Data Protection – Sharing Personal Data

What this guidance covers

This guidance note for staff sets out factors to consider when sharing personal data for which King’s is responsible with other organizations. It covers two types of data sharing:

- **systematic** data sharing: where personal data is shared with another organization on an ongoing basis (e.g. a regular annual transfer);
- **one off** data sharing: where personal data is shared in response to a specific request (e.g. from the police).

For the purposes of this guidance, ‘personal data’ means any information on an identifiable living person, while ‘sensitive personal data’ is personal data which relates to an individual’s health, ethnicity, religion or belief, sexual life, political opinions, trade union membership, or the commission or alleged commission of offences by them. Both types of data are protected by the Data Protection Act (DPA), and ‘sensitive personal data’ has additional protections. Unless otherwise indicated, ‘personal data’ is used in this guidance to mean both.

The Legal Compliance team can provide advice about data sharing and other aspects of Data Protection (see below for contact details).

Data sharing vs outsourcing

‘Outsourcing’ occurs when another organization processes personal data on the College’s behalf (e.g. a company that maintains a database for King’s under contract). The College remains legally responsible for what the contractor does with the personal data, and we have to ensure that the arrangement meets the Data Protection Act’s requirements for outsourcing contracts. The College has separate guidance on outsourcing and Data Protection which is available via the Policy Zone.

By contrast, this guidance covers situations where personal data is given to another organization for its own purposes rather than to process on the College’s behalf. The recipient organization will acquire control of the data (subject to provisions in the data sharing agreement), and will have to meet the requirements of the Data Protection Act in how it uses the data. However, as the originating body, King’s also has to ensure that the transfer of the data and its subsequent use will meet its obligations under the Act. Sometimes data sharing will involve two or more organizations having joint access to data (e.g. a shared database), and in these situations the organizations will also be jointly responsible for the data.

Why would we share personal data?

There are a number of situations in which we might want to share personal data, on a one-off or ongoing basis. For example:

- to meet a statutory obligation, where we are obliged by law to provide data to another organization;
- where there are public interest factors in favour of sharing personal data (e.g. sharing information to advance medical research);
- where the sharing of the data is in the interests of the individual (e.g. allowing us or other organizations to provide a better service to them);
- to assist the police or other agencies in criminal investigations.

However, it is not sufficient for there to be a good reason for sharing the personal data (although that is clearly important): the data sharing also has to meet the requirements of the DPA.
Systematic data sharing: data sharing required by law

In many respects, this is the most straightforward form of data sharing. Where we are required by law to provide personal data to another organization, the Data Protection Act will not stand in the way of that. For example, the College provides personal data on students and staff to the Higher Education Statistics Agency (HESA) in accordance with obligations imposed on universities by the Further and Higher Education Act 1992. However:

- we have to ensure that the data is transferred in a secure manner (see below);
- it is good practice to provide individuals with information that the data sharing is occurring, via a notice made available to them when their data is gathered.

This applies to transfers which are a statutory requirement. In the same manner, personal data can be shared where that is necessary for compliance with a court order, for the administration of justice, for legal proceedings or seeking legal advice, or for the exercise of government or statutory functions. However, data sharing which is required as a result of a contract between the College and the body receiving the data is not covered by these provisions in the DPA, and will have to be legitimized by other means – see below.

Systematic data sharing: other situations – factors to consider

Where the sharing of personal with another organization is not required by law, guidance from the Information Commissioner suggests that the following points should be considered before entering into a data sharing arrangement:

Is the data sharing justified?

- What is the sharing meant to achieve?

  The objectives of the data sharing arrangement should be clear and it is good practice to document them.

- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

  This relates to the requirement of the Data Protection Act that the processing of individuals’ data (including sharing of their data) should be ‘fair’, which includes compliance with the Act’s conditions around ‘fair processing’. In most cases involving personal data which is not ‘sensitive personal data’, this will involve balancing the benefits to the individual and to society of the data sharing against any detriment that might be caused to the individual.

  Where this balance falls will determine whether you need to seek the consent of individuals to the data sharing and how far you will need to actively inform them that it is occurring. If the transfer to another organization involves non-sensitive personal data, is unlikely to have a significant impact on an individual, is something that they would probably expect to happen and would not be expected to object to, seeking their consent is unlikely to be necessary and you could rely on a privacy notice placed on the website to inform individuals about the arrangement. Conversely, it is more likely that you will have to seek individuals’ consent and make them actively aware about the data sharing (e.g. by providing them with notice explaining the arrangement) where:

  - the personal data is ‘sensitive personal data’ or confidential information; or
  - the individual would be likely to object to the data sharing; or
  - the data sharing is likely to have a significant impact on an individual.
The expectation of the DPA is that individuals should normally be provided with information that
their data is being shared with other organizations. This should usually be done at the point when
the data is gathered from them by means of a data collection notice which explains how their
data will be shared (the notice can be written to anticipate future transfers). If it is necessary to
seek the individual's consent to the sharing (e.g. in the case of 'sensitive personal data'), the data
collection notice can also provide a way of capturing that consent. For further advice on data
collection notices, contact the Legal Compliance team.

