceedings for negligence have to be started within 15 years of the last date on which any negligent act or omission occurred).

Ideally, therefore, all records should be kept for at least 16 years after the final entry, but this is not always practical and in most cases, unnecessary. The following guidelines should help bureaux to identify high risk cases:

Level of risk	Keep for	Examples
Low risk	6 years	
High risk	16 years	Any case that has been subject to a serious complaint, insurance claim or other dispute (here 'other dispute' refers to the bureau's handling of the case and not to any other dispute which the client may be having with a third party). The bureau will not need to keep a file if a case has been referred to the insurers (see 'if there has been a claim or complaint').
		Any case relating to building works or surveyors' reports on the purchase of property or relating to property
		Any case which bureaux consider to be substantial, where the sums of money involved are, for example, in excess of £10,000 or where the advice given was especially complex, or where bureaux are otherwise concerned that the case is unusual.

This list is not definitive.

CASE /Petra case records

Currently no case record is deleted or archived within the case management systems CASE / Petra so all client records put on the systems will stay there indefinitely. This will be reviewed in the future and this document and CASE / Petra guidance updated accordingly. Bureaux will be informed about any changes.

Systems for identifying high-risk files

As soon as it becomes apparent that a case is 'high risk' (see [Case records: what to keep](#)) the file should be clearly marked. With paper files the easiest way is to mark the destruction date clearly on the front. It would also be useful to keep a list of 'high risk' files, setting out the name of the client, the type of advice given, the reason for being assessed as 'high risk', the date until which the file should be kept - and where the file is. High risk files should be assigned an information asset owner who is responsible for the risk management of the file.

To ensure consistency in the definition of 'high risk', bureaux should delegate to one person the responsibility for deciding which documents are 'high risks'. If necessary, the appointed person should discuss with the advice worker concerned the nature of the advice given, paying particular attention to any relevant time limits (this may well also identify potential claims in advance).

Weeding files

[Paper files](#)

[If there has been a claim or complaint](#)

- **Paper files**

If a bureau is dealing with paper files (i.e. prior to CASE or any documents which are not in CASE) and a case is closed, or it looks as though the client will not be seeking further advice, the file should be sorted into chronological order, separating the correspondence, case notes, and documents within the file and destroying any duplicates. If you have multiple files on a client, combine them so that all the documents relating to one client are in the same place. Any documents within a file relating to claims or complaints must be kept separate and must be securely stored (see ['if there has been a claim or complaint'](#)).

Once the file is in chronological order, the appointed person can assess whether the file appears to be 'high risk', if it has not already been identified as such. If there is any doubt and if space allows, keep it for 16 years.

Particular care should be taken with case records that refer to more than one problem relating to an individual client.

- **If there has been a claim or complaint**

Where a complaint or other dispute has been resolved, the papers should be kept for 16 years after the resolution in case any queries arise as to the terms of settlement.

If the case involved an insurance claim of less than £850, there is only likely to be a record in the bureau so the bureau should keep the file. For [professional indemnity claims](#) worth more than £850, Citizens Advice brokers, ADS, will keep files, so there is no need for the bureau to keep a copy.

Archiving case records prior to destruction

Having paper case records scanned, indexed and stored electronically does have significant advantages in terms of space and ease of access. There is a cost, but some bureaux have investigated this route as an alternative to paying for external storage facilities. If using this functionality, the bureau must ensure suitable encryption and storage methods are used, there is a clear information asset owner and the electronic based information is entered on the Information Asset Inventory.

Whichever route you are investigating for archiving, you need to consider ease of access to individual case records, and cost, and to ensure that confidentiality is preserved. If you are using an external firm you should ensure that you have a signed data sharing agreement and that the external parties security is adequate.

Disposal

The principle of [confidentiality](#) must be safeguarded when bureau records are disposed of.

- Destruction

The guidance below is taken from the [golden rules of data security](#), which bureaux should follow.

Data handling - secure deletion / disposal / sanitisation of sensitive data

In order to preserve the confidentiality of all copies of sensitive data, it is important that at the end of its life, the medium which held the data, is either securely sanitised or securely destroyed. Always follow the procedures below:

- Paper - a confidential shredding service should be used when shredding sensitive data.
- Laptops / hard diskdrives - when disposing of laptops / hard drives you need to ensure they are securely wiped to government standards. You will also need to obtain a data deletion certificate, which should be kept. Products should be CESG assured.
- Audio tapes - data that is not confidential can be cut into small five centimetre pieces and then burned. The Citizens Advice service does not offer incineration facilities, so cutting into small pieces and then placing in usual rubbish bins is sufficient. You may wish to separate cuttings into separate bin loads. You should take care not to touch the tape with your bare hands.
- Keep a record of all media / sensitive data which has been securely destroyed / sanitised so this can be audited at a later date if required.
- USB sticks and CDs - it is very difficult to securely erase these materials without destroying them (which is sometimes unsafe for individuals to do) or making them unusable. For these reasons you should avoid using removable media to hold sensitive data at all. It is very important that existing sensitive data held on these devices be securely and safely erased. If you have USB sticks or CDs which hold, or have held, sensitive data, please identify yourself to the bureau SIRO who can work with you to ensure the data and devices are securely disposed of.