IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

THE LEGAL RECORDS AT RISK PROJECT

Project patrons: William Twining, Quain Professor of Jurisprudence Emeritus, UCL and Avrom Sherr, Emeritus Professor, IALS

http://ials.sas.ac.uk/research/areas-research/legal-records-risk-lrar-project

Legal records, confidentiality and access: breaking down the barriers

The 3rd Legal Records at Risk seminar

27 October 2017, IALS Conference Room, 1.30-5.00 pm

Seminar Proceedings

Seminar attendees

Name	Occupation/organisation
Penny Baker	Vice- Chair, British Records Association
Philip Bouchier	Archivist, Herefordshire Archive and Records Centre
Tracey Calvert	Director, Oakalls Consultancy Limited
Sharon Cooper	Corporate Compliance Manager, Chartered Institute of Legal Executives
Clare Cowling	LRAR Project Director, Institute of Advanced Legal Studies
Joanne Cox	Researcher, Research Unit, The Law Society
Dr Mark Forrest	Collections Manager, Dorset History Centre
Clive Freedman QC	Barrister, 3 Verulam Buildings, Gray's Inn
Philip Gale	Head of Standards and Improvement Team, Archives Sector Development, The National Archives
Nicholas Le Poidevin QC	Barrister, New Square Chambers, Lincoln's Inn
Dr Elizabeth Lomas	Senior Lecturer in Information Governance, Department of Information Studies, University College London
Philippa Mole	Head of Archive, Guardian News & Media Archive, The Guardian
Professor Linda Mulcahy	Professor of Law, London School of Economics
Alan Shipman	Director, Group 5 Training Limited
Professor William Twining	Quain Professor of Jurisprudence Emeritus, University College London
Dr Michael Waibel	University Senior Lecturer and Co-Deputy Director of the Lauterpacht Centre for International Law, University of Cambridge
Dr Lisa Webley	Professor of Empirical Legal Studies, University of Westminster
Jules Winterton	Director and Librarian, Institute of Advanced Legal Studies

Agenda

Chair: Jules Winterton, IALS Director

1.30-1.50	Arrival and refreshments	
1.50-2.00	Welcome and introductions	Jules Winterton, IALS Director
2.00-2.10	Seminar introduction: what *are* the barriers to accessing legal records for research?	Clare Cowling, Director, Legal Records at Risk project, IALS
2.10-2.30	The legal practitioner's perspective (solicitors)	Tracey Calvert, Director, Oakalls Consultancy Ltd
2.30-2.50	The legal practitioner's perspective (barristers)	Nicholas Le Poidevin QC, Barrister, New Square Chambers, Lincoln's Inn
2.50-3.10	The researcher's perspective	Dr Lisa Webley, Professor of Empirical Legal Studies, University of Westminster
3.10-3.30	The archivist's perspective	Philip Gale, Head of Standards and Improvement Team, Archives Sector Development, The National Archives and Dr Elizabeth Lomas, Senior Lecturer in Information Governance, Department of Information Studies, University College London
3.30-4.00	Refreshment break	
4.00-4.50	Expert Panel: questions for the Panel and general discussion	All
4.50-5.00	Summing up	Jules Winterton

Seminar speakers and Expert Panel members: biographical details

Clare Cowling is an Associate Research Fellow of IALS and Director of the Legal Records at Risk project. She has been an archivist and records manager for over 40 years in Australia and the UK and has also co-managed two earlier projects on legal records, the Legal Records in the Commonwealth project, completed in 1994 and the Records of Legal Education project, which resulted in the establishment of the Records of Legal Education Archives at IALS in 2001.

Tracey Calvert is a lawyer who specialises in professional ethics, regulatory and legal compliance issues. She was previously employed by the Law Society as a senior ethics adviser and was part of the policy team at the Solicitors Regulation Authority which drafted the SRA Handbook. She now runs her own consultancy business, Oakalls Consultancy Limited, providing compliance services to other lawyers. She has written a number of books,

is on the boards of the Legal Compliance Association and the Law Society's Legal Compliance Bulletin, an officer of the professional ethics committee of the International Bar Association, and a contributor to Cordey on Legal Services.

Nicholas Le Poidevin is a barrister practising in London. He specialises in private client work, both contentious and non-contentious, appearing in some of the leading cases in trusts and estates in recent years, both in England and offshore, and has a particular expertise in the conflict of laws. He speaks and writes extensively on the law of trusts and estates and has for several editions been a senior editor of *Lewin on Trusts*. He has a strong interest in legal history and is editing for the Selden Society a collection of fifteenth-century law reports. A Bencher of Lincoln's Inn, he chairs it's Library Committee and is keen to maintain and expand the Library's holdings of historical material, both printed and manuscript.

Dr Lisa Webley is a Senior Fellow at IALS and Professor of Empirical Legal Studies at the University of Westminster. She undertakes research on legal ethics, the legal profession and access to justice and was until recently on the University Research Ethics Committee which had oversight of all research in the University. She is Secretary of the International Association of Legal Ethics and General Editor of the journal Legal Ethics. She is the incoming co-director of the Legal Education Research Network.

Philip Gale is the Head of Standards and Improvement Team at The National Archives which has the responsibility to develop and deploy effective standards and good practice to support the effective care of and access to archives. The key standards it works with are the Archive Service Accreditation and standards relating to Places of Deposit for Public Records. Since training at the University of Liverpool in 1983, Philip has held a variety of archival and records management posts with the Glamorgan Archives Service, Warwickshire Record Office, Bedfordshire and Luton Archive Service, the former Corporation of London Records Office and the Church of England Record Centre. He has a keen awareness of the importance of archives as an asset for supporting business operations and reputations as well as their wider historical and cultural significance for their owners and wider society.

Dr Elizabeth Lomas is a Senior Lecturer in Information Governance at University College London. Her research currently focuses on the research needs for the digital evidence base (RecordDNA https://recorddna.wordpress.com/) and developing tools to aid the navigating of information management and compliance challenges for society and business. She has particular expertise in information rights law and its application in practice. She undertakes small scale consultancy projects and currently these are increasingly focusing on GDPR. Elizabeth is a member of the Advisory Council on National Records and Archives and the Deputy Chair of the Forum on Historical Manuscripts and Research.

Speakers' Presentations

Seminar introduction: what *are* the barriers to accessing legal records for research?	Clare Cowling, Director, Legal Records at Risk project, IALS
The legal practitioner's perspective (solicitors)	Tracey Calvert, Director, Oakalls Consultancy Ltd
The legal practitioner's perspective (barristers)	Nicholas Le Poidevin QC, Barrister, New Square Chambers, Lincoln's Inn
The researcher's perspective	Dr Lisa Webley, Professor of Empirical Legal Studies, University of Westminster
The archivist's perspective	Philip Gale, Head of Standards and Improvement Team, Archives Sector Development, The National Archives and Dr Elizabeth Lomas, Senior Lecturer in Information Governance, Department of Information Studies, University College London

Clare Cowling, Nicholas Le Poidevin and Elizabeth Lomas gave powerpoint presentations which are available elsewhere under the seminar link.

