Guidance – determining 'legitimate interest'

Audience and Purpose

This guidance is for any member of University staff tasked with determining the legal basis for processing personal data who decides to use 'legitimate interest'.

You will need to use this guidance when:

- Customising a privacy notice to ensure it complies with current data protection legislation.
- Conducting a 'data protection impact assessment' (DPIA).
- Otherwise collecting or receiving personal data for a new initiative.

Definitions

- Personal data
- Sensitive personal data
- Data subject
- Processing

1. Processing in the legitimate interest

If personal data is to be used for purposes that do not relate to the University's core functions or public tasks, processing may also be possible if it is necessary for the legitimate interest of the University or a third party, and does not negatively affect the rights and freedoms of the people whose data you are processing. Thus, this legal basis requires a balancing of the legitimate interests of the University and/or the third party against the interests and fundamental rights of the data subject. When performing this balancing test, you will always need to consider the data subject's reasonable expectation of what is likely to happen to their personal data. Processing must also meet the strict requirements of being 'necessary'.

Moreover, if you rely on legitimate interest, you will need to be aware of and make provisions for data subjects' right to object to the processing. This means that if somebody can prove that their own rights and freedoms outweigh the University's, then their objection to processing must be taken into account and they must be opted out of the processing. Data subjects must be informed of this in every processing communication they receive.

2. What is 'interest'?

An 'interest' is the broad stake the University may have in the processing, or the benefit that the University derives, or which society might derive, from the processing. It must be real and not too vague.

Some interests are likely to be legitimate because they are 'strictly necessary' for University administration or related legal compliance issues, particularly where there is no legal obligation to comply with, but the processing is essential to ensure the University meets external or internal governance obligations.

Example:
Fraud prevention - where the processing is strictly necessary for the purpose of preventing fraud. This could include verifying that the registered address of the cardholder for a particular credit or debit card is the same as the cardholder's normal place of residence or work.

Other interests are legitimate because they are a routine part of the activities of the University but other lawful reasons for processing are not practical or are not available.

Example:

Alumni newsletter - a regular newsletter to alumni could be sent with consent as the legal basis. However, since consent requires a positive indication, an opt-in, it is not practical to ask for consent. Experience has shown that the return is minimal. It is also unlikely that alumni's rights and freedoms would outweigh the University's interest in sending regular updates.

Regardless of the importance of the processing activity to the University, an assessment must be made to ensure the processing meets the threshold required to rely on legitimate interests as a legal basis.

3. When is processing in the 'legitimate interest'?

Below are some generic examples of processing that will usually be in the legitimate interest:

Reasonable expectations - the fact that individuals have a reasonable expectation that the University will process their personal data for this purpose will help the make the case for legitimate interests to apply when conducting the balancing test.

Relevant & appropriate relationship – where there is a relevant and appropriate relationship between the individual and the University, such as between the University and its alumni.

Network & information security – where the processing of personal data is strictly necessary and proportionate for the purposes of ensuring network and information security.

Suppression lists – once somebody has opted out of receiving communications, the University will keep a suppression list to ensure that the individual will not be contacted again. Keeping this suppression list is in the legitimate interest of the University.

4. How to carry out the legitimate interest assessment

In order to rely on its legitimate interest, the University has to perform a three stage assessment:

1. identifying a legitimate interest,
2. establishing that the processing is 'necessary' and
3. conducting a balancing test.

The legitimate interest can be one of the University or of a third party to whom the data may be disclosed, as long as the three stage test is passed.

Contact the DPO at dpo@ed.ac.uk and you will be assigned an assessment in the online tool via OneTrust. Once the assessment has been completed and approved by the DPO, and the decision has been reached that 'necessary for the legitimate interest' is indeed the appropriate legal basis for processing, a short summary of the reasoning behind the decision must be included in the privacy notice.

1. Identifying a legitimate interest:

The first stage is to identify a legitimate interest – what is the purpose for processing the personal data and why is it important to the University?

A legitimate interest may be elective or business critical and can be those of the University or a third party to whom the personal data may be disclosed. It is possible that a number of parties may have a legitimate interest in processing the personal data. While you may only need to identify one legitimate interest, all relevant interests should be considered.

2. Carrying out a Necessity Test

You will need to consider whether the processing of personal data is 'necessary' for achieving the objective(s). The adjective 'necessary' is not synonymous with 'indispensable' but neither is it as wide as 'useful' or 'desirable'.

It may be easiest to simply ask, 'Is there another way of achieving the identified interest?' If there is no other way, then clearly the processing is necessary. It is, however, not enough to argue that processing is necessary simply because you have chosen to operate your business in a particular way. If there is another way but it would require disproportionate effort, then you may determine that the processing is still necessary. If there are multiple ways of achieving the objective, then a Privacy Impact Assessment (PIA) should be used to identify the least intrusive processing activity. Finally, if the processing is not necessary, then 'legitimate interest' cannot be relied on as a legal basis for that processing activity.

The 'necessary' test

3. Carrying out a Balancing Test

The University can only rely on a genuine legitimate interest where the rights and freedoms of the individual whose personal data will be processed have been evaluated, and these interests do not override the University's legitimate interest. Thus, you must carry out a balancing test. This balancing test must always be conducted fairly, which means that you must always give due regard and weighting to the rights and freedoms of individuals.

There are several factors to consider when making a decision regarding whether an individual's rights would override the University's legitimate interest. These include:

- the nature of the interests;
- the impact of processing;
- any safeguards which are or could be put in place.

The **nature** of the interests includes:

- the reasonable expectations of the individual: would or should they expect the processing to take place? If they would, then the impact of the processing is likely to have already been considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test;
- the type of data: special categories of personal data is subject to stricter rules on its use. This must be a consideration in a balancing test, and
- the nature of the interests of the University (e.g. is it a fundamental right, public or other type of interest):
    - Does it add value or convenience?
    - Is it also in the interests of the individual?
    - If there may be harm as a result of the processing, is it unwarranted?

The **impact** of processing includes:

- any positive or negative impacts on the individual, any bias or prejudice to the University, third party or to society of not conducting the processing.
- the University needs to carefully consider the likelihood of impact on the individual and the severity of that impact. Is it justified? A much more compelling justification will be required if there is the likelihood of unwarranted harm occurring.
- the status of the individual – a customer, a child, an employee, or other.
- the ways in which data are processed, e.g. does the processing involve profiling or data mining? Publication or disclosure to a large number of people? Is the processing on a large scale?

Any **safeguards** which are or could be put in place include:

- a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing, identified through a PIA, for example:
    - data minimisation

- de-identification
- additional layers of encryption
- data retention limits
- restricted access
- opt-out options
- anonymization
- encryption, hashing, salting

When the University is processing personal data relating to children, or special categories of personal data, special care should be taken with the balancing test, as it may need to give additional weight to the rights of the individual.