- **Is the sharing proportionate to the issue you are addressing?**

Only share the information which you need to share with the other organization in order to
achieve the objectives of the arrangement – do not transfer more data than is necessary.

- **Could the objective be achieved without sharing personal data?**

If anonymised data (in which identifying details of individuals are removed) would be sufficient,
share that instead of sharing personal data.

**Do you have the powers to share?**

Provided the requirements of the DPA and other legislation are met, King's can share data as it is
a chartered corporation which (subject to its Charter and Statutes) can do anything which a natural
person can do. However, bodies that receive data from us may need to check that they have the
legal powers to enter into data sharing arrangements, e.g. where their powers are derived from
statute.

**Data sharing agreements**

The Information Commissioner recommends that systematic data sharing should be governed by a
data sharing agreement between the provider and the recipient of the data. The purpose of the
agreement is to define a set a rules for the data sharing operation. The Commissioner suggests
that an agreement should cover:

- the purpose(s) of the data sharing arrangement;
- who will receive the data and the circumstances in which they will have access;
- the data to be shared;
- requirements around the accuracy of the data, how it will be updated and the format in which it
  will be transferred;
- data security (see below);
- how long the data will be retained;
- procedures for dealing with complaints, queries and requests by individuals for access to their
data;
- periodic review of the agreement; and
- sanctions for failure to comply with the agreement.

A data sharing agreement could also restrict the ability of the recipient to transfer the data to other
organizations without the College's permission. If the College wished to retain intellectual property
rights in the data, the agreement should specify this.

For advice on data sharing agreements, contact the Legal Compliance team (see below).
Data sharing and data security

The Data Protection Act requires King’s to keep personal data secure against unauthorized access, accidental loss, damage or destruction. This means that in any data sharing arrangement, it is vitally important that:

- the data is transferred to the other organization in a secure manner. The data must be encrypted, or you should use the College’s secure file transfer service. For further guidance, see the Data Security page on OneSpace;
- the receiving organization has systems and procedures in place to ensure that once the data has been received, it will be handled in accordance with the security requirements of the DPA.

Both points should be covered in the data sharing agreement. This should specify the security standards that will be followed when the data is transferred, and it should require the recipient to maintain a level of data security that will meet the requirements of the DPA. We should also take steps prior to entering into the arrangement to ensure that we are satisfied with the other organization’s security measures.

Sharing personal data outside the UK

The Data Protection Act places restrictions on the transfer of personal data outside the European Economic Area (EEA). While these transfers are possible under certain circumstances, this is a complex area, so we recommend that you seek advice from the Legal Compliance team before entering into a data sharing arrangement that will involve sending personal data outside the EEA.

One-off data sharing

One-off data sharing is where an individual’s data is shared with another organization in an ad hoc way rather than as a matter of routine – e.g. in response to a specific issue or request. The factors to consider are generally the same as those relating to systematic data sharing (see above). However, there are exemptions in the Data Protection Act that are relevant to some of the situations in which the College is asked to share data on a one-off basis. In particular, we can share personal data with other organizations without an individual’s permission or knowledge where that is required for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of any tax or duty;
- safeguarding national security.

When sharing personal data under these exemptions, we need to ensure that:

- the request for the data is bona fide (i.e. is genuinely from the body making the request). Usually, that will be obvious from the information provided but if there is any doubt, contact the agency via their published contact address to verify that the request is genuine;
- the basis for sharing the data is clear and is properly documented. Before any transfer takes place, the requesting body should explain in writing why they need the data in terms of one or more of the above exemptions. (Police forces will usually do so using a ‘section 29’ form, which certifies that the data is required for the prevention or detection of crime or the apprehension or prosecution of offenders). We should keep a record of this in case it is necessary to demonstrate why the data was shared.

1 The EU member states plus Norway, Iceland and Liechtenstein.
These exemptions in the Data Protection Act are permissive and do not require the College to provide the information, although in the interests of community safety King’s will normally do so where personal data is requested by relevant agencies for the purposes specified above. There may also be situations where we are required by law to share the information. For example, the Social Security Fraud Act 2001 requires education institutions to provide information to authorized officers of the Department for Work and Pensions or local authorities which they require for the investigation of fraud against the state benefit system.

Note, as well, that the Data Protection Act does not prevent the sharing of an individual’s personal data without their consent or knowledge in emergency situations where there is a danger to their life or that of another person.

Further advice on ‘one off’ data sharing is available from the Legal Compliance team (see below).

Further advice and guidance

The Legal Compliance team can provide advice to staff on data sharing and other aspects of the Data Protection Act. See the team’s Data Protection webpages or contact them at legal-compliance@kcl.ac.uk (020 7848 4260).

The following external guidance is also relevant:

- Information Commissioner’s Office: Data Sharing Code of Practice and Checklists
- Ministry of Justice: Data Sharing Protocol

Approved by the Head of Administration and College Secretary on 15 December 2011.