Tracey Calvert, Director, Oakalls Consultancy Ltd, made the following points:

1. There are two things we know about lawyers: they keep secrets safe and keep money safe.
2. Being a trusted adviser means that confidentiality is important.
3. With confidentiality, lawyers must comply with the law and professional ethics
4. Law first – the SRA Code of Conduct says that we must comply with all legislation relevant to our business, including the Data Protection Act and, from May, the General Data Protection Regulation (GDPR).
5. Data legislation – protects all of us from misuse of our personal data, there must be a valid reason for holding it, data subject rights etc
6. Data controllers must have retention, storage and destruction policies
7. We will be fined if get this wrong
8. So, in context of this topic, data legislation applies to data held about identifiable living humans and we have duties in respect of the storage of their data.
9. GDPR applies to all data. Professional ethics applies confidentiality duties to clients' and former clients' information.
10. Confidentiality continues forever – there is an example of a solicitor who was disciplined because he breached confidentiality in the 1980s.
11. Given that it never ends, perhaps the realistic question is when does the risk reduce to minimal impact? The SRA does not give an answer to this point.

12. The SRA does not provide guidance on document storage, destruction etc. The most recent guidance was issued in 1999 by the Law Society.
13. So none of the above is geared up to putting solicitors in a position where they will be able to assist archivists easily.

Conclusion: In the absence of a positive duty to assist archivists and a positive duty to preserve documents, and without the express consent of the client, you can see why solicitors are reluctant to do more.

Dr Lisa Webley, Professor of Empirical Legal Studies, University of Westminster, noted that:

1. The use of data by researchers is governed by university and professional body codes of ethics and it is very usual for academic researchers to need to go through a research ethics approval process before they are permitted to begin their research. The use of documents is considered to be the use of data and consequently archival research will be subject to ethical considerations under the codes.
2. Researchers are required to consider the ethical implications and wider effects of their research through the life-cycle of their study and then beyond when the disseminate their findings. They will consider:
    - The way that the data is collected, and if this is archival research this will include the purpose for which the documents were produced in their original form, by whom, to what end. When a researcher is collecting the data herself then the informed consent of all research participants, broadly drawn, would be the expectation. This is not usually possibly for data derived from pre-existing archive but that does not negate the need to think about those behind the documents and those affected by their use.
    - What confidentiality and other guarantees or expectations those involved in their original production may have had.
    - How the documents will be used by the researcher, how they are to be selected and analysed and the extent to which this is methodologically and ethically robust.
    - Any risk of harm arising from the use of the documents, and any benefit of their use in this way. Harm is considered both backwards and forwards, in other words it is assessed for the totality of the research including any harm and benefit that may arise from the findings being disseminated.
3. Some of these considerations raise thorny issues for the researcher as s/he is not able to control the conditions that gave rise to the production of the documents and it may be difficult in advance to foresee the range of interests that may be engaged ahead of consulting the archives. However, by thinking about the study in ethical terms it is often possible for a researcher to gain a greater degree of insight into the likely significance of the research and also to give real thought to the methods being used and thus to the study's rigour.

Philip Gale, Head of Standards and Improvement Team, Archives Sector Development, The National Archives, gave the following talk:

1. Introduction – TNA's role

The Archives Sector Development Department at The National Archives (TNA) has a general responsibility to support the development and sustainability of archive collections across the country. TNA has two spheres of responsibility:

- Our role as national repository for public records and oversight of the public records held by Places of Deposit (PODS) across the United Kingdom, including the records of courts and inquiries. This flows from the Public Records Act 1958 and subsequent legalisation.
- A wider more nuanced role of leadership of the archives sector which is essentially focusing on sustaining the preservation, access and value of the nation's archival collections for the present and the future. Legislation is largely absent and much of our role derives from the Historical Manuscripts Commission's (HMC) Royal Warrant and articulated in our recently launched policy document 'Archives Unlocked': http://www.nationalarchives.gov.uk/archives-sector/projects-and-programmes/strategic-vision-for-archives/

  The records of legal businesses generally come under the second element of our work.

2. TNA's perspective on legal business records

The business records, as distinct from court and inquiry records, of the various branches of the legal industry from our perspective form a category of business records; the primary obligation for firms is to meet their legal obligations (eg data protection legislation) and hopefully their cultural responsibilities to preserve records of historical significance, and those of corporate value (eg for sustaining a brand; to quote the website of a well-known firm, 'Farrer & Co is an independent law firm with a rich history').

It is not TNA's role to tell the legal profession how it should manage its records, but we do have a responsibility to encourage good practice and promote the cultural, economic, research and special value of archives.

3. TNA's management of archival risk

TNA has developed a system for selecting public records for permanent preservation in accordance with the Public Records Act as amended by other legislation eg Constitutional Reform and Governance Act 2010, amending the legislation to gradually reduce the deadline for transferring records to TNA from 30 to 20 years, implemented 2013–2022. The framework is largely determined by legislation.

We are responsible for:

- Selection of records for permanent preservation under the guidance and supervision of the Keeper of Public Records.
- Safe-keeping of those records.
- Transfer of records to The National Archives or an approved place of deposit by the due date unless they need to be retained, in which case the Secretary of State for Culture, Media and Sport's approval must be obtained.
- Considering formal applications for retention of records by departments are which are reviewed by our Advisory Council.
- Disposal of records not selected for preservation, by destruction or presentation to another institution.

Good practice is supported by the Code of Practice on the Management of Records, issued under section 46 of the Freedom of Information Act and the Civil Service Code for Staff, issued under the Constitutional Reform and Governance Act 2010, includes a requirement that civil servants should 'keep accurate official records'.

This elaborate system of appraisal and regulation may not immediately appear to be relevant to the business and clients records of a legal business. However, much of the good practice developed concerning public records can found across the wider archives sector.

4. Managing archival risk outside of TNA

A lot of what follows is a reiteration of good practice cited in the Legal Records at Risk Project Guideline 4: advice to legal institutions on confidentiality and research access to records relating to confidentiality and research access to records.

Risk diminishes over time

A basic observation is that that the risk of harm arising from the unauthorised access or inappropriate access to records diminishes with time. The content of relatively few records after 100 years will cause substantial harm or distress. Some public records are closed for longer periods, perhaps notably those of the intelligence services where, for instance, records giving details of informants might identify their immediate descendants might be protected beyond 100 years.

Similarly business records may include controversial material: Unilever's archives include the archives of the Royal Niger Company; landed families may be sensitive about the activities of their predecessors eg in relation to the slave trade or agricultural, clearances and institutions, eg the Churches over child emigration to the Commonwealth and child abuse.

The other area of risk is of clients, their heirs and personal representatives coming back to make a claim, but experience suggests that this increasingly unlikely with the passage of time. The sensitivities of well established businesses and institutions with long histories generally represent greater levels of risks than small businesses and individuals.

Deposit or self-curation?

The first fundamental choice facing any business or institution is whether to retain their archives in their own custody and management or deposit them with a reputable archive service. For organisations of a certain critical size retaining archives in their own direct custody under professional management may offer the best solution. One example of such a corporate archive is the Unilever Archives at Port Sunlight (https://www.unilever.co.uk/about/who-we-are/our-history/unilever-archives.html).

