

# MEMORANDUM FROM RESEARCH COUNCILS UK (RCUK) IN RESPONSE TO THE MINISTRY OF JUSTICE CONSULTATION ON THE USE AND SHARING OF PERSONAL INFORMATION IN THE PUBLIC AND PRIVATE SECTORS

## 1 Introduction

- 1.1 Research Councils UK (RCUK) is a strategic partnership set up to champion the research supported by the seven UK Research Councils. RCUK was established in 2002 to enable the Councils to work together more effectively to enhance the overall impact and effectiveness of their research, training and innovation activities, contributing to the delivery of the Government's objectives for science and innovation. Further details are available at [www.rcuk.ac.uk](http://www.rcuk.ac.uk)
- 1.2 This evidence is submitted by RCUK on behalf of all Research Councils (RC's) and represents their independent views. It does not include or necessarily reflect the views of the Science and Innovation Group in the Department for Innovation, Universities and Skills. The submission is made on behalf of the following Councils:
- Arts and Humanities Research Council (AHRC)
  - Biotechnology and Biological Sciences Research Council (BBSRC)
  - Engineering and Physical Sciences Research Council (EPSRC)
  - Economic and Social Research Council (ESRC)
  - Medical Research Council (MRC)
  - Natural Environment Research Council (NERC)
  - Science and Technology Facilities Council (STFC)
- 1.3 All RC's have contributed to the main text of this response. The following sections follow the order of the questions as set out in the consultation questionnaire and represent the collective view of the RCUK. The response is given from both the perspective of the RC's as data custodians and the perspective of the research community. Any instances of divergent views between the RC's are noted. Some Research Councils will submit individual responses to this consultation.

## 2 Background

### Question 1: Interest in data sharing

*What kinds of personal information do you collect, hold and share?*

*How do you collect, hold and share such personal information?*

*For what purposes do you collect, hold and share such personal information?*

- 2.1 Generally, the RC's hold personal information on the following groups:
- Research grant applicants, co-applicants and named project staff (both successful and unsuccessful)
  - Research Council funded students (both successful and unsuccessful applicants)
  - Grant Reviewers
  - Grant Assessors

- Lists of Council stakeholders and subscribers to publications
- Council, Board and Committee members
- Scientific and administrative staff employed by the Councils, including volunteers, agents, temporary and casual workers, and students
- Advisors, consultants and other professional experts
- Suppliers
- Councils who employ scientific staff within their own institute may also hold information on patients and other participants in research

2.2 Types of personal information collected from these groups include:

- Name
- Date of birth
- Job title
- Ethnicity
- Gender
- Personal postal addresses
- Work postal address
- Work telephone number
- Work fax number
- Work email address
- Home email address
- Supplier bank details (for processing travel and subsistence claims)
- Political affiliation (for Council member appointments)
- Bank account information
- National Insurance numbers
- Next of kin
- Salary
- Family, lifestyle and social circumstances
- Education and training details
- Trade union membership
- Physical or mental health condition
- Offences, criminal proceedings, outcomes and sentences

