File storage, retention and destruction guidance

Introduction

The issue of how long firms should keep closed client files is complex. There are no hard and fast rules and it is impossible to apply a one-size-fits-all approach. The SRA does not deal with the issue specifically, and the Law Society's direct guidance is largely limited to trust and will files.

With this lack of certainty, and the risk of possible claims or complaints against the firm if documents are wrongly destroyed, it is easy to see why many firms simply archive all their closed files, often indefinitely. However, the Information Commissioner has adopted the position that retaining personal data on a 'just in case' basis - or without taking into account the circumstances and context – would not be compliant with the Data Protection Act. The SRA is also pressing firms to deal with historic archiving issues, having incurred huge costs in archiving and storing the files of firms it has intervened in.

The Data Protection Act/GDPR allows only information that is adequate, relevant and not excessive to be processed; and it should not be retained for longer than is necessary. Under GDPR, when you collect personal data you are also required to tell data subjects how long you will store their data for or, if that is not possible, the criteria used to determine that period.

While the SRA Standards and Regulations which replaced the SRA Handbook in November 2019 do not provide direct guidance, a failure to adequately address issues relating to the management of a client's file may well be a breach of the shortened principles including:

- SRA Principle 1 (to act in a way that upholds the constitutional principle of the rule of law, and the proper administration of justice);
- Principle 2 (to act in a way that upholds public trust and confidence in the solicitors' profession and in legal service); and
- Principle 7 (to act in the best interests of each client).

The position is complicated by the ever-increasing digitisation of files and by the changing statutory and regulatory landscape. Firms need to ensure that they comply with the rules and appropriately protect data. Since the application of the General Data Protection Regulation (GDPR) in May 2018, firms are under greater scrutiny and face very substantial penalties if they get it wrong.

This briefing provides general guidance on the approach to the retention, storage and destruction of files; however, it should be noted that all-embracing guidance on such multi-faceted and complex issues is beyond the scope of this briefing note. What is clear is that law firms need to be alive to the issues, and tackle them head on, rather than accumulate potentially significant problems (and costs) for the future.

Policy requirements for managing the closure, storage and destruction of files and documents

The starting point is having an effective policy for the closure, storage and destruction of client files and associated documents, in whatever form they are stored. This should clearly set out your 'base-line' retention periods for the different work types your practice undertakes; outline circumstances which would justify exceptions to the base-line period; and set out the rationale for the retention period set.

Your policy should address:

File Closure

> Checking that all work has been completed, there are no undertakings outstanding, and no money is owed to or by the client; and that the financial housekeeping of the file is complete;

> Ensuring the file is well organised, with any unnecessary or duplicate documents removed. (These might include duplicates of originals that have not been annotated, drafts of letters, memoranda, reports, informal notes that do not represent significant steps or decisions in the preparation of an official record and printed materials obtained from external sources and retained primarily for reference purposes). This will be important if a claim or complaint is later made against the firm;

> Removing or highlighting any important original documents which should not be destroyed; and, if appropriate, returning them to the client;

> Arranging for any unnecessary or duplicate non-paper records such as DVDs and CDs to be securely destroyed with IT support if needed;

> Informing the client:

- That their file has been closed;
- That they can have the file returned to them if they wish;
- What will happen to the file if it is not returned to the client;
- How the file can be retrieved;
- Whether any charges will apply; and
- That it may be destroyed after a specified period;

> Provision for copies to be retained in order to protect the firm's position if the file is returned to the client.

It is important to remember that the file is likely to comprise material in different formats and in different locations: in addition to the paper or electronic file it will likely also include information held in other forms, for example video call recordings, handwritten notes in notebooks, voicemails, memory in mobile phones and other mobile devices and even online postings, such as on social media sites.