Depositing a collection with an established archive service regulated by deposit agreement is the alternative, but archives services are essentially there to facilitate access and generally are less enthusiastic about accepting large collections that cannot be accessed for many years. The acquisitions also need to be aligned with archives' collecting policies. Established archive services include those managed by local authorities and, particularly significantly for business archives, those managed by universities. A good example of a business archives held by a university are the Marks and Spencer Archives held at the University of Leeds (https://marksintime.marksandspencer.com/home).

If the decision is to deposit an archive collection archive services have developed a variety of techniques to protect sensitive information.

How archivists protect sensitive information

Archivists over the last century have developed number of measures to manage access to collections which can be used by an in-house archive unit or applied to a collection deposited with an archive service:

- Closure periods – generally these can range from 20–100 years depending on the sensitivity of the material on commercial, data protection and general confidentiality grounds. All catalogues with material subject to restricted access should clearly be marked.
- Confidentiality agreements with researchers; many academic institutions will have their own research codes of ethics to reinforce such agreements.
- Deposit agreements can specify closure periods and specific access arrangements eg the Wolfson Foundation archives deposited with at Royal Society Library can only be accessed with the prior permission of Foundation.
- Sensitivity reviews are widely used by government departments to assess the sensitivity of particular classes of records and businesses can develop their own forms of sensitivity reviews.
- Anonymisation and redaction of the data, especially for electronic data.

Sources of advice

TNA's website gives advice on data protection and includes a link to the supporting code of practice for archivists and records managers: http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/

The Information Management pages on TNA's website include much that is applicable to business as well as public records: http://www.nationalarchives.gov.uk/information-management/manage-information/planning/records-management-code/implementation-guides/

Conclusion

These techniques and measures are used by archivists to manage access to records while respecting legal requirements and the wishes of depositors and donors. Archival reputations rest on being trusted and any archives that allowed the disclosure of unauthorised information would face a fundamental loss of reputation equivalent to a leaking nuclear reactor!

The various legal professions including the traditional ones of the solicitors and the Bar as well as the newer professions of arbitrators, mediators, etc are increasing organised on an industrial scale and form a major part of economy and society. The cultural, economic, research and special value of legal archives are important to the wider archival heritage of the country. They also have to navigate changing expectations of accountability and transparency to society as well as to their clients and effective records management and where appropriate archival provision is one way of meeting their obligations to both clients and to society at large.

…….

Questions for the expert panel

The following questions were put to the Panel (comprising our speakers), with responses also invited from seminar attendees:

Question 1: A barrister present at the seminar noted that if the legal profession were to make client files available for research it runs the risk of being sued for breach of confidentiality, or at the very least suffering reputational damage, even after the clients are deceased. Admittedly this risk does diminish over time, but even so *what is the benefit to the legal profession in depositing records in archives for future access*?

Response: there may be a public interest in releasing some material. Examples included case files relating to historic child abuse. The point was made that aggregated or anonymised medical data is often released for research, though admittedly this is not so easy to do with legal records. Another point was made that the history of how the legal profession works is under-represented in archives and therefore in our national history and that it should be in the profession's interest to correct this imbalance. Attendees asked how the emphasis on client confidentiality and concerns over reputational risk square with the historic practice of many law firms and some individuals to offload records en masse to archives without any idea of what they contain; with leaving client files for decades in 3rd party repositories without any provision for appropriate disposal; and with auctioning records off to the highest bidder. Solutions for the future suggested better records management processes; including consent notices on how their data will be used and disposed of in agreements to be signed by clients; clearer guidance by the regulators on ownership, storage and disposal of data; the re-issue of The Law Society's practice note on depositing records in archives.

Question 2: An archivist whose repository has accepted deposits of client files from law firms wrote to ask: "Of course there are issues with preserving client files for historical purposes as I doubt any clients have given their consent to that and there are issues with solicitors not understanding the ownership of the material that they send us". *Should the permission of clients be sought prior to deposit of client files? Would this be feasible in practice?*

Response: Two questions to answer: 1) who owns the documents and b) do they contain confidential information? In an ideal world law firms would have a process in place whereby the client was asked (eg at the end of the relationship) if they were happy to have their records deposited in an archives on terms specified by the firm. Many clients may not be comfortable disclosing confidential information if they thought it may be shared, even at after a long closure period. In the past once records arrived at an archives the terms of the firm/client relationship had been lost, so this is really a question for future potential deposits. The legal regulator (ie the SRA) should be providing guidance on these issues.

Question 3: A firm which has already deposited records in a local authority archives is having second thoughts about eventually allowing access to researchers. There were two separate concerns from the firm a) complaint to legal ombudsman for breach of confidentiality from the descendent of a client and b) bad publicity from the impression that they would advise clients then make details public later on. *Are their concerns founded? if yes can they be allayed and if so how?*

Response: this law firm should have sorted out these questions before deposit. As above, all law firms should have a process in place to ensure that these questions have been dealt with. The SRA should also be providing guidance on these issues.

Question 4: The archivist of a large in-house business archive wrote: "We've encountered nervous resistance from the legal team when it comes to the transfer of certain types of records and, having slightly unexpectedly secured a few minutes of the senior lawyer's time tomorrow, I wondered if you might have any best practice examples to hand that I could use to reassure her? She is particularly concerned about the transfer of material that could be of assistance in legal proceedings, that discloses confidential sources or which may waive privilege having been transferred to the archive. We have of course clarified that records in the archive are not automatically open to researchers, and offered to take advice on appropriate closure periods, but because transfer to the archive affects the legal ownership of the records her concerns remain. For example, we are struggling to get permission to take in any records from the [-] legal team except statements of case and judgments (available elsewhere) and standard advice sheets (eg. on libel, data protection etc.) produced for journalists in house. We would like to take correspondence documenting key decisions in significant legal cases (eg those attempting to set precedents or make challenges for [-] rights), but there is concern that these records ought never to be transferred or made available to researchers, which seems a shame to me in terms of their potential interest and significance in future." *How would the Panel suggest that the archivist alleviate the concerns of this legal team?*

Response: the law firm should have a retention schedule in place which would specify which records should and should not go to the archives. The SRA should be providing guidance on retention, destruction and deposit of records in archives, as the Law Society once did with its practice note on disposal of solicitors' records (no longer available on the TLS website). Additionally an in-house archives is primarily there for the use of the law firm itself and can close records to the public for as long as it wishes. Setting up an in-house archives may in fact be the answer to many of the problems larger law firms face in managing their records appropriately.

Question 5: A barrister has offered his personal papers (which include notes on cases he has been involved in) to an archives. *Are they subject to legal professional privilege and if so for how long must they be closed to public access?*

Response: ownership is a major issue here. Are the papers copies of material held by other parties (eg the court; the organisations or individuals involved in the cases; the firm of solicitors employed?), or the barrister's own papers? Do they contain confidential material/personal data; if so just passing these papers to an archives could be seen as a breach of confidentiality, although the new Data Protection Bill will provide an archival derogation. The first action for a potential archival recipient is to obtain a detailed list of the papers. The regulators (ie the Bar Standards Board) should be providing guidance to practitioners on disposal of their case notes and related papers.

