Data Protection Guidelines for Student Projects

1. Introduction

   If you are using personal data in the course of your project, you are subject to the provisions of the UK General Data Protection Regulation 2016 and the Data Protection Act 2018 ("the Legislation").

   The Legislation lays down principles of data handling which are designed to make sure that personal data is used in a way which is fair and transparent to individuals and protects their rights. Breaches of the Legislation may constitute a criminal offence, and you may also be sued by individuals if your use of their data in breach of the Legislation has caused them damage or distress. It is therefore important that you follow these guidelines and the Coventry University Group Data Protection Policy to ensure that you are acting in compliance with the Legislation.

2. Definition of personal data

   Personal data is any data relating to an identified or identifiable natural person from which the person can be identified.

   Generic data about companies is not personal data, nor is aggregated statistical data, nor is data about deceased individuals. You should be aware that even if your project itself does not identify individuals, you are still bound by the Legislation when you are collecting 'raw' data from individuals.

3. Definition of special category personal data

   The Legislation places certain types of data under the heading 'special category' data. The following types of data about individuals fall into the category of special category personal data:

   - ethnic or racial origin
   - political opinions
   - religious or philosophical beliefs
   - trade union membership
   - the processing of genetic or biometric data for use in identifying an individual;
   - physical or mental health data
   - data relating to an individual's sex life or sexual orientation

   If you are using data of this kind, it is particularly important that you follow these guidelines carefully. Special rules also apply to the processing of personal data relating to criminal convictions and offences.

4. Privacy Notice

   The Legislation requires you to give individuals certain information at the time you collect their personal data. This includes: the purpose for which you intend to use their data, the legal basis on which you are processing their data, who you are going to

share their data with (and to which countries), and information about their data protection rights as set out by the Legislation. You should provide this information in a Privacy Notice at the time of collecting the personal data. If you are using a questionnaire to obtain data from your research subjects, the simplest way to provide the privacy notice is to include it in the questionnaire. If you need help in producing a privacy notice, please contact your project module leader.

5. Obtaining personal data from third parties

In some cases you will be using data obtained from a third party, rather than directly from the data subject. If it is possible to evidence that providing a privacy notice to these individuals would involve a disproportionate effort – you are exempt from this requirement.

In deciding whether or not there would be disproportionate effort, you should evaluate: time, cost, and ease of locating and contacting the individuals, and balance this against the prejudice of the individual not being provided with the notice.

Factors to be considered include: the size of the research sample, whether contact details for the individuals are already available and if not, how difficult it would be to obtain them, and the purpose and likely outcomes of the research and their effect on the individuals concerned. This evaluation process be documented in writing and if you are in doubt please refer to your project module leader or the Information Governance Unit.

6. Lawful Basis

While you may have to obtain the individual's consent to process their data for ethical purposes, you do not necessarily need to obtain consent for data protection purposes.

Instead, you must have one of a series of six a lawful bases to process the individual's personal data (one of which is consent). The lawful basis are set out under UK GDPR and are as follows:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Consent as a lawful basis carries with it inherent problems for research: for example the individual has a right to withdraw their consent at any time, a request which must be complied with. This could cause problems for your research since there are no exceptions as there are when you obtain consent for ethical purposes.

We recommend that the lawful basis considered is that of 'public task' – the data is necessary for processing for the performance of a task carried out in the public interest, or Legitimate Interests - the data is necessary for processing in the legitimate interests of Coventry University.

Consent should be considered as a last resort and where used the consent should be a freely given, specific, informed and unambiguous indication of the individual's wishes. The consent should be separate to any other terms and will need to be referenced in the Privacy Notice.

If you need assistance in establishing the appropriate lawful basis please contact the Information Governance Unit.

When special category personal data is being processed, there must be an additional legitimate basis from a further set of defined categories. Consent is the clearest additional basis, although the problems with this remain. It is recommended that you contact your project module leader or the Information Governance Unit for advice.

7. Design of questionnaires

   The Legislation requires that personal data should be relevant and limited to what is necessary for the purpose it was collected. You should bear this in mind when you design questionnaires and only ask for data that you really need to carry out your project. If you do not need personal information such as names and addresses, do not ask for them.

8. Security

   The Legislation requires that appropriate technical and organisational measures are put into place to ensure the security of personal data which you process. You should make sure that:

   - you do not allow third parties to access personal data held on computer by sharing your password or logging in to a computer and leaving it unattended
   - you follow the University's IT Security Policies and Procedures
   - you handle paper files containing personal data in a way that prevents access by third parties
   - you are careful about preventing loss or accidental disclosure of personal data when you are using it off-site e.g. on public transport or at home
   - you dispose of the data in an appropriate way when it is no longer required. You should make sure that any data stored on the hard disk of a computer, either the University's or your own, has been wiped. Simply deleting files may not be sufficient. IT Services or technical staff in your Faculty / School will be able to provide you with advice on how to do this. Paper files containing personal data should be shredded.