*Please note that only some of this information is collected from each group.*

- 2.3 There are three main routes through which RC's may collect personal information through research proposals. The primary route is via grant applications received by each RC. This is usually through the Joint electronic Submissions (Je-S) system; please note that the MRC does not currently utilise this system but anticipates joining Je-S in late 2009. Other applications may also be made, usually in response to a consultancy invitation or for ad hoc workshops or seminars, outside of any formal application system. The personal data from these applications is input onto the bespoke processing system. Further, personal data such as name and address are collected from potential grant Referees and Assessors and are input against the same systems. Finally staff in Research Council Institutes will hold the personal data of research participants which has been collected within research programmes.
- 2.4 There are occasions where such information may be shared between Councils particularly if two or more RC's are co-funding a research or training initiative. This is primarily done via the Je-S CDR (Common Data Repository) and is likely held on each Council's application files.
- 2.5 Some of this information is also shared with those who have been chosen by the RC's to review and assess funding applications. Each RC employs a rigorous system of peer review to ensure that only the highest quality funding applications of the most relevance to the research community in general are funded using public money. As such, individuals who are expert in a field relating to the proposal are asked to review the application and comment upon its relevance and quality – both in terms of the proposal itself and in terms of the proposed staff. This consequently means that reviewers are sent the application form that applicants have completed setting out their proposal.
- 2.6 Some RC's also fund studies that collect personal information from the general public. Whilst this information is not held by the individual RC's directly, the subsequent data are held by the funded research agency or institution and usually made available in an anonymised or aggregate form to inform secondary research.
- 2.7 In terms of the personal data held on RC employees, some information is shared between some Councils for payroll purposes. For example, the ESRC and EPSRC have a shared Human Resources so information on these RC's employees is shared, as is information between BBSRC and NERC.
- 2.8 There are some types of personal information (specifically name and place of work) held on Council, Board or Committee members that is made available on the relevant RC website. For an example see: <http://www.esrcsocietytoday.ac.uk/ESRCInfoCentre/about/what%5Fto%5Fdo/OurOrganisationandstructure/TheESRCCouncil/current%5Fcouncil%5Fmembership/>

### **3 Scope of Personal Information Sharing: benefits, barriers and risks**

#### **Question 2: Key benefits of data sharing**

*What are the key benefits of sharing personal information to (a) individuals, and (b) society? Give examples*

- 3.1 In terms of the RC's specifically, sharing personal data between Councils means that:
- individuals (as referred to in 2.1 above) do not have to issue their personal data more than once;
  - there is improved system efficiency by checking for and removing multiple entries of the same person;
  - Councils can guard against fraudulent claims for funding; and
  - by holding a shared repository, as long as the individual ensures their registration information is kept up to date, this information will update each Council's details; therefore we can ensure that the responsibility for keeping their data relevant belongs to the individual.

- 3.2 It should be noted that not all of these benefits are currently realised by the RC's. At present, the Councils generally have separate finance, human resources, and grants processing functions. However, the RC's are moving towards a model that will consolidate all of these separate functions into one organisation – a Shared Service Centre. Having consistent finance, human resources, grants and information technology processes across all Councils will improve efficiency, provide a seamless service and enable the above benefits to be fully realised.
- 3.3 From a research perspective, RCUK appreciate in the broadest sense the many potential benefits of data sharing to individuals and society as a whole, and some of the Councils have developed specific policies on data preservation and sharing. Data sharing:
- Facilitates high-quality, policy-relevant research by sharing and then combining datasets from different departments and agencies to form a full picture rather than analysing separate pieces of a jigsaw.
  - Reinforces open scientific inquiry thereby improving methods of data collection and measurements through the scrutiny of others.
  - Promotes new research and allows for the testing of new or alternative methods.
  - Reduces costs by avoiding duplicate data collection efforts.
  - Allows the creation of new datasets through the merging or linkage of two or more existing sources of information.
  - Provides an important resource for training in research by enabling new researchers to utilise existing data.
  - Can reduce the burden on respondents caused by multiple data collection efforts.
  - Reduces the information security risks associated with maintaining duplicated datasets in more than one location.
- 3.4 A concrete example of how data sharing can benefit both the individual and society is the sharing of aspects of clinical practice to develop expertise in the medical profession. This is achieved through sharing information on patients to explore unusual or new illnesses. Another example is the sharing of data between numerous agencies that make up local Crime and Disorder Reduction Partnerships. These partnerships involve agencies such as local councils, the police, ambulance and probation services who share their knowledge and expertise to help develop and evaluate local crime and disorder policies.

**Question 3: Key risks of sharing personal information**

*What are the key risks of sharing personal information to (q) individuals, and (b) society? Give examples*

- 3.5 RCUK perceive the key risk to the individual of data sharing to be:
- loss of data
  - fraudulent use of the data
  - inappropriate data storage policies and facilities leaving data at risk of misuse
  - individuals being subject to unwanted solicitations
- 3.6 The key risk to society of sharing personal data is loss of public trust in data custodians and users if data is lost or misused. Such a reduction in trust may result in disproportionate barriers to data sharing being implemented which, in research terms, would reduce the capacity to be able to undertake valuable policy-relevant work that could potentially benefit society as a whole.

