Data Protection and Research Data: Questions and Answers

Andrew Charlesworth, University of Bristol Law School

Abstract: Research data containing 'personal data' will be subject to UK data protection law, which is overseen by the Information Commissioner's Office (ICO), under the Data Protection Act 1998 and secondary legislation. What obligations does the law place on you as a researcher? This document sets out to provide guidance with regard to that question and some others you may have.

NB: Details of particular circumstances can make a major difference, so conclusions reached in an individual case might differ from those suggested here. If in doubt, seek advice from your Research Ethics Committee or Data Protection Officer. This document does not constitute, and should not be construed as, legal advice.

Contents

Prepared for JLIS (JISC) 2014. Minor amendments 2016.

Introduction

In the UK, the Data Protection Act 1998 (DPA 1998) currently regulates the use of information that relates to an identifiable living individual, as well as information which, when combined with other data accessible to the researchers, would permit the individual's identification (personal data).[1] It places obligations on those who are responsible for determining the purposes for which the personal data is processed (data controllers), and gives rights to those who are the subject of that data (data subjects). Processing of personal data for research purposes falls under the general provisions of the Act, but some specific research-related exemptions are provided.

We assume that you are a researcher who works for, or with, or in a university or research institution, and you are concerned about the application of the UK data protection legislation to the collection, storage, use transfer and disposal of your research data, including requests for access to that data by data subjects (subject access requests) and third parties.

Undertaking research that involves processing personal data will normally bring you into contact with your institutional research ethics committee (RECs) as such research is usually considered as research with human subjects. The boundary between the legal requirements of the DPA 1998, and the ethical principles that your REC use to guide their processes overlap, although those legal requirements and ethical principles may have differing objectives and may not map precisely (see Further Information below). Different institutions, and indeed disciplines, may also work to different ethical understandings, e.g. social science researchers may have rather different understandings of the nature and scope of ethical review than researchers in the bio-medical sciences. This Q&A will concentrate primarily upon the legal issues, but will note where legal and ethical approaches sometimes diverge.

This publication is primarily designed to be accessible, and so may over-simplify complex issues. We assume there will be two primary contact points in your institution who can advise on this complexity: specific institutional 'DP Practitioners' e.g. Data Protection officers, Information Rights officers, Information Compliance officers etc.; and institutional research ethics committees. Most institutions will have a Data Protection link on their homepage. This link will usually include a data protection policy or guide and details of your DP Practitioner. DP Practitioners will be crucial in responding effectively to subject access requests (SARs). Additionally, your institution may have specific policies and procedures that you are obliged to follow when using personal data in your research, and you are advised to investigate those at the project development stage, and before applying for funding.

A survey of existing practice at Universities indicates that, when designing a research methodology, it is usual for researchers to initially liaise with their REC to identify and address the DP issues it raises. However, where your research appears to pose a significantly higher level of risk, or if you receive a subject access request, or a request from a third party for information collected during your research that includes personal data (including Freedom of Information (FoI) and Environmental Information (EIR) requests), you should always involve your DP Practitioner (often also your FoI/EIR expert).

Remember, this FAQ is not advice; it is simply guidance aiming to help you have a better-informed discussion with your REC or DP practitioner, or to consider steps you might take in advance.

Related issues outside the scope of this document, but on which your REC or DP practitioner can advise, include issues relating to application of the Human Rights Act 1998, the law of confidence, and specific commitments made to sponsors under contract, or made via consent forms to research subjects.

---

[1] The EU General Data Protection Regulation (Regulation (EU) 2016/679) entered into force on 24 May 2016, and will apply in all Member States from 25 May 2018. It replaces the EU Data Protection Directive and national legislation implementing that Directive, including the UK Data Protection Act 1998, from 25 May 2018 onwards.

1. What is 'personal data'?

Under the Data Protection Act 1998 (DPA 1998), 'personal data' means information that relates to an identifiable living individual, as well as information which, when combined with other data accessible to the researchers, would permit the individual's identification. This includes any expression of opinion about the individual and any indication of the intentions of the data controller, or any other person, in respect of the individual. While for many types of research it will be obvious when you are processing personal data, the ICO has provided detailed guidance in Determining what is personal data (2012).

Despite the initial distinction made by the DPA 1998 between manual and computerised processing of personal data, later amendments by the Freedom of Information Act 2000 concerning processing by 'public authorities' (which term includes virtually all UK universities) mean that for the purposes of the DPA 1998 and university research, it is appropriate to assume that all manual and computerised processing of personal data will fall under the Act. See Millard, 2011.

Further issues may arise in specialised areas of research, for example if you are researching in large data sets concerning human subjects. 'Big data' research suggests that in certain circumstances processing of data which appears on its face to be anonymous (see Q4, 4a, 4b) may allow researchers (and third parties with access to resulting research datasets) to identify individuals through data 'triangulation' and reconciliation of multiple sources. When developing such research (e.g. text and data mining projects), it is advisable to consider the risk of de-anonymisation, the impact that this might have on individuals, and how possible negative impacts might be prevented or ameliorated.

2. Is everyone potentially a 'data subject'? What about children, the elderly and the deceased?

A data subject is simply an individual who is the subject of personal data. Thus, from the time of their birth to the time of their death, a person will be a 'data subject' where another party is collecting personal data about them. Whether a person is capable of exercising their rights as a data subject is another issue. For example, the DPA 1998 has no minimum age requirement. Children can thus exercise their DP rights provided they are capable of understanding the nature of those rights. How you handle DP issues in relation to children involved in research projects requires sensitivity to the point at which a child is mature enough to make their own decisions, and must respect those, including where a child revokes a consent made on their behalf earlier by a parent or guardian. Equally elderly and vulnerable data subjects may (or may not) wish a third party to exercise their rights for them – it is up to the third party to provide evidence of their right to do so. Deceased persons are not data subjects, as personal data refers to living individuals. However, commitments made to data subjects, e.g. that their identity will not be disclosed, may remain enforceable by their estate after they have died.

From a related FoI perspective, the exemption for personal data in the Freedom of Information Act ceases on death of the data subject (in Scotland there is a 100 year FoI exemption for a deceased person's medical records), but disclosure of, or access to, the deceased person's personal data will require consideration of third party personal data, e.g. that of relatives, and of any duty of confidence between researcher and deceased. You may also need to consider whether personal data that was accessible to you by virtue of consent of the data subject will remain accessible after their death, if their personal representatives refuse access, or there is no personal representative to give permission: e.g. medical records.