Question 6: the Chartered Institute of Arbitrators' Practice Guideline 1: Confidentiality in Mediation states "Save as required or permitted by law… the Institute, the parties, their representatives, their advisors and the mediator(s) shall keep confidential all information

(whether given orally, in writing or otherwise) produced for, or arising out of or in connection with, the mediation passing between any of the participants and between any of them and the mediator made for the purposes of the mediation, including the fact that the mediation is taking place or has taken place…The mediator's duty to protect the confidentiality of the mediation proceedings commences with the first communication to the mediator, is continuous in nature, and does not expire upon the termination, for whatever reason, of the mediation under Rule 11. The mediator's duty extends to all information relating to the mediation proceedings, even indirectly, such as previous invitations and/or negotiations leading to mediation, terms of the agreement to mediate, appointment of mediators and performance, or non performance, of the settlement agreement. All records, reports, or other documents received by a mediator, as well as all notes taken by the mediator during, with reference to, or for the purposes of, the mediation should be returned to the parties or kept secure until no longer needed for any purpose relating to the mediation and then destroyed." *Is this a direct instruction to individual arbitrators and mediators NOT to deposit their case notes and papers in archives or could "*any purpose relating to the mediation" *also be interpreted as including research?*

Response: possible research value cannot be used as a justification for keeping these records.

Question 7: The ILA - ICA COMMITTEE REPORT, THE HAGUE 2010 Confidentiality in International Commercial Arbitration has stated: "The duration of confidentiality obligations, as regards both the moment when it arises and when it ends, is equally the subject of uncertainty and is not dealt with in the sources. The answer will probably vary to a large extent depending on the nature of the information and, obviously, on the source of the duty. If the source is contractual, the duration might be stated in the contract (which may be prior to the beginning of the arbitration or subsequent) or should be able to be derived through the interpretation of the contract. The fact that the duty of confidentiality usually covers the award seems to point to an expectation that the regime of confidentiality should outlive the arbitral proceedings and that the obligations will not cease after the end of the arbitration. It is less clear whether the obligations are perpetual or whether at some point they lapse, and if so at what point. It is reasonable to assume that the obligations cease where it can be established that confidentiality is no longer relevant." *Can the Panel suggest scenarios where confidentiality is "no longer relevant"?*

Response: confidentiality is no longer relevant if the information comes into the public domain. It may also no longer be relevant if both parties are companies or businesses which have dissolved. The legal regulators should be providing advice on whether confidentiality obligations are perpetual or, if not, when they may lapse.

…….

General discussion and points raised

The following points were raised by attendees during the seminar:

1. There are legal and ethics issues around the management of client files, in particular the duty to keep client records confidential.
2. The Data Protection Act and the GDPR also require personal data to be kept confidential.
3. Confidentiality of client records is, according to the members of the legal profession present, infinite, so a risk-based approach to releasing material for research is required.
4. There are also issues over document ownership which must be dealt with before records are made available for research.
5. Research ethics require rules around: collection of data; use of data; storage of data; and disclosure of data.
6. Collection of data requires informed consent (why is it being collected; who will see it; how it will be used; how it will be confidentially destroyed). If the rules are relaxed what is the potential for harm? Informed consent of course can't be obtained from the dead, so a risk-based approach is needed.
7. Storage and destruction of data: researchers usually have an end date in mind, but how many of them do actually destroy the data? Where are the checks on confidential storage and destruction? The same questions on storage and destruction of the information they hold about and on behalf of clients should be asked of the legal profession.
8. There is a need for clear guidance from the legal regulators on records ownership, records management and records disposal. At present there is very little.
9. There is a need for better guidance from the legal regulators on confidentiality and legal professional privilege – in particular definitive statements as to whether confidentiality obligations are in fact perpetual or, if not, when they lapse.
10. The legal regulators should define client consent processes which are transparent about destruction and/or archival deposit of client documentation.
11. There is a need for generic templates to be made available to the legal profession when depositing records in archives eg a templated deposit contract agreed with ICO, SRA, ARA and BRA which includes access terms. This template ideally needs to agree legal costs for dealing with access disputes.
12. The changes imminent as a result of the GDPR (eg the requirement for legal institutions to draft and implement retention schedules) need to be more widely circulated within the legal profession.
13. There is a mismatch between the public and private sectors over transparency. The public sector and some parts of the business sectors are leaning heavily towards being more open and transparent; the legal sector is still leaning towards secretiveness. This is a major issue because the legal profession is an important part of our national heritage but is still under-represented in archives.
14. Information risk diminishes over time. TNA usually imposes closure periods of 75-100 years on personal or confidential data.

15. The legal profession is risk averse and out of step with recent trends in both government and business towards transparency, public accountability and community engagement.
16. The legal profession needs to be more aware of its responsibilities around good record keeping and to stop viewing information and records management as a separate overhead to be undertaken as an afterthought, if at all, instead of as an intrinsic part of running an organisation in the same way as Finance or HR.
17. If the legal profession does not facilitate the preservation of records of value we will be left with a major gap in our historical record, undermining the understanding of the importance of legal developments to our nation's history.

Seminar information pack

The following documents were included in a pack as background information for attendees:

The National Archives guideline on data protection and personal information 2016

http://www.nationalarchives.gov.uk/information-management/browse-guidance-standards/?letter=p

Introduction

The purpose of data protection legislation is to ensure the proper use of personal information about living individuals. The legislation imposes obligations on those who hold such personal information, while giving rights to those the information is about – data subjects.

Archivists have a different role in relation to personal data from those who collected the personal data in the first place. Firstly, they do not control the type of data collected, because they were not involved in why, when and how it was originally collected and used for business purposes; secondly, their interest in the personal information lies in its value as a record of its time that can be used in future research, and its current accuracy is therefore not of concern; and thirdly, they have no interest in the future of the individual data subject, only their past.

This means that the activities of archivists can sit uneasily within the data protection legislative field, as at times they are obliged to comply with provisions which were designed for a different purpose. However the Data Protection Act 1998 (DPA), which came into force in March 2000 (amended by the Freedom of Information Act (FOIA) in 2005), does recognise the importance of data being kept for historical purposes, and contains provisions for this to be achieved within the framework of the legislation.

The DPA imposes a duty on those holding personal data to register such data with the Information Commissioner, to comply with eight data protection principles, and to allow individuals to access and, in certain circumstances, to correct data that relates to them. With the implementation of the FOIA, the DPA has been extended in scope so it that it applies to all information about living individuals held by public authorities, whatever the format or structure of the records.

The National Archives, Society of Archivists, Records Management Society and National Association for Information Management produced a Code of practice for records managers and archivists under s 51(4) of the Data Protection Act 1998 which may be of interest.

Archiving personal data for research purposes, s33

The definition of research purposes in the DPA includes processing for historical research purposes. This is an important section for records managers and archivists, as it lays down the conditions with which the data controller of an archive should comply if the archive is to be exempt from compliance with various other requirements of the act.

Without the benefit of such provisions, archiving data could be in breach of the second and fifth data protection principles. The second data protection principle requires that personal data shall only be obtained for one or more specified and lawful purposes and shall not be further processed in a manner which is incompatible with such purpose(s). The fifth data protection principle requires that personal data shall not be kept for longer than is necessary for such purpose(s).

Section 33 provides that processing for research purposes is compatible with the purposes for which the data were collected, and the data may be kept indefinitely if the relevant conditions apply. These are:

- that the data are not processed to support decisions about individuals, and
- that substantial damage or substantial distress is not likely to be caused to any data subject

Personal data can be selected for permanent preservation, and stored, if these two conditions apply, on condition that the other data protection principles are complied with.

Note that The National Archives has registered personal data in transferred records to the Information Commissioner with the special purpose of processing for the purposes of archival preservation.

Closure of personal information

The most common reason for records at archives services to be closed is that they contain personal information about an identifiable living individual and disclosure would breach one of the Data Protection Principles (and consequently is exempt under FOI exemption 40).

Note that the name of a person may not in itself be enough to make the person identifiable and it usually depends on the context in which it appears or the presence of supplementary information enabling a person to be identified.

Usually such information falls within the DPA's definition of sensitive personal data, namely information on a data subject's:

- racial or ethnic origin
- political opinions
- religious, or other, beliefs
- trade union membership
- health (physical or mental)
- sex life
- offences, committed or allegedly committed details of proceedings for offences

The Information Commissioner's Office has issued guidance on what personal information should be considered exempt. Note that not all sensitive personal information must be withheld for the full lifetime of the data subject. The particular content and context of the information may allow earlier access. Guidance on closure periods should be applied on a case-by-case basis.

One difficulty is establishing whether the person to whom the information relates is still alive. In practice, it is usually impossible for a department or archives service to know if an individual is still living and impracticable for them to find out. The Advisory Council has recommended that a lifetime of 100 years should be assumed. Thus if a person is aged 30 in a 1950 record and the information should not be released during their lifetime, the closure period would last until the end of 2020 (open on 1 January 2021).

If a person's age is unknown, estimate the closure period. If it is obvious the person is an adult then the estimated age at the time of the record should be 16. If it is not obvious what age a person is from contextual evidence then the full 100 year closure period should be used, for example, a child who is the victim of crime.

It may be possible from contextual evidence to reduce the closure period, for example, if it is known a person has a professional qualification that requires several years of training or where a person is applying for a benefit such as a pension that has a minimum age. In these circumstances the closure period should be reduced accordingly.

……..

Research exemptions under the Data Protection Act and the General Data Protection Regulation (GDPR)

Data Protection Act 1998 S.33 Research, history and statistics

(1) In this section—

- "research purposes" includes statistical or historical purposes;
- "the relevant conditions", in relation to any processing of personal data, means the conditions—

  (a) that the data are not processed to support measures or decisions with respect to particular individuals, and

  (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

(2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle, be kept indefinitely.

(4) Personal data which are processed only for research purposes are exempt from section 7 if—

(a) they are processed in compliance with the relevant conditions, and

(b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed—

(a) to any person, for research purposes only,

(b) to the data subject or a person acting on his behalf,

(c) at the request, or with the consent, of the data subject or a person acting on his behalf, or

(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

General Data Protection Regulation (GDPR):

Article 5 of the GDPR requires that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or

historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes".

……

Code of Practice for records managers and archivists under Section 51(4) of the Data Protection Act 1998

2007, The National Archives (on behalf of the Crown), the Society of Archivists, the Records Management Society and the National Association for Information Management.

Excerpts from s.4 Responsibilities of archivists (for the full text of the Code see: http://www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf)

RESPONSIBILITIES OF ARCHIVISTS

The purpose of this chapter is to complement chapter 2 by summarising the particular responsibilities of archivists for personal data held by them. Responsibilities common to records managers and archivists have been described in chapter 3.

4.1 Responsibilities

4.1.1 While ultimate responsibility for compliance with the Act is at the corporate level (see 2.1 above) it is likely that the archivist will play a key role in ensuring organisational compliance with the Act. The archivist, like the records manager (see 3.1), should ensure policies and procedures are compatible with the Act, particularly in relation to storage and access.

4.1.2 Archivists will be concerned with two types of personal data: personal data in their own administrative records, such as staff and reader records and correspondence with depositors, and personal data in the archives within their repository.

4.1.3 Archivists often manage the collections of many different organisations and individuals within their repository, and the nature of the agreement made with the depositor or donor will determine the role of the archivist in relation to each collection. The responsibilities of each party in relation to data protection must be clear.

4.1.4 As a general rule archives received by an archives repository can fall into any of three categories:

• Records transferred from within the organisation, which may be a public authority or a private sector body such as a business. Corporate policy should set out the basis on which archives containing personal data will be passed to the archivist and the level of control and responsibilities that will be passed with them. Like the records manager, the archivist may be acting in a "local data manager" capacity (see Annex A) in relation to transferred records

• Gifts, legacies or purchases, the common factor being that ownership of the archives passes to the archives repository or its parent organisation. The data controller will be the organisation of which the archives repository is a part, with the archivist as "local data manager" unless there is explicit provision to the contrary

• Deposits on loan from external sources, whereby custody passes to the archives repository but ownership remains with the depositor or another party, such as a Trust. In such Data Protection Code of Practice August 2007 27 cases the organisation of which the archives repository is a part may become sole data controller or may share that

responsibility with the owner as joint data controllers, or may act merely as a data processor, leaving control wholly in the hands of the owner. Which applies will depend on the terms of the deposit. As a general rule, the more control over access and use passed to the archives repository, the more likely it will be that its parent organisation has acquired data controller responsibilities. A variant of this last option occurs when control passes to the archives repository in whole or in part, but storage is contracted out to a third party which is a data processor. What is vital is that the owner's continuing interest in the records and the obligations of all parties are set out clearly in the deposit agreement. If the terms of deposit are unclear and the current owner is unknown or cannot be contacted, the organisation of which the archives repository is a part should be regarded as data controller by default.

4.1.5 Given the large number of individuals commonly featuring in archive collections, archivists will not be in a position to ascertain whether they are still alive and hence protected by the Act. If it is not known whether a data subject is alive or dead, the following working assumptions can be used:

• Assume a lifespan of 100 years

• If the age of an adult data subject is not known, assume that he was 16 at the time of the records

• If the age of a child data subject is not known, assume he was less than 1 at the time of the records

4.1.6 When researchers obtain copies of personal data from an archives repository they become the data controllers in respect of those copies and must observe the data protection principles, unless they can claim an exemption, for example because their processing is for domestic purposes only, i.e. personal, family or household use. However, archivists cannot control subsequent use of personal data and it is advisable to assume that researchers will be subject to the Act and make them aware of their responsibilities.