**Question 4: Scope and methods of personal information sharing**

*What scope and what methods, in your view, pose the greatest opportunities or risks? Explain reasoning behind response.*

- 3.7 RCUK recognise the benefits that secure and safe data sharing could potentially have for informing research across a wide spectrum of disciplines. Its scope should therefore include:
- data sharing within and between government departments and agencies to help facilitate joined-up working and improve services for the public; and
  - allowing approved researchers access to such data to conduct policy-relevant and further knowledge in disciplines such as the medical sciences. This may be achieved through appropriate linking of datasets to enable more detailed analysis of a particular area/topic.
- 3.8 RCUK accept that there is a greater risk to the security of data the wider the scope is and hold the view that personal data should not be made available to any researcher but that controls should be put in place to mitigate the risk. For example, the Economic and Social Data Service offer access to detailed microdata from some Office for National Statistics surveys and since these datasets pose a higher risk of disclosure they have special conditions attached to their access and use. This is set out in the form of a Special License (SL). The SL requires the signature(s) of the researcher(s) and the institution with responsibility for the researcher. It also needs the explicit permission of the data owner to release the data to the researcher(s).
- 3.9 The SL contains:
- the conditions for access for statistical research purposes
  - the obligation of the researcher(s) and the measures for protecting and respecting the confidentiality of statistical data

- statistical purpose and how the data are to be used
- justification why access is needed to the more detailed version of the data
- standards and methods for disclosure control for any outputs
- requirement on the researcher to supply the bibliographic details of any published work, based wholly or in part on the data collection(s) accessed
- clauses relating to data and site security and destruction of the data on completion of the project
- sanctions to be applied to breaches of confidentiality

**Question 5: Public authorities**

*Provide examples of where, in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.*

3.10 RCUK has no comment to make in relation to this question.

**Question 6: Private sector organisations**

*Provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.*

3.11 RCUK has no comment to make in relation to this question.

**Question 7: Examples of potential beneficial data sharing between two or more bodies**

*Provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place. Explain why information is not being shared, detailing what the barriers to data sharing are.*

3.12 RCUK would like to highlight here the opportunities that improved data sharing in the UK offers for academic and non-academic research. The opportunities are broadly two-fold. First is the potential that administrative data offer in terms of providing a more comprehensive evidence base to assist in policy making. The second relates to the potential for using administrative data as a means of achieving cost savings, in terms of utilising data which would otherwise remain dormant as well as avoiding duplication of data collection through surveys. In order to realise these benefits it is essential that legislation facilitates broad data sharing for research purposes, whilst protecting individuals by ensuring that their data are dealt with ethically and within the law.

**Question 8: Examples of data sharing between two or more bodies that should not be taking place**

*Provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place. Describe the information sharing concerned and why you believe it should not be taking place, including the risks involved in such data sharing.*

3.13 RCUK has no comment to make in relation to this question.

## 4 The Legal Framework

### Question 9: Strengths and weaknesses of the Data Protection Act

*How well does the Data Protection Act work? Outline what you perceive to be the strengths and weaknesses of the Act.*

- 4.1 RCUK view the strengths of the DPA to be:
- The requirement that authorities must be open about how the information they collect will be used – this helps to ensure transparency of process and protect the individual.
  - Individuals have control over how their information is handled and they have rights of appeal if their information is handled incorrectly.
  - Individuals have the right to request all information held on them by a specific authority.
  - Authorities must register as Data Controllers with the Information Commissioners Office; this provides more governmental control over which authorities actually process data and thereby helps to monitor the implementation of the Act.
  - The DPC overrides the Freedom of Information (FoI) Act so individuals cannot undermine the principles of data protection by trying to gain access to personal information through FoI requests.
- 4.2 The Act is not considered to have a weakness as such with regard to providing individuals with rights and authorities with rules, but authorities must ensure their staff understand that the Act is relevant to their jobs, even if they do not actually collect or handle any personal data, they need to be aware of the data protection principles and know never to release, disclose or misuse data.