3. What is the difference between 'personal data' and 'sensitive personal data'?

The DPA 1998 makes a distinction between 'personal data' and 'sensitive personal data'. Processing of 'sensitive personal data' is subject to more stringent rules and generally requires more careful consideration. Sensitive personal data is defined as personal data relating to the data subject's:

- racial or ethnic origin
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- membership of a trade union,
- physical or mental health or condition,
- sexual life,
- commission or alleged commission of any offence, or
- involvement in criminal proceedings for any offence or alleged offence committed by them, including outcomes such as judgement and sentencing.

If you intend to process sensitive personal data in the course of your research, or there is a possibility that sensitive personal data may be processed, this will impact upon the conditions you will need to satisfy to carry out that processing lawfully, the justifications you may need to provide to your REC, and the uses to which the research data and research outputs can be put. (See Q8)

It should be noted that the Act does not consider the context of the data processed. For example, if you are interviewing research participants in government about the role of trade unions in ensuring fairness for people with disabilities, if a participant has a disability or is a trade union member, and this is recorded, then the Act applies, e.g. "Mr X, Deputy Chair of the Print Workers Union's Disability Rights Committee", or "Ms Y, Minister for Trade who has [particular disability]. It does not matter that the interviewees occupy public positions/roles because of disability or union membership. Nor does it matter that the focus of the interviews is an official process. The default position is that the data is 'sensitive personal data': the Act and secondary legislation then provide conditions under which it is permitted to process that data.

4. If my data is anonymised, do I need to consider data protection issues?

Data which cannot be linked to an identifiable living individual is not personal data, as defined by the DPA 1998, and thus in principle falls outside the DP regime. However, until data is anonymized, it will be considered 'personal data' for the purposes of the DPA 1998. Additionally, certain types of research (e.g. data mining and matching) may result in anonymous data becoming linked or re-linked to an identifiable data subject. Risks relating to the possibility of de-anonymisation should thus be considered where appropriate.

4a. What is the difference between 'anonymous' and 'pseudonymous' data?

The issue of anonymisation is a complex one. Technically, data is only anonymized when an individual can no longer be identified from it. Thus a dataset that has been 'link-coded', with names and other key identifiers removed, but which is linked to a separate file held by, or accessible to, the researcher which enables individual research subjects to be identified (including, potentially, consent forms) is not anonymized – such a dataset would usually be considered to be 'pseudonymised'. Both raw datasets containing names and other key identifiers, and pseudonymised datasets capable of linkage to identifying data held by the data controller, will be subject to the DPA 1998.

A key principle of data protection is 'data minimisation', i.e. if data is not collected, the risk of its future misuse is automatically reduced. In the research context, you might consider for example, whether satisfactory research outcomes can be achieved without collection of personal data or with only minimal collection of personal data: e.g. your research may not require a data subject's date of birth, just their age range, or just the first part of their postcode rather than their full address.

There may be good reasons why a research dataset containing personal data is not fully anonymised e.g. where researchers wish to undertake long term studies with the same research subjects, or where anonymity would prevent other researchers from testing the validity of the data. Additionally, fully anonymising data may be difficult to achieve with certain types of dataset, for example if the research context is such that even without obvious identifiers like a name or address, an individual may still be identifiable to researchers from the data processed, or in combination with other data that they hold; or identifiable to third parties from the data processed and information or knowledge already available to the public. In such cases, you must ensure that the data is processed in accordance with the DPA 1998.

4b. How can I anonymize my research data sufficiently for data protection purposes?

It is useful to think about the issue of anonymisation in terms of both the original research dataset, and research publications drawing upon information from the original dataset.

In datasets held by you, data will be effectively anonymised if all data that would allow you to identify an individual data subject has been destroyed: if you can identify them the data is personal data and falls under the DPA 1998.

In research outputs that you publish, data will be effectively anonymised if, on the balance of probabilities, individuals cannot be identified by third parties cross-referencing the 'anonymised' data with information or knowledge already available to the public. The data disclosed will not be personal data and will not be covered by the DPA 1998.

Common Services Agency v Scottish Information Commissioner [2008] UKHL 47
Department of Health v Information Commissioner [2011] EWHC 1430 (Admin)

Detailed guidance on good practice in anonymisation has been produced by the Information Commissioner's Office in Anonymisation: Managing Data Protection Risk - Code of Practice (2012)

5. Who is the 'data controller' for my research?

All UK universities will have notified the UK Information Commissioner's Office (ICO) that they wish to be included on the register of data controllers. In that notification they will include all the purposes for which they intend to process personal data, this will normally include a purpose covering research in any field, including market, health, lifestyle, scientific or technical research.

Under such a notification, where you are conducting research in the course of your employment, or in the course of your studies, then your institution will be the responsible data controller for personal data processed for that research. You will be considered as part of the data controller for the purposes of the DPA 1998.

If you hire a third party to process data for your research, e.g. a transcription service to transcribe audio tapes of interviews, they will be a 'data processor'. It is the responsibility of the data controller to ensure that a data processor handles research data in conformity with the law. You should ensure that you have a contract with such a third party that meets your institutional requirements for the handling of personal data.

Where you are conducting independent research, which is neither in the course of your employment or studies, then you will be the data controller for any personal data processed for that research, and you are likely to need to make your own separate notification to the ICO.

5a. Where do I find my institution's DP Registration Number/Data Protection Register entry?

The ICO publishes the complete Data Protection Register on line. You can search for your institution's Registration Number and Register entry at:

http://ico.org.uk/esdwebpages/search

5b. What do the terms 'joint data controller' and 'data controller' in common mean?

If you share personal data with another researcher at another university for the same purpose (e.g. a joint research project) and your institutions will be jointly responsible for the processing they have carried out for that purpose, then the two institutions would be 'joint data controllers'.

If you share personal data with another organisation for different purposes, and your institution and the other organisation remain individually responsible for the processing they have carried out for their respective purposes, then the two institutions would be 'data controllers in common' for that data.

5c. If I am processing personal data as part of a collaborative research project, which institution is the data controller?

The answer to this question depends on how your relationship with the other institutions is structured. If they are processing data for a purpose determined by you, and they have no role in determining the purpose or methods of processing, then your institution will be the data controller and they will be data processors. You will be responsible for ensuring that the other institutions process the data in accordance with the DPA 1998 and, as data controller, your institution will be liable if they do not. You will need to ask your DP practitioner about Data Processor contracts.

If the institutions are processing personal data under a jointly agreed purpose and methodology they will probably be joint data controllers.

If you are collaborating with other institutions in collecting particular personal data, but you are then utilising the data for different purposes, your relationship may be one of data controllers in common.

In the case of both joint controllership and controllership in common you will need to ask your DP practitioner about Data Controller agreements, or appropriate clauses for a consortium agreement, including processes for handling SARs (Q16-19).

