

MANCHESTER METROPOLITAN UNIVERSITY
DATA PROTECTION FACTSHEET

What is the Data Protection Act 1998?

The Data Protection Act 1998 (DPA) is designed to protect individuals' privacy rights and regulate the way in which personal data is used. The DPA gives individuals certain rights over their personal data and place obligations on organisations, who are Data Controllers, in relation to the processing of personal data. Most notably, the Act requires that organisations comply with the eight data protection principles where processing personal data. Compliance with the Act is enforced by the Information Commissioner, an independent regulatory office with powers to issue fines and enforcement notices for breaches of the Act.

The DPA will be superseded in May 2018 by the [General Data Protection Regulation](#) (GDPR). Although the GDPR is a piece of European legislation, the U.K Government have announced to Parliament their intention to implement domestic legislation which will mirror the GDPR. Much of the basic framework under the DPA will be kept intact under the GDPR. However, the GDPR will introduce stricter obligations on Data Controllers, extend obligations to Data Processors and strengthen the powers of the Information Commissioner.

Key definitions

The DPA is sometimes regarded as a complex piece of legislation partly due to the technical, legalistic language used in the Act. To help you understand the University's obligations under the DPA we have set out a quick guide to the key definitions in the Act.

Data subjects: the individuals to who the personal data relates.

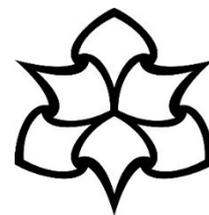
Data Controller: the person or organisation responsible for determining the manner and purpose of the processing of personal data.

Data Processor: a person or organisation processing personal data under the instructions of a Data Controller (e.g. an external contractor).

Processing: involves almost anything you do with personal data such as collecting, analysing, sharing, deleting and storing.

Personal Data: information which relates to a living individual who can be identified from that information or other information which is in the control of the Data Controller.

Sensitive Personal Data: categories of data which are afforded special protection under the DPA including personal data about ethnicity, sexuality and criminal offences.



The 8 Data Protection Principles

Anyone processing personal data must comply with the 8 data protection principles (DPPs). The obligation to comply with the DPPs will remain under the GDPR, although in some cases the principles will be more onerous. Further guidance on the DPPs can be found on the Information Commissioner's [website](#).

Principle 1: Personal data must be processed fairly and lawfully. The processing of personal data must also satisfy a condition in Schedule 2 to the Act and the processing of sensitive personal data must meet an additional condition in Schedule 3 of the Act.

Principle 2: Personal data must not be processed for a purpose which is incompatible with the original purpose for which it is processed.

Principle 3: Personal data must be adequate, relevant and not excessive.

Principle 4: Personal data must be accurate and kept up to date.

Principle 5: Personal data must only be kept for as long as necessary

Principle 6: Personal data must be processed in accordance with individual's rights

Principle 7: Personal data must be processed securely

Principle 8: Personal data must not be transferred outside the European Economic Area unless certain approved adequate arrangements are in place.

The Conditions For Processing

As set out above, all processing of personal data must satisfy a condition under Schedule 2 to the DPA and processing of sensitive personal data must satisfy an additional condition under Schedule 3 to the DPA. Some of the most common conditions relied upon by the University include;

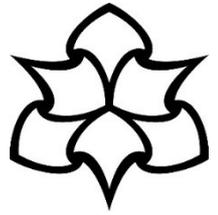
- (i) The individual has given their **consent** to the processing (personal data)
- (ii) The individual has given their **explicit consent** to the processing (sensitive personal data)
- (iii) The processing is necessary for the **performance of a contract**, or entering into a contract, with the data subject (personal data and sensitive personal data); and
- (iv) The processing is necessary for legitimate interests (pursued by the University) except where the processing is unwarranted because of the prejudice caused to the data subjects' privacy rights and freedoms.

Further guidance on the conditions for processing is available on the [ICO's website](#).

Data Subjects' Rights

The DPA provides individuals with certain rights in relation to their personal data:

Subject Access: Individuals have a right to access of their personal data and can exercise this request by making a subject access request. Please forward any subject



Right to prevent processing: individuals can request Data Controllers stop processing their personal data where the processing causes unwarranted substantial damage or distress

Right to prevent direct marketing: individuals can request that Data Controllers stop processing their personal data for direct marketing purposes

Right to block, erase, rectify and destroy: individuals can apply to the Court to request that Data Controllers block, erase, rectify or destroy personal data containing an expression of opinion that is based on inaccurate data.

Rights in relation to Automatic Decision Making: individuals have a right to request that decisions about them are not taken solely on the basis of automatic processing where the decision has a significant effect on them.