Storage

> Specifying the firm's standard minimum periods of retention for the various categories of files, with an indication of the factors that may make it necessary to extend this period;

> Recording a proposed destruction date for every file, which should be reviewed before the file is destroyed – this should ideally be done by the main fee earner with reference to the firm's retention policy;

> Keeping a central record of:

- The files stored;
- The date they were sent to storage and the date of any recall/return if appropriate;
- Details of the provisional destruction/review date;
- The date of destruction.

The firm will need to give careful consideration to how and where files are to be stored (e.g. on-site, an off-site storage facility or using a third-party storage company) and the risks associated with the various options such as theft, fire, flood or the third party storage company going into liquidation. It is no good having an excellent storage policy if the files are then kept in a damp basement prone to flooding.

Electronic storage

The core principles applying to the storage and retention of documents are essentially the same whether they are in paper or (increasingly the case) in electronic format. Consideration could be given to a different approach to electronic documents (say for the storage of those for a longer period) particularly as such material does not carry the same budgetary concerns as the long-term storage of paper documents. Such differential for electronic documents would however have to the subject of a clear policy explaining the reasoning, satisfy the various regulatory requirements and be reflected in the relevant terms and conditions of the retainer with the client. You will also need to assess the risks before destroying the original files, if planning to retain only an electronic copy.

For electronic files it is important that all fee earners understand how the firm's electronic data is stored and preserved, how back-ups are created and maintained and for how long emails are retained.

You should also bear in mind the risk of data being corrupted during any migration process, and you will need to put in place systems to ensure the confidentiality, integrity and availability of the data. If you do intend to store files electronically you should make this clear to the client in your retainer letter and give the client the option of having the original file returned to them.

Destruction

- Procedures for authorising destruction, ideally by a senior member of the firm/head of department. Destruction should not be automatic when the proposed destruction date is reached; the file should be checked by someone who appreciates the importance of the task – this is not simply an administrative task and consideration should be given to each file on an individual basis. A case-by-case approach needs to be taken with appropriate review at the time of proposed destruction;
- Clear procedures for destruction which take into account the need to protect client confidentiality;
- Keeping a central record of all files destroyed including the date of destruction, the name of the person who authorised destruction and the reason for destruction.

The policy should be reviewed and monitored regularly to ensure it is being adhered to and remains legally compliant and cost-effective. There is little value in having a policy providing for most files to be destroyed after 7 years if the policy is not followed and files continue to stack up in an external storage facility.

Original documents

Original documents will require particularly careful handling and should always be returned to the client where possible, with a record of the return retained by the firm (such as recorded delivery slip or a receipt signed by the client).There may of course be a formal instruction for such documents to be held in safe storage; there could be occasions where the documents are sent to the person / entity entitled to them (e.g. unregistered property deeds to the purchaser on the completion of a sale transaction).

Where a firm decides to retain files indefinitely these may be reviewed periodically, for example after 10 years and then at 5-year intervals, to determine whether there has been any change in circumstances that would allow for the file to be destroyed.

Storage period for closed files

In determining the time periods for retaining files and other data, you have to balance the need to be able to access the information (for example to defend a claim) with the requirement not to hold information longer than necessary. Having a well-considered and rigorously applied policy in this regard is essential. The actual time periods in your policy, for the retention of closed files, are ultimately for each firm to decide, bearing in mind issues such as:

- The types of work the firm undertakes;
- The size of the firm and its client base;
- Limitation periods;
- The possibility of claims or complaints against the firm, including the firm's record of claims and complaints and how long these have taken to surface;
- The firm's assessment of the risks of destroying files versus the cost of storage;
- Whether it is the firm's normal practice to return files to clients when their matter is completed;
- The firm's experience of clients asking for the return of documents or files after they have gone into storage.

Most of the documents on a file belong to the client and, strictly speaking, should not be destroyed without the client's consent. In reality it is often impossible to obtain consent at the time you are considering destroying files, so this should ideally be dealt with in your retainer and/or closure letter.