### Question 10: Adherence to the Data Protection Act

*How well do public authorities and private organisations adhere to the second principle of the Data Protection Act? Provide examples and reasoning.*

*How valuable to you think the second principle is? Provide examples and reasoning.*

- 4.3 The second principle is that data are obtained and used only for specified and lawful purposes. This incorporates the ‘obtaining’, ‘holding’ and ‘disclosing’ of data; therefore authorities should not add person names and other information to databases or mailing lists without that person’s consent. This is not always the case however and is a risk taken by authorities who may continue with this practice.
- 4.4 Further weaknesses may be caused by employees taking personal data out of the office environment, i.e. on a laptop, memory disk, hard copy or contained within emailed information. From an RC perspective, this practice occurs where staff are frequently away from the office or for long periods of time, and when staff are attending meetings where they are

required to minute the discussion or access a large quantity of material (for example during a commissioning panel meeting) that would be unwieldy to produce hard copies of. The RC's are currently undertaking a review of their data transportation practices and are taking steps to ensure that all electronic devices are suitably encrypted and that employees take great care to ensure that data remains secure and safe when away from office locations.

**Question 11: Barriers to the Data Protection Act**

*What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Provide examples.*

- 4.5 Lack of clear information and subsequent knowledge. Authorities should ensure that their websites contain sufficient Data Protection information and privacy confirmation for individuals in a clear and concise manner (plain English) to ensure understanding.
- 4.6 It could be argued that the effectiveness of the DPA has been diluted by advances in technology where it is now possible to store huge datasets on one small device. This increases the risks to security.

**Question 12: Amendments to the Data Protection Act**

*What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA?*

- 4.7 In general, RCUK perceive the legal framework surrounding data sharing as requiring clarification and would welcome any amendments to the Act that assists the sharing of data for research purposes.
- 4.8 RCUK advise that the DPA is updated to reflect technological developments, especially in terms of what is considered as personal data in this digital age. For example, are video and audio recordings and digital images covered?
- 4.9 Also, it is important to note that the DPA is not the only piece of legislation designed to protect and safeguard personal information. Any revision of the DPA should consider its links with the Freedom of Information (Fol) Act 2000 and relevant copyright legislation.

**Question 13: UK or EU law**

*Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Provide examples.*

- 4.10 RCUK view positively the EU Directive 95/46/EC as it enforces Member States to protect the fundamental rights and freedoms of individuals, to respect their right to privacy and to adhere to the principles of processing their personal data.

**Question 14: Unavailable statutory powers**

*Are there any statutory powers unavailable that would enable better and more secure sharing of personal information – for example identity authentication purposes – between (a) public authorities and (b) public authorities and private organisations? If so, what are they? Provide examples.*

- 4.11 RCUK has no comment to make in relation to this question.

**Question 15: Unreasonable burden on business**

*Are there any parts of the legal framework that place an unreasonable burden on business? Provide examples.*

- 4.12 RCUK has no comment to make in relation to this question.

**5 Consent and Transparency**

**Question 16: Clarity of requirement to obtain individual consent**

*Is it clear whether and when you need individuals' consent to share information about them? Provide examples.*

*Are you clear about the form that consent should take? Provide examples.*

- 5.1 RCUK's view from an organisational perspective is that it is clear that individuals' consent must be given before information can be shared about them; the consent must be in writing to provide accountability for authorities.
- 5.2 From a research perspective however this is perhaps not so clear. All RC's require the research they fund to be conducted ethically and with appropriate consent. All RC's have an ethics framework which they expect researchers to follow. For instance, researchers are expected to gain appropriate approval from their research ethics committee prior to undertaking their research.
- 5.3 While researchers seek appropriate consent to undertake specific research programmes or projects, this may not always include adequate provision for future use. For example, an ESRC funded researcher conducting a study on a sensitive topic such as social influences on sexual behaviour may seek to reassure their study participants by stating in the consent form that the resulting data will only be used by the research team. This then causes a problem for the researcher as they are

obliged by ESRC to offer their dataset for deposit at the Economic and Social Data Service.