5d. If I receive personal data for research purposes collected by a 3rd party (e.g. a police force) for their purposes, who is the data controller?

If you are supplied with personal data by a third party like a government body or a police force, it is not unusual to find that they are unclear on your respective positions under DP law. In such circumstances you may be asked to sign a "data processing agreement", which states that the third party is the data controller and you are a "data processor". In fact, unless you are processing the personal data on behalf of that third party, you cannot legally be a 'data processor' – if you are determining the purpose for which the data is processed, i.e. research which is not commissioned by the third party, then you are a data controller as well. If you and the third party are processing the data for different purposes, you are 'data controllers in common', and you are both responsible for your respective processing. You cannot contract out this responsibility under the law.

It is in the best interests of you and your institution that the relationship between you and the original data controller is accurately characterised and an appropriate agreement agreed between the parties. Failure to do so may leave both you and the supplier of data misinformed about your respective liabilities in the event of a breach of the DPA 1998, and lead to inadequate analysis and audit, by your institution, of the data handling processes and risk amelioration strategies appropriate to the data to be processed. Any such agreements should automatically be referred to your DP practitioner. You should not sign any DP agreement yourself; it should be signed by the properly authorised person in your institution.

Some organisations will refuse to permit the reuse of their data for research purposes unless you agree to their "data processing agreement." If your DP practitioner cannot persuade them that they are mistaken in their belief, you may have to sign the agreement in order to carry out the research. Regardless of the documentation, in such circumstances you should assume that, in the event of a breach the ICO may 'look

behind the veil' of the agreement and deem both parties to be data controllers. As such, it is sensible to operate on the assumption that your institution will be liable if there is a breach of the DPA 1998, and organise your project so as to be able to demonstrate that you have acted as a responsible data controller.

5e. Can I take my research data with me when I move to a new institution?

If you have taken appropriate steps when collecting research data from data subjects, data protection law should not prevent you from transferring it, or seeking access to it, when you leave one research institution for another. If you are using consent as your condition for processing the personal data (see Q7 & 8), you might consider whether the consent sought should explicitly cover transfer of the personal data between research institutions. If you are not using consent as a DP condition (bearing in mind that RECs will usually expect informed consent to be obtained for ethical reasons, see Q7b), you may still need to decide whether it is necessary to inform the data subjects of any transfer (see Q9a). Your original institution will also wish to ensure, as data controller, that when they are permitting the transfer of personal data to another entity (i.e. your new institution), that entity is both willing and capable to act as data controller for the data. It is worth noting that there may be other problematic issues to consider, such as intellectual property rights.

6. What does 'processing' mean? Is it just to do with computers?

Processing is defined as 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data.' In practice, if you collect, record, organize, store, adapt/alter, retrieve, consult and use, disclose by transmission/dissemination, align/combine, block, erase or destroy personal data, you are processing it. The breadth of the definition means that the full lifecycle of personal data used for research purposes, from its collection, through to either its destruction or anonymisation, is considered 'processing' for the purposes of the DPA 1998, whether on paper or in electronic form.

7. What are the basic rules for processing 'personal data'?

You must process personal data in accordance with the DPA 1998. The 8 'Data Protection Principles' provide a basic framework for compliance, they are:

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

For you to process personal data fairly and lawfully, issues such as how the data is collected (i.e. were data subjects deceived or misled as to the purpose of the processing), and the information you will provide to data subjects (e.g. who is the data controller, the purpose for which it is to be processed, any information especially relevant to the particular processing, third parties to whom the data may be supplied) must be considered.

Additionally, the DPA 1998 sets out 6 conditions for processing of personal data: you must meet at least one of these before the processing can be considered fair and lawful. Two of those conditions are usually appropriate for researchers:

- the data subject has given their consent to the processing;
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or by third parties to whom the data are disclosed, unless it would prejudice the rights and freedoms or legitimate interests of the data subject.

For most research projects involving personal data, consent would be the normal condition under which empirical research is conducted (See Q7), but if the nature of your research makes it impracticable or otherwise undesirable to attempt to seek/obtain such consent, you could consider establishing a reasoned case that the processing is necessary for the purpose of a legitimate interest, and would not unfairly damage the interests of the data subjects. This would provide an alternative condition for the conduct of research.

The ICO suggests that where a condition specifies that processing must be necessary for the purpose stated; you should be able to show that it would not be possible to achieve your purpose(s) with a reasonable degree of ease without the processing of personal data. Where you could achieve, with a reasonable degree of ease, a purpose using data from which the personal identifiers have been removed, that would be the more appropriate course of action.

7a. What should I tell data subjects about why I'm collecting their data?

When collecting data from research subjects it will normally be expected for you tell people who you are, the name of the institution that will hold the data, what you are going to do with their information and who it will be shared with. However, you may wish to tell them more than this, e.g. information about their rights of access to their personal data, or your arrangements for keeping their data secure. If you think the person would be surprised by a potential use of their personal data by you, you should make a point of explaining it. Providing such information will normally be expected as part of the process of obtaining 'informed consent' for ethical purposes: it will also ensure that information is collected and used fairly for data protection purposes. It is good practice to try to put yourself in the position of the people you're collecting information about, e.g. information notices should be written taking into account the likely language skills and reading levels of the average member of the research subject cohort, and should not resort to legal or academic jargon.

Simply telling most research subjects that "your data will be processed in conformity with the DPA 1998" is pointless. Unless they are data protection experts, research subjects will often have little idea what this means either in terms of their rights or of your obligations. That is inadequate for both ethical and legal purposes.

Detailed guidance on privacy notices has been produced by the Information Commissioner's Office in Privacy Notices: Code of Practice (2009).

RECs will usually expect that you will provide research participants:

- Who you are and your institutional affiliation;
- Who, if anyone, is funding the research;
- What you are asking the participant to do or provide (and how long this will take);
- That participation is voluntary and that participants can withdraw from participation at any time (although you should be careful to spell out what this means in practice, ie, do participants have the right to withdraw any data they have already given you? Up to what point in the research process will this right hold good?)
- How you plan to store the data (including details on any anonymisation process);
- What you will do with the data (including details on how it will be used in any subsequent publications);
- What will happen to the data once the research is concluded (i.e. secure archiving or destruction). This may also be influenced by external considerations, such as Open Access requirements.

It is important that prospective participants understand the information being conveyed to them in order to obtain their consent. Materials you produce for the purpose of informing research participants should be

appropriately drawn up for those who have poor, or non-existent, levels of literacy, or for whom English is not their native language:

Based on your assessment of the characteristics of their research participants, you should provide an assessment of whether particular difficulties or risks may arise in the provision of appropriate information about the research, and if so, how you intend to convey your information to facilitate understanding, e.g. written documentation might be supplemented with audio and/or visual aids, language barriers might be addressed by the use of an intermediary who has the necessary language skills to ensure effective communication etc.

7b. Why does my REC want me to get informed consent from my research subjects when I'm not using consent as a DP condition?

As we've already noted (Q7), consent is not the only DP condition under which personal data can be processed, so if you can satisfy another condition applicable to research, this is not a barrier to your research. However, prior informed consent is seen as a key component of most human subject research, and your REC may be reluctant to grant ethical approval to a research methodology which does not seek prior informed consent. However, there are circumstances where a REC may accept you delaying informing research subjects about your collection of research data, where informed consent may be obtained for ethical purposes without a formal recording, or in rare cases where obtaining informed consent is simply not possible e.g. seeking consent itself poses a risk to research subjects. It is essential to consult your REC in advance in circumstances where you plan not to seek prior informed consent.

Detailed guidance on consent and ethical approval has been produced by the UK Data Archive in the Consent and Ethics section of their website.

7c. If I will be processing personal data obtained from a third party, what obligations do I have to check that it has been obtained in an appropriate manner?

The answer to this will depend on issues such as: where and when the data was collected, what information was provided to data subjects, the expectations of data subjects about how their data would be used, the potential impact of reuse on data subjects' rights and freedoms, the importance of the data to the research and the importance of the research to the public interest. Whether you can use the data will depend not just upon the position at law, but also upon your institution's ethical viewpoint. For example, if you receive recent data from an overseas institution where you know that written consent was not obtained and/or the collector was in a position of authority relative to the participants at the time, regardless of the DP position, it is unlikely that your REC would consider the data collection to be ethical.

Where you reuse data collected by a third party for research purposes, you have a degree of exemption from some DP rules (See Q9), but you still have obligations to data subjects (See Q9a, Q10), including the primary obligation to process their data 'fairly' (Q6). If you know the data was not obtained fairly, then by definition you are not in conformity with the DP Principles. It would be reasonable to expect you to have engaged in at least some investigation of the circumstances in which the personal data was obtained.

Where you are using historical personal data collected at a time prior to DP legislation and/or when ethical standards for collection of research data were different, you should still decide prior to processing whether research use of the data is fair, whether data subjects could reasonably be informed of the reuse of their data, and what risks the proposed reuse poses for data subjects. It is good practice to keep a record of your decisions and the reasons for them.

Where you are receiving personal data as part of a research consortium, it will be expected that you have ensured that your partners will be collecting the data in conformity with both relevant DP law and ethical practice. Additionally, If you are a primary investigator/lead institution in a multi-partner research project, funders may require you to ensure the data protection arrangements of your partners and any service

providers are appropriate, even if you are satisfied that your home institution won't handle any personal data.

7d. I am carrying out covert or deceptive research; do I have to tell data subjects that I'm collecting data about them?

Covert research is where you collect research data without the consent or knowledge of research participants or subjects. Deceptive research involves the deliberate deception of participants, where you don't reveal the true purpose of the study (or reveal it only after the study is completed). Both forms of research are controversial, not least because neither involves obtaining prior informed consent from research participants.

The DPA 1998 permits a delay in disclosure of the information you should provide to data subjects as long as such disclosure takes place as soon as practicable after the time you first process the data. Clearly, with covert or deceptive research, such disclosure will not take place during the data collection phase, but if practicable should take place as soon as the research methodology permits.

Even where the DPA 1998 permits the covert or deceptive methods to be employed, RECs may refuse to approve such research, or if it is permitted, may require you to clearly identify:

- how the covert or deceptive methods will be employed;
- why other approaches cannot be utilised to collect the data;
- what post-collection information provision and consent processes will be utilised, and why e.g. participant, proxy or community debriefing; provision to participants of the LREC's contact details; participant ability to provide informed consent or to withdraw data.

It is essential to consult your REC in advance in circumstances where you plan to undertake research with human subjects using covert or deceptive methods.

7e. I'm lurking in an Internet chat room; do I have to let all the participants know I'm recording their conversations?

Disappointingly for those seeking a definitive answer to this question, both legally and ethically the answer is 'it depends on the context'. The Internet is increasingly a site for research, and studies of and on the Internet cut across all academic disciplines. Indeed, the term 'Internet research' covers a wide range of technologies, devices, capacities, uses, and social spaces. Examples of Internet research with DP implications include:

- collecting data or information, e.g., through online interviews, surveys, archiving, or automated means of data scraping;
- studying how people use and access the internet, e.g., through collecting and observing activities or participating on social network sites, listservs, web sites, blogs, games, virtual worlds, or other online environments or contexts;
- using visual and textual analysis, semiotic analysis, content analysis, or other methods of analysis to study the web and/or internet-facilitated images, writings, and media forms.

The temptation with much Internet data is to argue 'But the data is already public…', this overlooks both the legal requirement that personal data must be processed not just 'lawfully' but also 'fairly', and the ethical principle that, as far as possible, researchers should avoid causing harm to their research subjects. Your REC will almost certainly want you to consider the specifics of your project, including its risks to data subjects and its social benefits, in addition to considering the practicality of communicating information about your research to the subjects of that research for DP purposes.

A good discussion of this topic can be found in:

AoIR, Ethical decision-making and Internet research: Recommendations from the AoIR ethics working committee (2002)

AoIR, Ethical decision-making and Internet research 2.0: Recommendations from the AoIR ethics working committee (2012)

8. Are the rules for processing 'sensitive personal data' different?

We have already noted that the DPA 1998 makes a distinction between 'personal data' and 'sensitive personal data' (Q3). You may process 'sensitive personal data' if you meet one of the conditions for processing personal data (Q7) AND one of 10 additional conditions. Four of these additional conditions are likely to apply to researchers:

- the data subject has given their explicit consent to the processing of the personal data;
- the personal data has been made public as a result of steps deliberately taken by the data subject;
- use of the data is necessary for medical research undertaken by a health professional, or a person owing an equivalent duty of confidentiality.
- use of the data is in the substantial public interest, necessary for research purposes and neither supports measures or decisions with respect to any particular individual, nor is likely to cause substantial damage or substantial distress to any person.

The first condition appears to be the normal basis on which non-medical research involving the processing of sensitive personal data proceeds. For the purposes of the DPA 1998 there is no requirement that 'explicit consent' need be in written or recorded form (although written or recorded consent will provide the best evidence that consent was actually given explicitly).

It may not always be practicable or possible to obtain explicit consent for the processing of sensitive personal data (for example, a large-scale study of case files held in court archives) in which case the recourse to the fourth condition may be appropriate. If you can demonstrate that your methodology and use of the data meets its requirements, then you may process the sensitive personal data.

8a. What is the 'substantial public interest'?

It is unlikely that simply stating that you are conducting 'research' will be sufficient to meet the requirements of the "substantial public interest" test - rather, in cases involving sensitive personal data, a case for "substantial public interest" should be explicitly made out. The Scottish ICO in Decision 021/2005 *Collie and the SCA for the Scottish Health Service* (2010) noted "the very high tests required for these conditions to apply". The rules on notification of data subjects (see Q9a), will also apply where research is carried out on an existing dataset containing sensitive personal data.

Again, archived data which has been fully anonymized (e.g. by destruction of link codes, or removal of identifying factors) will not fall within the scope of the DPA 1998 (Q4, 4a, 4b).

9. Are there any special rules for processing 'personal data' as research data?

There are certain exemptions for the use of personal data for 'research purposes,' including statistical or historical purposes. If you can show that your processing for research purposes is not to be used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, you can:

- process personal data for purposes other than for which they were originally obtained (permitting the secondary analysis of datasets, for example) - exemption from Principle 2;
- effectively hold personal data indefinitely (permitting long-term archiving of research data, for example) – exemption from Principle 5.

Additionally, where the research results (in articles, research reports, dissertations etc.), or any resulting statistics, are effectively anonymised, you can claim an exemption from the data subject's right of access to their personal data held in your research dataset – partial exemption from Principle 6.

As a result, if your research meets the requirements of an exemption, your processing and archiving of research data is made simpler. However, there is no blanket exemption from the Data Protection Principles for research purposes. Thus, for example:

- you should inform data subjects of any new data processing purposes, the identity of the data controller, and any disclosures that may be made – Principle 1;
- data subjects must be able to meaningfully exercise their right to object to your data processing because it would cause/has caused them significant damage or distress – Principle 6;
- you must ensure appropriate security of the data, including higher levels of security for sensitive data, as appropriate – Principle 7.

To take advantage of the exemptions, you should be able to:

- identify the condition for processing you intend to use;
- show, as appropriate, that you have made an objective assessment that your new processing is both necessary for your research and proportionate to your purpose;
- demonstrate your research meets the exemption criteria.

Where you are processing archived data which has been fully anonymized (e.g. by destruction of link codes, or removal of identifying factors) this will not fall within the scope of the DPA 1998 (Q4, 4a, 4b).

9a. Does that mean that if I want to reuse a dataset containing personal data, I have to inform every data subject of my new research purpose?

Where you wish to carry out research on an existing dataset containing personal data, notification of data subjects may be avoided if:

- the data was obtained directly from the data subject, but your new processing purpose was not known at the time, and you can make a plausible case that it is now 'not practicable' to provide the relevant information;
- you have obtained the data from a third party; AND
  - provision of information to data subjects would involve disproportionate effort; AND
  - the data subject has made no prior demand in writing for information about the processing; OR if they have made a demand in writing, you do not have sufficient information about them to determine whether you are processing personal data about them, and you notify them in writing that you cannot provide the required information because of your inability to make that determination, with reasons for that inability. AND
  - you record the reasons for believing that 'disproportionate effort' applies.

The ICO has advised that assessing practicality and disproportionate effort should include factors such as cost, time and ease of provision of information weighed against benefit/risk to the individual. Where data is obtained from elsewhere, particularly if the data is not recent, then it may be impossible, or at least disproportionately difficult, to inform the data subjects.

10. What rights do data subjects have with regard to personal data?

Data subjects have a variety of rights with regard personal data about them held by data controllers. Failure to respect these rights can result in civil or criminal actions against the data controller. Most data subject rights are linked to, and/or depend for their usefulness upon, the availability of an effective right of subject access. Subject access means that a data subject is entitled to be told by a data controller whether personal data about them is being processed by, or on behalf of, that data controller, and to be given access to a copy of that data (see Q16). The rights include the ability to:

- make subject access requests
- prevent processing likely to cause damage or distress
- prevent processing for direct marketing purposes
- take action for compensation if they suffer damage caused by breach of the Act
- take action to rectify, block, erase or destroy inaccurate data,
- request the Information Commissioner to assess whether the Act has been breached

In principle, these rights apply to personal data collected for research purposes. However, research data can be exempted from certain of these rights (See Q9)

11. I'm supposed to keep my data up to date 'where necessary', what does this mean??

Once research data has been collected elements of it may become dated quite quickly. The DPA 1998 requires data to be kept up to date where necessary. The key phrase is "where necessary". Research outputs will often be based on information representing the situation at a particular moment in time, and there will be no reason to update this information as circumstances change. Care needs to be taken, however, if you are conducting research which might be used to support measures or decisions taken concerning individuals (e.g. a longitudinal study for a government department): in such circumstances, not only will the research exemptions (Q9) be unlikely to apply, there will also be a requirement that the data is up-to-date and accurate.

12. What responsibility do I have for the security of the personal data I process?

Research data may be collected in many ways, e.g. paper questionnaires, tape or digital recordings of interviews and focus groups, online surveys; and stored in a range of formats e.g. handwritten notes, analogue and digital recordings, computer files. Each mechanism for collecting and storing data poses particular issues with regard to security against unauthorised access and use, prevention of accidental loss or damage, and eventual disposal. Your institution, as data controller, is responsible for ensuring that personal data is held appropriately, taking into account the nature of the data, e.g. if it is sensitive personal data, it may justify requiring greater protective measures, e.g. access controls, encryption and audited disposal. As a researcher, it is your role to ensure that your institution is adequately informed about the nature of your research data, the scale of data to be collected, how you intend to protect data gathered during field work, whether and when data will be pseudonymised or anonymised, how long it needs to be retained etc. This information will usually be gathered as part of the research ethics process, and a REC may require you to:

- identify the means and mechanisms you will employ for collecting, processing and storing your research data;
- demonstrate your understanding of the particular legal and ethical risks pertaining to those means and mechanisms, e.g. use of internet based tools: see further, Charlesworth, 2008.
- provide details of measures taken to secure research data e.g. physical security of equipment and notes (at work, at home and in the field), and digital security mechanisms, such as system, program and file passwording and use of encryption.

Failure to address security issues appropriately, particularly where data is unlawfully disclosed, may result in breaches of your institution's research ethics rules, and damage to your professional reputation, as well as your institution being audited or fined by the ICO. Serious data losses, e.g. disclosure of personal data about victims of child abuse and child abusers, from a research project investigating how authorities could seek to prevent abuse occurring, could currently result in fines of up to £500, 000.

12a. What are 'appropriate technical and organisational measures'?

What are considered to be 'appropriate technical and organisational measures' will vary depending upon the personal data processed and as the 'state of the art' in technical security measures and data management

protocols changes over time. As such, the answer to this question is not fixed. For example: as the cost of encryption falls, its availability in recording and storage devices becomes standard, and its use becomes simpler, there will be an expectation not just that it is used for particularly risky or sensitive personal data, but that it is used ubiquitously to protect all personal data. If encryption of even basic personal data becomes the norm, a researcher's failure to use it will increasingly be seen as bad data management practice, even if the risk that inadvertent disclosure presents to data subjects is relatively low. You will be expected to have undertaken a risk assessment relating to personal data processed in your research, to have developed a research data management plan, and to be aware of current developments and good practice in secure processing of personal data. To meet these requirements, it will be important to liaise not just with your REC, but also with your institutional IT services or other technical support.

See the Jisc Research Data Management webpages (2013)

12b. Can I store my data in the Cloud?

Cloud computing is a term that encompasses a wide range of use cases and implementation models. In essence, a computing 'cloud' is a large shared pool of computing resources including data storage. It is assumed here that the question refers to cloud storage solutions run in large data centres accessed by customers over the public internet (often called 'the public cloud)'. Advantages of public cloud storage are low cost, rapid scalability, and easy accessibility. Questions that should be asked about personal data storage in the Cloud from a data protection perspective are:

- what is the nature of the personal data to be stored in the cloud?
- what measures are there to prevent loss of, or damage to, the data?
- is the data secured against unauthorised access and are all accesses audited?
- is the data encrypted at the end-user's location or at the cloud service provider?
- can data be processed in specific geographic locations?
- can the data be easily extracted from the cloud service?
- can the data be verifiably deleted from the cloud service?
- does the cloud service conform to recognised data management/security standards, e.g. ISO 27001 or 27002?
- Whose law applies to the cloud service provider?
- Whose law applies to the contract between you and the cloud service provider?

If you cannot answer questions like these you should think very carefully about whether the cloud service you are seeking to use can meet your requirement to utilise appropriate technical and organisational measures to protect the personal data you are processing.

12c. Can I use web surveys?

Web surveys are an increasingly popular means of conducting empirical research online. If used with appropriate attention to the type of personal data being collected and with a clear understanding on your part of the possible risks, their use should be unobjectionable, indeed the ICO commissions online research from researchers who use web survey providers, such as Survey Monkey. However, your institution may require use of specific web survey providers, and you should always check before using any new online data collection, transfer, or storage system to ensure you are not breaching internal institutional rules.

A key thing to remember is that potential data protection breaches are often not caused by the technology employed, but are down to researchers not fully understanding the risks of the technologies they are using, or engaging in research practices which compromise the security of those services.

The following examples demonstrate how data protection law breaches might occur:

A researcher posts a link to a web-based questionnaire on an e-mail list, asking for responses. Her website contains a web page providing a detailed outline of the research and describing how the data collected will be used.

- The link in the e-mail goes directly to the questionnaire, inadvertently bypassing the web page of information, meaning respondents never see it. At the start of the questionnaire, where consent to use their personal data is requested, respondents have not been given adequate information to provide informed consent.
- The link in the e-mail goes to the start of the questionnaire, which contains a further link to the web page of information. However, that link is at the bottom of the questionnaire web page and respondents may not scroll down far enough to see it.

Another researcher collects sensitive personal data from respondents using a web-based questionnaire. He states that responses will be confidential and held securely.

- A respondent's computer caches the questionnaire pages, including responses, leaving them accessible to other users of that computer.
- The link between respondents' computers and the computer hosting the questionnaire is unencrypted, and communications between them can be intercepted.
- The web survey software does not compartmentalise questionnaires. Any researcher in the researcher's department, including research students, can view both questionnaire and responses.
- All researchers in the department log into the web survey software using the same password. (Charlesworth 2008)

13. I'm collaborating with researchers at a University in the European Union; can I share my research data with them?

Under the DPA 1998 data controllers are not allowed to transfer personal data that they hold outside the UK unless the country or territory to which the data is to be sent ensures an 'adequate level of personal data protection' for data subjects. All European Economic Area countries (the EU Member States, plus Iceland, Liechtenstein and Norway) are assumed to have an adequate level of protection. There are thus no legal restrictions on your transfer of personal data to researchers in other EEA countries, provided you have informed research subjects that their personal data may be shared with these institutions. However, if you are planning to share research data containing personal data with researchers at an EEA research institution, you should still notify your DP practitioner, and seek advice on an appropriate formal data sharing/data controller agreement.

13a. I 'm collaborating with researchers at a University outside the EEA, can I share my research data with them?

The European Union only considers a few countries outside the EEA to have 'adequate protection'. These are Andorra, Argentina, Australia, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay.

Where you intend to share research data containing personal data with research institutions outside the EEA, this may be possible, provided you have informed research subjects that their personal data may be shared with these institutions, if:

- the country to which the data will be sent has been accepted as ensuring an "adequate level of protection" by the EU Commission; OR
- your institution has undertaken an adequacy assessment to determine whether there is adequate protection for the rights of individuals, in all the circumstances of the transfer; OR
- The data subjects have given their informed consent to the transfer; OR
- The transfer is made on contractual terms of a kind approved by the ICO as ensuring adequate safeguards for the rights and freedoms of data subjects.

Determining which of the possibilities apply to your research will require an expert assessment, and thus potential transfers of personal data outside the EEA should always be referred to your DP practitioner well in advance of any transfers taking place.

13b. Whilst on a field trip in Hong Kong, I'm going to collect personal data from research subjects to analyse when I return to the UK. What are the data protection implications?

Personal data that is processed in the UK by a data controller, regardless of where it is collected and the nationality of the data subjects, will fall under the DPA 1998, and foreign data subjects are entitled to exercise the same rights over their personal data as UK citizens. For processing to be fair you should provide the research subjects with information about your project in a form that is comprehensible to them, this may involve translating the information into other languages.

If you are collecting personal data in other countries, you should also be aware of any national legislation that applies to your processing, including the international transfer of that data to the UK e.g. Hong Kong has its own data protection laws. It is good practice to make clear in the information you provide to overseas research subjects that their data will be transferred to, and processed in, the UK, and to ensure that you have their consent, ideally in writing or some other permanent form, to such a transfer. International research is usually subject to heightened scrutiny by RECs due to a broader range of ethical risks, including possible data protection complications.

14. I intend to archive my research data, should I anonymise any personal data before archiving?

While the research exemptions in the DPA 1998 clearly permit research data containing personal data to "be kept indefinitely", it is worth remembering that if the personal data is unanonymised, it remains subject to the DPA 1998, and your institution remains liable, as data controller, to keep it in accordance with the applicable Data Protection Principles. Long term storage will require effective institutional data management protocols to be developed and policed, and ongoing review of the adequacy of technical and organisational measures pertaining to the data, e.g. the research data is archived securely, in a known location, and is accessible to authorised parties (Q12a). Thus, there are strong arguments in favour of anonymising research data which will be archived for long periods, where this will have no ill-effects on the potential revisiting or reuse of the research. This approach will prevent liability arising from inadvertent disclosures.

Some funders/sponsors will provide archiving facilities (e.g. the ESRC Research Data Policy requires all research grant award holders to offer data collected during the course of their research for preservation and sharing through the ESDS). It is important to note that data will often only be archived, if appropriate metadata (data about the research data, e.g. copyright status, data protection status) is provided. See further, UK Data Archive, Managing and Sharing Data (3rd ed).

15. If I no longer need research data containing personal data, and I don't want to archive it, what should I do with it?

If you have personal data which is not required to be formally archived, it should be anonymised or destroyed when it is no longer required for the purpose for which it was collected. The proper disposal of research data is vital for compliance with data protection rules, and for maintaining guarantees of confidentiality and anonymity for research participants.

As a basic standard, when no longer required:

- data held in paper form should be disposed of by shredding. Most institutions will have appropriate shredding systems in place for disposal of confidential data.

- data held in digital form should, wherever possible, be destroyed by multiple over-writing. Simply using the 'delete' function on a computer (even if you empty the 'recycling bin'), or even doing a simple disk reformat, will not usually erase data permanently.
- data held in non-rewritable digital media, such as CD-ROMS, DVDs and Blu-Ray discs, should be disposed of by destruction of the physical media (e.g. by shredding).

Disposal of higher risk data, such as 'sensitive personal data' under the DPA 1998, may require greater security measures, including third party audit of equipment and media to ensure data is effectively deleted.

Care should be taken to examine and erase research data from all digital equipment, including voice recorders, laptops, cameras, etc. This is particularly important where equipment is to be disposed of to third parties (e.g. by donation or resale). Many institutions now routinely remove and securely dispose of internal storage media, such as computer hard disks, prior to disposal of equipment.

16. What is a Subject Access Request?

A subject access request (SAR) is a written request by or on behalf of a data subject for information about whether data is held by a data controller about them, what the data is, why it is being processed, and to whom it has been or may be given. There is no set form for an SAR, it does not have to be labelled as such, or even mention the DPA 1998. Members of the public may confuse FoI requests and DP SARs, but if it is clear that the data subject is asking for their personal data than a request should be treated as an SAR. An SAR does have to be in writing, but does not have to be hard copy, e.g. an e-mail may suffice. An SAR is valid even if it is not sent to your institution's DP practitioner. There are circumstances where it is legitimate for a third party to make a SAR on behalf of a data subject.

Detailed guidance on subject access requests has been produced by the Information Commissioner's Office in Subject Access: Code of Practice (2014).

17. What should do if I think I have received a Subject Access Request?

If you are conducting empirical research with research subjects you will usually have disclosed in advance what personal data you are collecting, how it will be used and who will have access to it (see Q7), and you may well continue to discuss this with them as part of a process of 'rolling consent.' Such conversations should be seen as routine 'business as usual', and need not be treated as an SAR (even if, formally speaking, some of them are). If you are engaging in such processes you should continue to do so, paying due care and attention to normal research considerations e.g. ethics, privacy and confidentiality.

However, in circumstances where you don't want to supply personal data, or you think there are legal or ethical reasons why you shouldn't supply it, or a request (either written or oral) is specifically identified as a DP or FoI request, then you should consult your DP Practitioner as soon as possible. They will be best placed to assess whether the SAR meets the formal requirements, and if not, to discuss with the requester what further is required.

18. What am I likely to have to do if my research data is subject to an SAR?

The DPA 1998 requires your institution to confirm whether or not it holds personal data about the data subject, and to supply the information, or a refusal notice, within 40 calendar days from receipt of the request. Because of the time limit, it will help your DP Practitioner if you inform them immediately. Your DP practitioner will work with you to determine

- whether you are in fact holding personal data relating to the requester;
- whether your institution is required to provide the data , or if there is a relevant exemption;
- if personal data is to be provided, whether that data can be released 'as is', or whether some of it needs to be redacted, explained, or placed in a particular format;

so that your institution can respond effectively. Ideally, you will have considered the DP implications for your research data as part of your initial research data management plan, and in particular identified whether you may have grounds for withholding personal data from a SAR.

19. What are the exemptions from a SAR?

There are limited grounds for not providing a requester with their personal data. The two primary grounds that would apply to research data are:

- the personal data is exempt as research data from subject access (see Q9);
- it would involve disclosing information about another individual (see Q19b);

Whatever your reasons for not wishing to provide data, we strongly recommend that your DP Practitioner take over correspondence with the requester. Any person who believes that their SAR has not been handled correctly can ask the Information Commissioner to assess whether the processing has been/is being carried out in compliance with the Act, and even appeal to an Information Tribunal, and ultimately to the courts.

19a. Can I just delete data, if I don't want to release it?

You can delete your research data unless a request has been made for it via a SAR. Once a SAR has been made to an institution covered by FoI legislation, it becomes a criminal offence to alter, deface, block, erase, destroy or conceal any part of the data subject's personal data. Most of the sanctions under this legislation will apply to your institution, but if you delete requested information or order deletion, you could be personally liable. Don't do it, and make sure it is not deleted accidentally after the request.

A policy on managing research records (which may be required by your funder) can be helpful in demonstrating that any data deletions were the result of a pre-determined schedule, and not to avoid fulfilling a SAR.

19b. Some of the information may identify other living individuals. Must I disclose it?

Your institution does not have to comply with a SAR if this means disclosing information about another individual who can be identified from that information, unless:

- the other individual has consented to the disclosure; or
- it is reasonable in the context to disclose without their consent.

This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. It is strongly advised that this determination should be left to your DP practitioner.

19c. What does 'redacted' or 'redaction' mean?

This term refers to the practice of removing some information from a document while leaving other information intact. It is typically used to remove exempt information, e.g. in the case of an SAR, the personal data of a third party. Because redactions must be done carefully, it is strongly advised that they should be left to your DP practitioner.

20. What form should I provide the data in?

While a requester is entitled to see their own personal data: this is not a right to see copies of documents that contain their personal data, although providing original documents may be the easiest way for you to provide the relevant information, unless significant redaction is required.

Personal data has to be supplied in permanent form, unless the data subject agrees otherwise. If the data subject asks for the information in a particular form, and you can reasonably easily supply it to your DP

practitioner in that form, you should do so, as this will help your institution meet its duty to be helpful to requesters.

You should remember that some digital data formats can contain information that is not visible but can still be extracted. In order to ensure that your institution does not supply information inadvertently that it should not, it will be helpful for you to advise your DP practitioner on the formats you have used, and any technical issues you are aware of relevant to those formats.

20a. The personal data that I am using is held in a coded form, e.g. with abbreviations or codes for particular details, is this a problem?

Your institution must provide information to a data subject in 'intelligible form', i.e. the information you provide to your DP practitioner should be comprehensible to the average person, and this may require you to provide an explanation of project abbreviations or codes.

21. How common are SARs for research data?

A survey of research universities suggests that SARs requesting personal data collected as research data are currently relatively rare, but not unheard of. It is worth noting that SARs are often used by data subjects when they are already unhappy about some aspect of the data controller's operations. Providing clear and detailed information notices to your research subjects (Q7a) about how their personal data will be processed, and with whom it may be shared, will help avoid such situations.

22. What do I do if someone asks me to delete their personal data used in my research?

Under the DPA 1998, a data subject may write to you and require that you not process, or cease processing, their personal data because it is causing, or is likely to cause unwarranted and substantial damage or distress, to them or to another person. In such circumstances, you must give notice within 21 days of receipt that you will comply with the notice or provide reasons why you believe the request to be unjustified and whether you intend to refuse to comply or comply only in part with the request. The data subject may challenge any refusal in court.

A data subject who has given consent to their personal data being processed cannot follow this process, but can potentially withdraw their consent. The law is, however, unclear as to the ramifications of such withdrawal. The ICO suggests that "Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given."

In practice, as discussed above (Q7b), RECs will usually require that researchers obtain prior informed consent from their research subjects. From a research ethics perspective, withdrawal of such consent is usually taken to mean that the research data pertaining to the individual can no longer be used in the course of the research, unless material containing the data (in either anonymised or unanonymised form) has already been published, or specific restrictions on withdrawal have been agreed in advance with the research subjects. Thus, even if the DPA 1998 suggests that the personal data may be retained for research purposes, institutional research ethics may still be a barrier to its retention and use.

23. Can someone other than the data subject demand their data from me?

Under normal circumstances, where you have collected personal data for your research, you will have identified and informed the research subjects which categories of third parties, if any, will have access to the unanonymised personal data. Having done so, you should not make the personal data available to third parties outside those categories without informing the data subjects. If you are relying on consent as your condition for processing, you should, unless it is impractical to do so, seek data subject's further consent for the additional parties' access. However, the DPA 1998 permits third parties who are legally authorised to do so, to demand access to the personal data you hold, for specific purposes, e.g. police officers in possession of a court order requiring disclosure.

24. How does Data Protection legislation interact with Freedom of Information legislation in the UK?

Freedom of Information (FoI) and Environmental Information (EIR) legislation provides the public with a right to access information held by a UK public authority, which includes most universities, colleges, or publicly-funded research institutions. See Charlesworth A. & Rusbridge C. (2010). Freedom of Information and research data: Questions and answers, JISC.

The information requested could include your research data, and must be provided unless an exemption or exception allows your institution not to disclose it.

Probably the most important exemption for University researchers is that for information intended for future publication and research information. This states that information is exempt from disclosure if, at the time when a University (as public authority) receives a request for it:

- it holds the requested information;
- it intends the information to be published at some future date, whether that date is determined or not; and
- in all the circumstances it is reasonable to withhold the information until its planned publication.

This is a 'qualified exemption' and therefore a University must consider whether the public interest in maintaining the exemption is greater than the public interest in disclosing the requested information.

Once information has been published, the exemption will no longer apply to any of the same information contained in either earlier draft versions, or in other documentation. See ICO. (2015) Freedom of Information Act: Information intended for future publication and research information (s.22 and 22A).

Personal data is another key exemption to FoI legislation, where the requester is the subject of the data held (there is a similar exception under EIR). If the requester is not the subject of the personal data held, the exemptions become more complicated. Always discuss such cases with your FoI Practitioner and/or DP Practitioner.

In some cases where an FoI exemption applies, it will be an ‘absolute exemption’, so no public interest test is needed. The exceptions under EIR are differently worded but similar in effect, although a public interest test may be needed in this case.

FoI requests may also ask for details of ethical approvals for research or details of research data management oversight, including effective compliance with DP obligations.

Further information

Helpful material, such as the Privacy Notices: Code of Practice (2009), Anonymisation: Managing Data Protection Risk - Code of Practice (2012), and Subject Access: Code of Practice (2014) is available via the Data Protection section of the Information Commissioner's Office website. Your DP practitioner and Research Ethics Committees will be able to advise on how such general advice and guidance relates to actual instances of research practice.

Your institution will often have detailed guidance on research data management and research ethics. Good examples include the University of Edinburgh's Research Data Management website and the University of Sheffield's Research Ethics website.

The importance of conducting research in accordance with legal, ethical and professional obligations is outlined in Universities UK. (2012) The Concordat to support research integrity, particularly Commitment 2.

Charlesworth A. (2008) 'Understanding and Managing Legal Issues in Internet Research' in Fielding, N. Lee, R. & Blank, G. (eds.) *The SAGE Handbook of Online Research Methods*, Sage Publishing.

Corti, L. *et al.* (2014) *Managing and Sharing Research Data: A Guide to Good Practice*, Sage Publications

Millard C. (2011). Defining 'Personal Data' in e-Social Science. *Information Communication & Society* 15(1): 66-84.

Whilst accepting that all errors and infelicities of style remain his own, Andrew Charlesworth would like to acknowledge the help and comments of the following people in developing this document:

Anne Cutler, Academic Information Manager, and colleagues at the University of Sheffield
Peter Dinsdale, Information Security Officer (Compliance), University of Newcastle
Charles Fonge, University Records Manager and Archivist, University of York
Susan Graham, University Records Manager, University of Edinburgh
Dr James Knapton, Information Compliance Officer, University of Cambridge
Rachael Maguire, Records Manager, London School of Economics and Political Science
Matt Morrison, Information Rights Officer, University of Bristol
Professor Tonia Novitz, Research Director, Law School, University of Bristol
Adrian Slater, University Solicitor, University of Leeds
Paul Smallcombe, Records & Information Compliance Manager, Queen Mary University of London
Dr Birgit Whitman, Head of Research Governance, University of Bristol