Where you do not have the client's consent to destroy the file you will need to strike a balance between the ongoing cost of storing files and the risks attached to destroying them (e.g. that the client will want the file back or will bring a claim or complaint against you.)

Recommended base-line retention periods

The schedule at the end of this guidance sets out the suggested base-line period for different types of file to be retained, assuming that any important original documents are removed before destruction. It must be stressed that these are suggested base-line periods and there may be reasons to retain certain files for longer. Even when the allotted storage period for a file comes to an end, the decision to destroy the file should be considered on a file-by-file basis, following a documented process, taking into account issues such as:

- The nature and complexity of the work involved;
- Whether the client was vulnerable, under a disability or particularly difficult to deal with;
- Whether the client is likely to instruct you again on a related matter;
- Whether an issue has been raised which could have future implications for a complaint or a claim.

Time periods: the general rule

Most advice recommends minimum periods of between 6/7 and 15 years, with a few exceptions in relation to certain files and important original documents. These reflect the primary and long-stop limitation periods for the majority of claims - most commentators now recommend at least 7 years to allow for claims made towards the end of the primary cut-off point. Some firms prefer to store all files for a minimum of 15 years, by which time the majority of claims would be statute-barred (although in some matters, for example relating to wills and trusts, or involving children, even this may not be long enough – see below).Others prefer to store different categories of file for different periods according to the level of risk involved, in which case a minimum of 7 years is recommended for the files deemed less risky.

It's worth bearing in mind that the 15 year long stop is for a claim in negligence starts to run from the date on which the alleged negligent act or omission that is said to give rise to damages occurred; that could be an earlier date than the date the cause of action accrued.

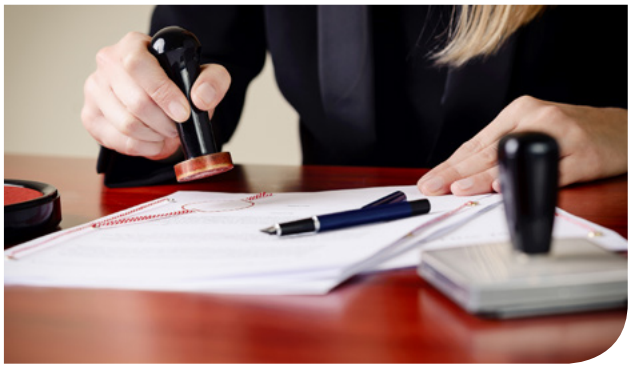
What does the SRA say?

The SRA is largely silent on this subject and the only guidance that touches on it relates to the closure of a practice and focuses on the need to assess the risk of destroying documents belonging to the client without the client's consent.

The SRA has, however, reviewed and amended its policy on storing the files of firms it has intervened in, following concerns about the substantial and increasing costs involved. The SRA made clear in its consultation on the subject that the issues discussed applied only to storage by the SRA and not to file retention by firms, where different considerations apply. However, it may be possible to glean from the SRA's revised approach some useful pointers for firms, in particular in relation to what is considered to be an "original document" and which types of files should be retained for longer than the standard period of 7 years from the date of file closure (e.g. files relating to family matters, trusts, wills and probate will be retained for 21 years, medical negligence files for 15 years).

Special cases: files and documents that need to be kept for longer

Files relating to certain types of work need to be stored for longer. For example, special considerations apply to files relating to wills and trusts, where the risk of disputes appears to be increasing and claims can surface many years after the original work was carried out, particularly in relation to wills. In cases involving children, the normal limitation periods can be considerably extended.



Wills and Probate

Original wills should normally be kept indefinitely, if they are not returned to the client. Even if a will is subsequently revoked, the original will may be relevant if the later will is subsequently disputed. It can also be important to keep records relating to the circumstances in which the will was made and make clear that appropriate advice was given, in case the firm is asked to justify its position in any subsequent dispute. Also bear in mind that documents relating to VAT liability need to be retained for at least 6 years, if you decide not to keep the whole file with the will. You should also consider whether it is necessary to keep details of the estate of a client's deceased spouse or civil partner in relation to the transfer of unused inheritance tax nil rate band allowance. The Law Society has produced detailed practice notes on the retention of documents in relation to wills and probate matters which should be consulted:

https://www.lawsociety.org.uk/en/topics/private-client/file-retention-wills-and-probate

Trusts

The original trust deed and any deeds amending its provisions or appointing new trustees are held to the order of the trustees and should be stored safely. As with wills, the risk of litigation is increasing, and proper record retention is essential. Disputes can arise several years after the original trust was drawn up and the normal limitation periods will not always apply. Without adequate records your firm may not be able to defend its position. The file should normally be retained for at least the duration of the trust. The Law Society generally recommends retaining trust administration files for the duration of the trust plus six years and longer for tax papers. It has produced detailed practice notes on the retention of documents in relation to trusts, which should be consulted:

https://www.lawsociety.org.uk/topics/private-client/file-retention-trusts.

Closing your firm

When a firm closes it is important that files are dealt with properly: either returned to clients, securely stored or destroyed if appropriate. Once the firm has closed, members of the firm must take care not to practice or be held out as practicing through the firm when dealing with the disposal of documents. It is unlikely that you will be considered to be practicing if you are simply dealing with the disposal or storage of files, but you continue to use your firm's notepaper when dealing with these, or other outstanding administrative tasks, you will need to adapt it to make it clear that the firm has closed. Both the Law Society and the SRA have guidance on file management where a firm is closing:

https://www.lawsociety.org.uk/en/topics/business-management/file-closure-management

https://www.sra.org.uk/solicitors/guidance/closing-down-your-practice/ (note in particular the useful guidance on original deeds and documents).

GDPR and Client Consent

This guidance focuses on the effect of the GDPR and its UK equivalent on issues in relation to the retention, storage and destruction of client files. We consider the impact of the GDPR on client consent in relation to the processing of data and flag a number of wider concerns. It is outside of the scope of this guidance to consider the implications of data protection law more widely.

Currently having the client's consent is often used as a basis for the lawful processing of client data in a wide range of contexts. Whilst consent remains a legal basis for processing personal data under the GDPR it introduces a higher standard - for the purposes of the GDPR a data controller must provide the data subject at the time the personal data is obtained with information necessary to ensure fair and transparent processing (Article 13).

Firms will need to periodically review the mechanisms that they've adopted and whether they're adequate to meet the data retention requirements. The obligation is on the firm to notify the data subject that the firm will be processing the data and the specific purpose of the processing of that data. The biggest change was that the GDPR raised the bar as to consent mechanisms – clear granular opt-in methods are required together with good records of consent and simple easy to access ways for people to withdraw their consent. For more information, read the ICO guidance on consent issues: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

You are also required to notify clients of how long you will be keeping their personal data. Consent may be the only ground to process sensitive personal data although it may be possible to rely on the ground that processing is necessary for the establishment, exercise or defence of legal claims. The relevant grounds should be communicated to the client at the time the personal data is collected, ideally when instructions are first being taken. Further, any policies for the retention, storage and destruction of files will need to reflect the increased rights of the data subject under the GDPR – in particular the right to be forgotten; rights of access and certain new rights such as the right to portability of data. These rights together with the period for which personal data is retained must all be communicated to the client.

Do not forget that consent is not the only basis for processing personal data; there are other alternatives that are likely to be more appropriate. For personal data other than sensitive personal data (special category data under GDPR) other potential lawful grounds include:

Where the processing is necessary for the performance of a contract;

Where the processing is necessary for compliance with a legal obligation; and

Where the processing is necessary for the purposes of the legitimate interests of the data controller or a third party.

However, it should be noted that a balancing test needs to be undertaken to ensure that your legitimate interests as the data controller are not overridden by the legitimate interests of the data subject.

Appendix: Suggested base-line retention periods

Type of matter	Suggested base-line retention period	Exceptions/reasons for storing file for longer	Suggested reason for retention
Crime	7 or 15 years depending on seriousness of crime	Where a life or indeterminate sentence has been imposed	Limitation period for actions in negligence 6 years
Employment	7 years		Limitation period for actions in negligence 6 years
Immigration, including advice, asylum, tribunals, work permits, applications for citizenship/nationality/ passport	7 years		Limitation period for actions in negligence 6 years
Wills and probate	Indefinitely if keeping with will. See https://www.lawsociety.org.uk/en/topics/private-client/file-retention-wills-and-probate		Reflects the potential "long tail" nature of potential claims
Trusts	Duration of trust plus 7 years. See https://www.lawsociety.org.uk/topics/private-client/file-retention-trusts		Reflects the potential "long tail" nature of potential claims
Family, including divorce, separation, custody and contact, injunctions, child protection and court of protection	15 years		Limitation period for actions in negligence 6 years; potentially longer where there are children.
Business, including company/partnership formation, insolvency, trademark/copyright/ patent	15 years		Limitation period for actions in negligence 6 years – to include long stop of 15 years

Appendix: Suggested base-line retention periods

Type of matter	Suggested base-line retention period	Exceptions/reasons for storing file for longer	Suggested reason for retention
Property sale	7 years		Limitation period for actions in negligence 6 years
Property purchase and mortgage	15 years		Limitation period for actions in negligence 6 years – to include long stop of 15 years
Leasehold and tenancy	Length of term plus 7 years		Limitation period for actions in negligence 6 years
Personal injury	7-15 years, depending on seriousness of injury and complexity of case	Longer if involves, children, complex issues, e.g. lifetime or provisional damages awarded	Limitation period for actions in negligence 6 years – to include long stop of 15 years
Medical negligence	15 years	Longer if involves, children, complex issues, e.g. lifetime or provisional damages awarded	Limitation period for actions in negligence 6 years – to include long stop of 15 years
General litigation e.g. tribunals, mental health, prison matters, application for alcohol licence, harassment	15 years	Longer if client is under a disability	Limitation period for actions in negligence 6 years – to include long stop of 15 years
Private client non-litigation advice, e.g. employment, pensions, powers of attorney, change of name, debt, personal insolvency, housing disrepair	7 years		Limitation period for actions in negligence 6 years

Original documents that should be retained indefinitely or as indicated:	The following documents may also be important to the client and difficult to replace, therefore you should exercise caution before destroying them:
> Unregistered property deeds > Mortgage deeds (including assignment of mortgage) / legal charge, where unregistered title > Abstract of title > Lease documents – store for at least its term > Power of attorney / court of protection deputy > Tenancy agreement – retain for at least its term > Grave deeds > Share certificates / bonds > Will / codicil > Deed of gift / trust > Statutory declaration > Life assurance / mortgage of life / endowment policies > Mortgage of life policy > Guarantee certificate > Personal effects / valuables.	The following documents are important to clients and can be difficult to replace, therefore additional controls should be put in place before they are destroyed, > Certificates of birth or marriage for foreign nationals who may find it difficult to obtain replacements > Deeds of partnership > Patents / copyrights > Medical records such as x-rays.

This guidance has been produced in conjunction with Berrymans Lace Mawer LLP.

For more information

If you would like to discuss your wider file management arrangements in more detail, please contact either Calum MacLean or Deborah O'Riordan in QBE's Risk Solutions team.

Contacts

Deborah O'Riordan
Practice Leader
QBE Risk Solutions
deborah.o'riordan@uk.qbe.com

Calum MacLean
Senior Risk Manager
QBE Risk Solutions
calum.maclean@uk.qbe.com

QBE European Operations

30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
QBEeurope.com

Made possible
QBE

333173/2110