- 5.4 What this example serves to illustrate is that explicit and informed consent should be obtained that not only means the participant understands their involvement and what their data will primarily be used for, but also highlights the fact that their anonymised data may be shared with others where appropriate.
- 5.5 An issue that requires clarity is whether consent should be sought for the sharing of administrative data. By its very definition administrative data have not been obtained through research and therefore are not designed for research purposes. As such, consent to share such data are unlikely to have been sought which, if enforced, may hinder data sharing initiatives across government. Given the enormous potential that administrative data and subsequent data linking has for policy research and thus the advantages that its appropriate use poses for society, it is critical that this ambiguity is clarified.

**Question 17: Barriers that gaining consent would cause for information sharing**

*What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Explain reasoning.*

- 5.6 From an organisational perspective, gaining consent to share personal information could be seen as a barrier, but a necessary barrier as it guards against inappropriate data sharing which would be a breach of the DPA. It would leave individuals without any security or clarification about exactly what will happen to their data. If an individual refused to give consent to have their data shared, this would cause an immediate barrier to the work of many authorities, such as the RCs, and would have the implication of not being able to process funding applications or use relevant and appropriate reviewers within that field or discipline. Please see paragraph 5.5 for a research perspective.

**Question 18: Transparent information sharing**

*Do you have any suggestions on how to make the sharing of information more transparent?*

- *Should individuals be given strengthened access rights? If so, how?*
- *Should organisations be expected to do more to explain their use and sharing of personal information to the public? If so, how?*

- 5.7 RCUK endorse the view that organisations should be clear about how data they collect will be used and shared. In particular, data protection notifications could be more specific so that the public can judge whether processing is legitimate. Currently only the data controller and the Information Commissioners Office can make this judgement.

**Question 19: Development of data sharing policy**

*How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?*

*How valuable is the Information Commissioner's recently published Framework Code of Practice for Sharing Personal Information?*

*How valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December?*

- 5.8 To ensure that an information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability, RCUK advise that the public be fully engaged in the policy development process. Without the support of the public, whose data are being held, any policy would likely fail to reassure the public that their data are safe and will be handled and shared in a respectful and ethical manner.
- 5.9 Apart from being a good practice guide to dealing with shared information, where responsibility lies, establishing legal positions etc, the Framework Code of Practice is/will be invaluable to update the individual RC's existing policies on data protection, as well as the creation of a checklist to evaluate existing procedures.
- 5.10 The privacy impact assessment will be valuable to assess the potential benefits to the RCs of sharing information, to identify the dangers, and minimise the risks of the process.

**6 Technology**

**Question 20: Impact of technological advances on data sharing**

*What impact in your view have technological advances had on the sharing and protection of personal information? Provide examples.*

- 6.1 Technological advances pose both risk and reward for data sharing. We are living in a more mobile society with internet enabled mobile phones and PDA's being common place. Faster and more secure internet and email have meant that more data are being sent electronically than ever before, and the 'paper-less' office has resulted in more data storage on PC's and data distribution via CD's or other electronic formats. All of these, whilst being more convenient and faster to use than manual, paper methods, do pose some risk to data security from hackers, internet viruses and data loss. One way to counter this risk would be to better educate the public about using technologies safely in terms of protecting their personal data from fueling criminal activity such as identity theft
- 6.2 Having said that, in many ways technological advances have enhanced data security by helping develop more sophisticated ways to control for

disclosure of personal information, creating firewalls and installing advanced password protection systems. It has also helped to facilitate data sharing. For example, researchers can access electronic copies of large survey datasets from data archives and conduct powerful secondary analysis on them; local doctor's surgeries can quickly share patient information with a hospital if that patient is taken seriously ill. There are many more examples of the societal benefits that technology has enabled.