4.2 Acquisition and processing of personal data (Principles 1 and 2)

4.2.1 According to Principle 2, personal data should only be collected for one or more specified lawful purposes and further processing should be compatible with those purposes. As a general rule, processing for the purposes of archival preservation can be Data Protection Code of Practice August 2007 28 considered a compatible further use of the data and the special purpose set out at 2.3.7 will apply.

4.2.2 Processing for the purposes of archival preservation is undertaken by reference to the "research exemptions" set out in section 33 of the Act (outlined in Annex B, B4). Personal data may be stored indefinitely as archives for research purposes provided that the "relevant conditions" are observed, namely:

• The data is not processed to support measures or decisions relating to particular individuals, and

• The data is not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject The meaning of "substantial damage and distress" is discussed further at 4.9

4.2.3 When personal data categories (a)-(d) are being processed in accordance with these conditions, there is also an exemption from Principle 5 but the other Principles must be

observed unless the personal data is “eligible data”, (see Annex A), in which case further exemptions apply (see Annex B). The data may be disclosed to third parties for research purposes in accordance with section 33 or to the data subject without the exemption from Principle 5 being lost. (See also 4.9.) Category (e) personal data is exempted from Principles 1-3, 5, 7 and 8. (See Annex A for an explanation of the different categories of personal data.)

4.2.4 All archives repositories acquiring personal data falling into categories (a) to (d) and wishing to undertake further processing must be able to show that there is a “fair” and “lawful” basis for doing so, in accordance with Principle 1 (See 2.2.5–2.2.6). This means looking at the conditions in Schedule 2 and, for sensitive personal data, Schedule 3.

4.2.5 For schedule 2, archivists dealing with public records will be exercising statutory functions under the Public Records Act and so can refer to paragraph 5(b), which relates to processing for the ‘exercise of functions … conferred by an enactment’. Archivists dealing with other public sector records can refer to paragraph 3, which relates to processing ‘in compliance with any legal obligation’ (other than a contract), paragraph 5(c) which relates to processing for ‘the exercise of any functions of … a government department’ or paragraph 5(d) which relates to processing for ‘functions of a public nature exercised in the public interest’. Archivists in the private sector can refer to paragraph 5(d) also, particularly if the organisation admits Data Protection Code of Practice August 2007 29 visitors seeking to undertake research. Another possibility for private sector archivists is paragraph 6(1), which relates to processing that is necessary ‘for the purposes of the legitimate interests of the data controller’ or by third parties to whom the data is disclosed, except where processing would be unwarranted because of ‘prejudice to the rights and freedoms or legitimate interests of the data subjects’.

4.2.6 One of the conditions in Schedule 3 must also be identified for sensitive personal data. Archivists processing sensitive personal data who are unable to comply with any of the conditions specified in Schedule 3 may benefit from SI 2000 No. 417 Data Protection (Processing of Sensitive Personal Data) Order 2000. This sets out additional circumstances in which sensitive personal data may be processed and thereby provides supplementary Schedule 3 conditions. Paragraph 9 of the Order makes lawful any processing which, in addition to satisfying the general requirements that sensitive data are processed lawfully and fairly: “(a) is in the substantial public interest; (b) is necessary for “research purposes” (which expression shall have the same meaning as in section 33 of the Act); (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person.”

4.2.7 Except when they themselves collect data for the purposes of administering their offices, archivists will generally not be expected to inform data subjects of processing they undertake for research purposes because to do so would involve disproportionate effort. The unfairness of not so informing data subjects is minimal where the relevant conditions are observed and records either kept closed for an appropriate period or used only for research which will be anonymised.

4.3 Appraisal (Principle 5)

4.3.1 Archivists involved in the appraisal of records prior to their transfer should ensure that personal data worthy of permanent preservation is identified as soon after creation as possible and scheduled for retention accordingly (Principle 5).

4.3.2 There is a danger that over-cautious interpretation of the Act may lead to the weeding, anonymising or destruction of files containing personal data that would otherwise be passed to the Data Protection Code of Practice August 2007 30 archives repository. An archivist's ability within the Act permanently to retain personal and sensitive personal data for the purposes of research (see 4.2.1) should therefore be made clear to potential depositors. The legislation contains the necessary safeguards for depositors.

4.3.3 When considering the permanent preservation of sensitive personal data for the purposes of research, archivists should give serious consideration to how far this will be in "the substantial public interest". This will mean weighing up whether society as a whole, and the research community in particular, will benefit from preservation of the data for research purposes. All appraisal decisions should be documented as a matter of good professional practice.

4.4 Accessioning

4.4.1 All newly received archives, whether manual or electronic, should be checked to ascertain whether they include personal data covered by the Act, for example a database or a series of case files about named living individuals. Bodies that are not subject to the FOI Acts will find that some manual archives fall outside the Act because they are neither accessible records (category (d) personal data) nor records from a relevant filing system (category (c) personal data).

4.4.2 Bodies subject to the FOI Act should assume that all archives containing personal data about identifiable living individuals are subject to the Act. Archivists in public authorities should note that category (e) personal data in archive collections of private origin may fall within the Act by virtue of being held by a body subject to the UK FOI Act. The position is different for bodies subject to the Scottish FOI Act; personal data of private origin will fall within the scope of the Act only if ownership has passed to the archive repository or its parent body.

4.4.3 When arranging the transfer of archives, archivists should ascertain from the donor or depositor whether they contain data already covered by a notification, whether the data is already exempt from subject access and whether measures have been taken to confirm its accuracy. Transfer documentation should incorporate questions that confirm these points (see examples at Annex C). 4 Assessment of private archive collections to determine whether they fall under the FOI Act is the subject of guidance issued by The National Archives in 2005 - see http://www.nationalarchives.gov.uk/documents/guidance_private_archives.pdf Data Protection Code of Practice August 2007

4.4.4 Transfer and deposit agreements should clarify the responsibilities of the archivist, stating whether the originating person or body is retaining or transferring data controller responsibilities as outlined at 4.1.3. It may be necessary to obtain legal advice to ensure that the wording of these agreements is accurate.

4.4.5 As a general rule, it is simpler to accept only those sets of personal data that are no longer required for current business and hence can be retained for the sole purpose of archival preservation. This is because it will be clear that they are a contemporary not up to date record. However, this may not always be practicable and continued use may prove necessary (see 4.11 for further guidance on this). Notification should accommodate

expected use of the data. It should also be clear to someone consulting the data whether the records are still in active use and have been kept up-to-date, or instead reflect a historical position.

4.9 Third party access to personal data

4.9.1 The Freedom of Information Acts have made significant changes to provision of third party access where bodies subject to those Acts are concerned. The text that follows deals first with access in accordance with the Data Protection Act (4.9.2 - 4.9.6) and then with the effect of the FOI Acts on access to personal data (4.9.7 - 4.9.12). Access in accordance with the Data Protection Act

4.9.2 The Act does not give third parties rights of access to personal data. Access to personal data in archives by someone other than the data subject or the data controller (or his employees) will normally be permitted for historical or statistical research under the relevant conditions (see 4.2). Such access will be subject to closure periods up to a maximum of 100 years, the assumed lifetime of the individual. In administering shorter closure periods or otherwise authorising disclosure of data, archivists should be able to cite conditions in Schedules 2 and 3 as applicable and should consider the following two criteria:

4.9.3 (a) Access must be lawful Principle 1 requires data to be processed lawfully and so, even if the Act seems to provide no impediment to access, other aspects of lawfulness must be considered:

• Statutes protecting the confidentiality of personal information must be respected. For example, the Sexual Offences (Amendment) Act 1992 protects the identity of victims and alleged perpetrators of rape and some other sexual offences during their lifetime. Archivists should check whether any statutory bars to access apply to personal data they propose to release. The former Department for Constitutional Affairs published a report which identifies the main statutory bars Data Protection Code of Practice August 2007 35 that apply.5 It can be seen at http://www.foi.gov.uk/reference/ReviewOfStatBars.htm .

• A duty of confidence may attach to particular records, such as health records, where the consent of the individual is required unless there is an overriding public interest in disclosure. This will necessitate consideration of the way in which the information was first acquired, its nature and age (see 4.9.4), and whether research will make possible the identification of individuals:

• The information made available must not be libellous or obscene

• If the information is held by a public body, the Human Rights Act may make access impossible (see 4.9.12)

4.9.4 (b) Access must be fair Principle 1 also requires data to be processed fairly. Fairness to people about whom personal data are held is the overriding concern of the Act and the guiding principle is when in doubt, withhold the data. The impact of disclosure, including whether it would cause substantial damage or substantial distress, should be assessed, taking into account the following factors:

• The nature of the information must be considered. Some personal information, including some “sensitive personal data”, is comparatively innocuous, some is not. To take medical information as an example: information about hospitalisation for a broken leg 20 years ago is not something people feel a need to keep secret whereas information about treatment

for a mental illness 40 years ago is still considered to carry a stigma and hence is not for disclosure. In both cases the information is “sensitive personal data” under the Act but different judgements as to whether substantial damage or distress are likely to be caused by disclosure can be formed. Another example, not relating to “sensitive personal data”, is information about receipt of public funds. When the funds are received as of right (such as the old age pension or housing repair grants) there are no implications about the income of recipients and hence it is unlikely to be considered embarrassing, whereas when the funds depend on means testing (such as supplementary pensions or social fund payments) receipt is associated with low income and disclosure could be regarded as invasion of privacy and hence unfair to the individual.

• The age of the information may be relevant. The need to provide protection diminishes over time. For example, The report deals with statutory bars within UK legislation. Some of them may apply to information held by Scottish public authorities but any Order under the UK Act to repeal or amend these statutory bars can apply only to bodies subject to that Act. Note that the review did not look at statutory bars in legislation passed by the Scottish Parliament. Data Protection Code of Practice August 2007 36 membership of an extreme political group or party may be of little interest after 20 years and none after 40 and disclosure therefore may not damage the data subject’s reputation or standing in the community. The age and status of the data subject should also be considered as this can affect the extent of distress they might feel.

• Genuine information (as opposed to speculation) already in the public domain because it is a matter of public record should normally be accessible. An example would be conviction for an offence in a court where no restrictions on naming the person apply (although note that a court case file may contain a mixture of information placed in the public domain at the time of the trial and information that was not made public). Potentially distressing information deliberately made public by the data subject should also be made accessible

• The credibility of the data, i.e. its likely accuracy and comprehensiveness, should be considered as this affects whether the good name of the individual is likely to be put at risk by disclosure

• It is impossible to anticipate what research may be done on any particular set of data but, if substantial damage or substantial distress to any individual would be a likely consequence of any research, the data should remain closed. (Note that processing for medical purposes and racial equality monitoring is allowed, see Schedule 3, paragraphs 8-9) 4.9.5 Steps to safeguard the fair and lawful use of data include:

• Explaining to intending researchers the “relevant conditions” that apply to the research use of particular data, including sensitive personal data (see 4.2)

• Requiring researchers to sign a declaration that, as a condition of access to data that might otherwise be closed, they will comply with the relevant conditions and Data Protection Principles (1, 3-4 and 6-8). Application forms to consult specific personal data subject to these conditions should be signed and kept as an audit trail

• Informing researchers that they are responsible under the Act for any processing by them of personal data disclosed to them, including copying, realignment, transmission abroad and publication (see 4.1.6)

• If researchers are bound by a sectoral code of practice or particular employer requirements, e.g. guidelines produced by a university ethics committee, making access conditional on the researcher undertaking to comply with that as well as with any special conditions applying to specific sets of personal data. This is particularly relevant if he intends to Data Protection Code of Practice August 2007 37 publish or to make use of the data for purposes other than private research

4.9.6 Note that if researchers breach the terms of any access conditions and publish name-identifiable information, the exemption from section 7 will be lost but not the general exemption for processing for research purposes.

……..

Legal Records at Risk Guideline 4: advice to legal institutions on confidentiality and research access to records

Legal records and historical research

Private sector "legal" records have never been collected systematically in the UK other than by a very small number of specialist archives[1]. Collecting in the public archives sector has tended to be ad hoc (ie as and when individuals or legal bodies such as law firms decide to clear out some of their records). As a result research using legal records is inevitably weighted towards the pre-twentieth century study of government policy, legislation and the courts, producing a historical picture of the UK's legal framework and legal services which is skewed towards the policies and actions of central government. One reason for this dearth of private sector legal records may be the legal profession's legitimate concerns about record confidentiality and a mistrust of or misunderstanding about how archival repositories respect and manage this, plus the reluctance of archives to accept deposits of records with unfeasibly long closure periods. These issues, and how to resolve them, are discussed below.

Legal records and confidentiality

The Legal Records at Risk project seeks to broaden the concept of "legal" records from the traditional definition of them as court records or formal documents such as deeds to the business records of private sector institutions with a connection to the law such as law firms, barristers' chambers, regulators, membership bodies, pressure groups and educational bodies as well as to legal records created and held by businesses, companies, charities etc. "Business records" will include corporate governance records, policy and procedures files, marketing, public relations and accounting records; as such they will be bound by the usual conditions of commercial confidentiality and the Data Protection Act. In this respect the records of a legal institution should not be treated any differently to the records of other private sector organisations when seeking to make them available for research and so there should be no particular confidentiality problems in depositing them in archives. There is, however, one exception to this rule as follows.

Legal professional privilege and client confidentiality

[1] Such as the Archives of the Inns of Court, the Law Society and the Records of Legal Education Archives. Not to be confused with the almost universal practice followed by institutions of depositing their non-current records en masse in a warehouse, basement or lower-tier server for indefinite storage.

All client information is held by legal institutions under a long-term obligation of confidentiality[2]. Legal service providers are bound by their professional codes of conduct to keep client and complaints information confidential (see **Appendix**). This may be the primary reason both for the reluctance of legal providers to make *any* information about their work available for research despite the fact that many of their records will not be subject to client confidentiality. It may also explain why archive repositories may not wish to collect and store such records where unfeasibly (in archival terms) lengthy closure periods are demanded.

How long does client confidentiality last?

The question is whether this guarantee of confidentiality is in perpetuity or for a limited (in archival terms) period. None of the Codes of Conduct listed in the **Appendix** specify a length of time, so the next question is whether there is a tacit assumption of confidentiality in perpetuity, and whether this has ever been challenged.

'Actionable Breach of Confidence' is a useful base-line for discussion. An action for breach of confidence can only be brought by a deceased person's personal representative – ie executor or administrator. Once that person can be proved or presumed dead (say 82 years after death of the data subject, if we assume that a personal representative must be at least 18 – though 16 might be safer), there is no legal risk in releasing the information. This may be useful in dealing with the confidentiality for individual clients but is more problematic for companies, which do not "die" unless they are wound up or dissolved. It is not an insuperable barrier to eventual release of client information but it may well be an obstacle too far for archive repositories, which as a rule simply cannot afford to sit on material for hundreds of years until they can make it available.

Legal bodies presumably have a responsibility not to transfer client information to a third party unless and until the files are no longer subject to an obligation of confidence (ie the client has died and the time limit for all legal actions has expired or the company has been dissolved/wound up), when they can legally be destroyed or sent to an archive repository.

It appears to be easier to say that this responsibility implies confidentiality in perpetuity than to make decisions as to when client files become redundant and can safely be disposed of. Yet client files cannot be held indefinitely, not least because where individual clients are concerned such retention would be in breach of the Data Protection Act[3]. LRAR suggests, therefore, that legal institutions and practitioners look afresh at the way in which they manage their client files and make carefully considered decisions as to disposal.

Archives and confidentiality

[2] The 2004 Clementi Report *Review of the regulatory framework for legal services in England and Wales* describes confidentiality thus (p.23): "The codes of conduct of the legal professional bodies generally require lawyers to keep clients' affairs confidential. Communications between a client and his lawyer may be subject to Legal Professional Privilege (i.e. certain communications between a client and legal adviser in the context of obtaining legal advice or assistance are protected from disclosure, even in legal proceedings)."

[3] See Schedule 1 and the 8 Data Principles, in particular Principle 5: "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

All archival repositories[4] have well developed techniques for dealing with 'sensitive' records, including closure periods and conditions on access and use; they operate under strict confidentiality guidelines and follow The National Archives' advice to close all records for at least 20 years and personal data for 100 years[5].

Deposit agreements: any legal institution or individual depositing records with an archives can also stipulate their own confidentiality requirements (though the archives, equally, can refuse to accept records with an unfeasibly long closure period). Where a private sector organisation deposits records in an archives an agreement is always drawn up specifying the length of time the records should be closed to public access unless the depositor is happy with the archives' own standard access rules.

Standard closure periods based on confidentiality applied by archival repositories, after which records may be made available for research, are as follows:

- Records in general: all records held by an archives are closed for 20-30 years other than material already in the public domain or for which permission for earlier access has been given by the depositing organisation/individual.
- Commercial confidentiality: usually assumed to expire after 20-30 years, unless a specific stipulation is made by the depositing body that it should be closed for a longer period.
- Personal data: the Data Protection Act specifies that the term "personal data" only applies to the data of living individuals, so archives close such data for 75-100 years as recommended by The National Archives. Once the data subject is deceased or presumed deceased the Act no longer applies. In certain circumstances personal data may also be examined for bona fide research purposes provide a legally binding guarantee of anonymisation is signed, or research bodies may redact personal data to make it available[6]. In other words, client confidentiality is not an insuperable barrier to making client data available for research.

There is, therefore, no reason for any legal institution to be concerned that an archive repository will not professionally manage access to deposited records.

Appendix to Guideline 4: Institutions specialised to law: Confidentiality Codes of Conduct and Practice Guidelines

The Bar: the Bar Standards Board Handbook states in S12: "The regulatory objectives of the Bar Standards Board derive from the Legal Services Act 2007 and can be summarised as follows…that the affairs of clients are kept confidential" and rC106: "All communications and documents relating to complaints must be kept confidential".

Solicitors: the SRA Code of Conduct 2011 states in Ch 4 Client confidentiality: "firms are required to have effective systems and controls in place to identify risks to client

[4] The term "Archival repositories" in this guideline refers to places where archival records (ie collections of records selected for long-term preservation as evidence of the activities of organisations or individuals) are stored, preserved and made accessible. The term does not refer to the mass storage of information in 3rd party records stores, basements or lower tier servers pending disposal.

[5] TNA Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act

[6] Section 33 of the Data Protection Act 1998 refers

confidentiality and to mitigate those risks…... Protection of confidential information is a fundamental feature of your relationship with *clients*. It exists as a concept both as a matter of law and as a matter of conduct. This duty continues despite the end of the retainer and even after the death of the *client.*"

Arbitrators: institutions have their own rules eg Article 30(1) of the Rules of the London Court of International Arbitration states: "Unless the parties expressly agree in writing to the contrary, the parties undertake as a general principle to keep confidential all awards in their arbitration, together with all materials in the proceedings created for the purpose of the arbitration and all other documents produced by another party in the proceedings not otherwise in the public domain - save and to the extent that disclosure may be required of a party by legal duty, to protect or pursue a legal right or to enforce or challenge an award in bona fide legal proceedings before a state court or other judicial authority."

Mediators: the Chartered Institute of Arbitrators' Practice Guideline 1: Confidentiality in Mediation states "Save as required or permitted by law… the Institute, the parties, their representatives, their advisors and the mediator(s) shall keep confidential all information (whether given orally, in writing or otherwise) produced for, or arising out of or in connection with, the mediation passing between any of the participants and between any of them and the mediator made for the purposes of the mediation, including the fact that the mediation is taking place or has taken place…The mediator's duty to protect the confidentiality of the mediation proceedings commences with the first communication to the mediator, is continuous in nature, and does not expire upon the termination, for whatever reason, of the mediation under Rule 11. The mediator's duty extends to all information relating to the mediation proceedings, even indirectly, such as previous invitations and/or negotiations leading to mediation, terms of the agreement to mediate, appointment of mediators and performance, or non performance, of the settlement agreement. All records, reports, or other documents received by a mediator, as well as all notes taken by the mediator during, with reference to, or for the purposes of, the mediation should be returned to the parties or kept secure until no longer needed for any purpose relating to the mediation and then destroyed."

Conveyancers: Outcome 3.6 of the Council for Licensed Conveyancers' Code of Conduct requires that: "Clients' affairs are treated confidentially (except as required or permitted by law or with the Client's consent)".

Notaries: Ch. 17 Recordkeeping and file storage of the Master of Faculties Code of Practice states: **"**A notary's records are as a general principle confidential [Practice Rule 23.6]".

Patent and Trade Mark Attorneys: the Chartered Institutes of Patent Attorneys and Trade Mark Attorneys have produced joint Business practice guidance containing many references to the need to safeguard clients' confidential information, including information of clients for whom the attorney no longer acts.

Will writers: the **Institute of Professional Willwriters'** Code of Practice **states: "**Members shall act with independence and integrity, maintain proper standards of work and keep the affairs of the Client confidential" [**S.5.1].**