- 6.3 To counter public concern over data security there is an increasing need for greater availability and use of secure environments in which only authorised researchers can access to sensitive information. Such environments do already exist and a good example is the Office for National Statistics' Virtual Microdata Laboratory (VML)<sup>1</sup>. The VML is a research access facility through which confidential, sensitive data can be accessed within a secure environment. Due to the nature of the data, access is tightly restricted and procedures and audits are in place to ensure that only non-disclosive analysis is carried out. The ONS has therefore taken steps to allow researchers access to sensitive data by utilising available technology to ensure that the data are kept safe and secure.
- 6.4 The ESRC are looking to develop a Secure Data Service (SDS) that will be modeled on the ONS' VML. The SDS will provide controlled access to sensitive and/or disclosive personal or organisational information which cannot be released for research purposes under End User Licence<sup>2</sup> or Special Licence<sup>3</sup> conditions. For more information about the SDS and the way it will utilise technology to further data sharing please see the separate ESRC response to this consultation.

#### **Question 21: Mandating technical safeguards**

*Should the law mandate specific technical safeguards for protecting personal information? For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?*

- 6.5 RCUK endorse the view that there should be mandated technical safeguards to protect personal data but note that technology advances so quickly it may be difficult to legislate. As such only minimum standards may be possible to define (e.g. 128 bit encryption as a minimum requirement for personal data on mobile devices).

#### **Question 22: Privacy enhancing techniques**

*How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?*

<sup>1</sup> The VML can be accessed from all four ONS sites at Titchfield, Newport, London and Southport.

<sup>2</sup> For more information about the End User License follow: <http://www.esds.ac.uk/aandp/create/eul.asp>

<sup>3</sup> For more information about the Special License follow: <http://www.esds.ac.uk/orderingdata/speciallicence.asp>

*Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?*

- 6.6 Overall privacy enhancing techniques help to mitigate the risk of data being subject to privacy invasive technologies. Both anonymisation and pseudonymisation are concerned with protecting personally identifiable information and as such reduces the risk of such personal data being misused.
- 6.7 The application of the legal framework for data sharing means that data custodians must be careful to ensure that the practice is lawful and that confidentiality is maintained. In practical terms this means anonymising data before release. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification<sup>4</sup>. In addition the data custodian must also show due regard to disclosure risk whereby individuals (and their confidential data) may be recognised by inference even after anonymisation.
- 6.8 Pseudonymisation has the advantage of allowing the clustering and integration of data from individuals or organisations without revealing their identities. It is particularly useful for the analysis of longitudinal data as entries from the same person can be linked by a unique identifier. The person's true identify can only usually be discovered if the data are matched with a particular piece of information. Pseudonymisation therefore means that a dataset remains complete which helps facilitate accurate and reliable research.

---

<sup>4</sup> Pseudonymised differs from anonymised data in that the original provider of the information may retain a means of identifying individuals.

## 7 International Comparisons

### **Question 23: Jurisdictions that may benefit the UK**

*Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Provide examples.*

7.1 RCUK has no comment to make in relation to this question.

### **Question 24: International good practice**

*Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?*

7.2 RCUK has no comment to make in relation to this question.

### **Question 25: Jurisdictions restricting information sharing**

*Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?*

7.3 RCUK has no comment to make in relation to this question.

### **Question 26: Public attitudes**

*Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Provide examples.*

7.4 RCUK has no comment to make in relation to this question.

## 8 Additional Questions

### **Question 27: Additional issues**

*Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering? Do any of these issues apply specifically to your sector?*

8.1 RCUK would like to take this opportunity to stress that the perspective of researchers (both academic and non-academic) should be taken into account when considering the benefits and risks of sharing personal data. The opportunities that improved data sharing and access has for research, particularly policy-relevant research, is enormous considering the vast number of different administrative datasets that are in existence from public bodies. The ability to share and subsequently link these datasets has the potential to form a rich evidence base from which research can be undertaken that would benefit the whole of society in areas such as health, crime and social care.

**Question 28: Additional suggestions**

*Please set out any additional suggestions of observations you have that you believe will be assistance to the review.*

8.2 RCUK has no comment to make in relation to this question.

**9 Further Information**

9.1 In drafting this response comments and advice was sought from the seven Research Councils that form RCUK. Any enquiries about the response or requests for further information should be addressed, in the first instance, to: