Appendices Index.

- Appendix A: Guidance for DPIA.
- Appendix B: Guidance for privacy notices.
- Appendix C: Guidance on writing a privacy notice.
- Appendix D: Guidance on reporting an incident.
- Appendix E: Article 6.1.
- Appendix F: Statement of Tasks in the Public Interest.
- Appendix G: Legitimate interests.

Data Protection Impact Assessment

Introduction

A Data Protection Impact Assessment (DPIA) is a process which helps to identify and mitigate potential risks to privacy and compliance with data protection law when processing personal data.

Whilst there was no statutory requirement to undertake DPIAs, under previous data protection legislation, they are regarded as good practice by the UK Information Commissioner's Office (ICO) and help to demonstrate compliance with existing data protection legislation. Under the new data protection legislation, in force from 25 May 2018, DPIAs are required for high risk processing activities.

We have developed this brief note on carrying out a DPIA, as it now forms part of our research registration process. This should assist researchers with making their own judgements for each project that they undertake which has potential privacy impacts.

How does a DPIA work?

A DPIA enables organisations to identify and reduce the privacy risks of a project by analysing how the proposed uses of personal information and technology will work in practice.

When should a DPIA be carried out?

Carrying out a DPIA is mandatory where the processing of personal data is likely to result in a high risk to the rights and freedoms of individual data subjects.

You should consider conducting a DPIA during the planning stage of new projects. A DPIA may also be required if changes are made to an existing project.

DPIAs must be updated as the process develops, particularly if issues are identified which may affect the risk to the data protection rights of affected individuals.

For Researchers: does your project require a DPIA?

To help researchers identify whether a DPIA is required we have set out the following screening questions in our existing research registration form, reproduced for reference below:

If the answer to any of these questions is 'yes', then a DPIA is required before any processing takes place	**Yes**	**No**
Will the project require individuals to provide information about themselves?		
Will information about individuals be shared with organisations or people who have not previously had routine access to the information?		
Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
Will the project result in you making decisions or treating individuals in ways which can have a significant impact on them?
Is the information about individuals likely to raise privacy concerns or expectations, e.g. health records or information that people would consider to be particularly private?
Will the project require contact with individuals in ways they may find intrusive, eg unexpected telephone calls?
Will the project use personal data, including personal data obtained from live or operational systems for access or transfer outside the UK (e.g. use of Cloud, Hybrid or offshore support purposes)?
Will the project involve processing sensitive personal data?

When is a DPIA not required?

The processing is not is not necessary to conduct a DPIA in all circumstances. For example, a DPIA would not be required where:

- The processing is not likely to result in a high risk to data subjects' rights;
- The nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has already been carried out. Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations; or
- Personal data is not being processed.

Who is responsible for completing a DPIA?

- In the context of a research project, the Chief Investigator, Principal Investigator, or Supervisor is normally responsible for ensuring the completion of a DPIA, as part of the research registration form.
- Note that in all cases, input and support from relevant third party data processors should be sought where applicable.

Where can I find further information on DPIAs?

- For further information on DPIAs and to download the DPIA form, please visit the **Data Privacy Impact Assessment** pages, or see the ICO's **PIA Code of Practice**.
- Please contact us at **data-protection@ucl.ac.uk**

Click here to return to Index page

Privacy

The General Data Protection Regulation (GDPR) came into force on the 25 May 2018. UCL has designed a comprehensive Programme of work designed to deliver the changes necessary for GDPR compliance. We will continue to update this statement as the work develops and progresses.

As part of our legal obligations we have published Staff, Student and General Privacy notices. Where require local privacy notices will be issued to inform individuals about what personal data is gathered, how it is used, stored and retained.

UCL also has a data protection policy that sets out our commitment to the safeguarding of personal data processed by its staff and students and our stances on compliance with data protection legislation. This policy describes how UCL will discharge its duties in order to ensure compliance with the data protection principles and rights of data subjects in particular and will be updated for GDPR in due course.
You can find information about the changes from the Information Commissioner's Office (ICO). The ICO is the UK regulator who oversees compliance with data protection legislation. Information Commissioner's Office Guide to the GDPR

UCL Privacy Notices

- General privacy notice
- Staff privacy notice
- Student privacy notice
- Alumni privacy notice
- Participants in health and care research privacy notice
- UCL Subsidiaries -

  ## UCL Consultants Privacy Policy Sept 2018

  UCL Consultants Privacy Policy Sept 2018
- UCL Data Protection Policy this is under review and will be updated in due course

There may be instances where local privacy notices are used to provide additional information about a UCL service. Please check these as you engage with them.

UCL Statement on the use of 'Public Task' as a lawful basis for processing

Where UCL processes personal data in connection with the carrying out of tasks in the public interest in its capacity as a public authority, UCL may rely on the 'public task' ground as its lawful basis for processing that personal data.
Where the processing of personal data by UCL is separate from UCL's tasks as a public authority, a separate basis for processing that personal data will be established.
Please note that where UCL processes 'special categories of personal data' or criminal convictions data in its capacity as a public authority then a legal basis for processing

that personal data will need to be found in line with the GDPR in addition to the 'public task' ground.
For more details on UCLs use of ‘Public Task’ please see the document:

UCL statement of tasks in the public interest August 2018

UCL statement of tasks in the public interest August 2018

Click here to return to Index page

Guidance on writing a privacy notice

Guidance on writing a privacy notice

The General Data Protection Regulation (GDPR), prescribes that you should be open and fair with individuals about what personal data you are collecting, for what purpose and for how long. You can do this is through a 'Privacy Notice' (sometimes called a 'Fair Processing Notice' or 'Information Sheet').

example of a local privacy notice Sept 2018

example of a local privacy notice Sept 2018

When do you need a Privacy Notice?

UCL has published 'Global Privacy Notices' to cover processing activities in three broad areas: staff, for students, and a 'General Privacy Notice' that covers wider requirements website use. Between them and in broad terms, these Global Privacy Notices will cover all processing of personal data that UCL undertakes. However GDPR places strong obligations on UCL to be transparent and fair to individuals about how it uses their personal data so 'local' privacy notices will often be required to provide such information. Use local privacy notices to:

Provide clear and detailed information to individuals about what you are doing with their personal data.

Convey fully on how you are using personal data that may not be sufficiently covered by the Global Privacy Notices.

When you wish to deviate from the details in these Global Privacy Notices.

Where should a 'Privacy Notice' be placed?

A 'Local Privacy Notice' should be placed at the initial point of collection and should be visible to the individual to ensure fairness of processing. This gives the individual an opportunity to read and review the notice prior to providing their personal data. Where possible, a layered approach using 'just in time' methodology should be used to make privacy notices as accessible and as meaningful as possible.

How do I prepare a 'Privacy Notice'?

For new Projects: If you are undertaking processing that is **likely to result in a high risk** to individuals' interests then you must complete a Data Protection Impact Assessment (**DPIA**) before starting your project. If you are unsure about the risk, we strongly recommend that you complete a DPIA. This will help you identify what types of personal data you are processing, the risks to privacy involved, and the safeguards or controls you will need to have in place to meet your statutory requirements.

For existing Projects: You should check any previous risk review you have previously undertaken as part your project for risks to privacyIf you had already identified these and put controls in place, it is unlikely that you will require a new DPIA.

If you have not completed a previous risk review with data protection elements, you *must* complete a Data Protection Impact Assessment **DPIA**
For all projects new or old, you must schedule in a review of your design against the original risk review to ensure that your purposes, and/or techniques have not changed.

Once you have defined the types of data you will be collecting as well as the processing which you will be undertaking, you can begin to describe these in your privacy notice.

How do I present my 'Privacy Notice'?

Note: If you are gathering data on individuals under the age of 18 please see the section below on 'Privacy Notices for Under 18s
Depending on the scale of your project, your privacy notice could become detailed. There is no prescribed length, however, your privacy notice should be clear, succinct and complete. To do this you can 'layer' your privacy notice – in the same way this guidance note is 'layered' through the concertina or 'roll up' effect. This allows the user to easily identify the areas they would like to read and focus on them.

Where can I check that I have completed my Privacy Notice correctly?

What information do we need to provide?	
The name and contact details of your organisation	✓
The name and contact details of your representative	✓
The contact details of your Data Protection Officer (email and address)	✓
The purposes of the processing	✓
The lawful basis of the processing	✓
The legitimate interests for the processing (if any)	✓
The categories of personal data obtained	✓
The recipients or categories of recipients of the personal data	✓
The details of transfers of the personal data to any third countries or international countries	✓
The retention periods for the personal data (see if your processing is covered under UCLs record retention schedule)	✓
The rights available to individuals in respect of the processing	✓
The right to withdraw consent (if consent is the basis of processing)	✓
The right to lodge a complaint with the ICO	✓
The source of the personal data (if required)	✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓
The details of the existence of automated decision-making, incliding profiling	✓

Privacy Notices for Under 18s

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

Your privacy notices must be clear, and written in plain, age-appropriate language. There is no prescribed "age-appropriate language", however, a good 'average' is a reading age of 14; ie. The language of your 'Local Privacy Notice' for persons under 18 should be readable for a 14 year old.

You should ensure that you use child friendly ways of presenting privacy information, such as diagrams, cartoons, graphics and videos, dashboards, layered and 'just-in-time' notices, icons and symbols.

You should explain to children why you require the personal data you have asked for, and what you will do with it, in a way which they can understand.

As a matter of good practice, you should explain the risks inherent in the processing, and how you intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

You *must* tell children what rights they have over their personal data in language they can understand.
As a matter of good practice, if you are relying upon parental consent then you should offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

How often should we review our Privacy Policy?

You should review your Privacy Policy at regular intervals against your DPIA prior to publishing to ensure you have captured the necessary information. It is good practice to schedule such reviews at regular intervals throughout your project. Privacy Polices should be updated when necessary to ensure that individuals are aware of any changes.

Where can I get further assistance?

You should write your 'Local Privacy Policy' yourself and check this against the **ICO Privacy Policy** checklist in the first instance
If you still require assistance you can contact the **Data Protection Team** for assistance.
Please note: the DPO team are not able to write Privacy Notices for you. They are able to review and answer specific questions related to your concerns.

Click here to return to Index page

Reporting a loss of personal data

Under the General Data Protection Regulation (GDPR) data controllers, such as UCL, have a responsibility to ensure that the personal data they are processing is done in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

In cases where there has been an incident which resulted in a potential breach of the GDPR, it is imperative that you report this immediately to Information Security Governance.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Examples of reportable breaches and 'near misses'

While this list is non-exhaustive it does give examples of some of the more common data breaches and 'near misses' that should be reported.

- Accessing personal data by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor affecting the security of personal data;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- altering personal data without permission;
- losing the availability of personal data; and
- any 'near miss' incident that had the potential to cause a data breach even though it might not have done so.

Potential consequences and the effect of a breach

Whilst UCL could face potential fines of €20m or 4% of global turnover for data breaches, it is often the unseen consequences that have a greater impact, for example the harm to the individual. A breach resulting in privacy harm to an individual could leave them with lasting damage and could result in secondary consequences for the individual.

Furthermore, Article 28 notes that "the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." As such, one consequence of a data breach could be that a 3rd party organisation does not recognise that UCL can provide sufficient guarantees

and therefore stop the transfer and/or processing of data. This could have a detrimental impact on UCLs core business.

Method of reporting

The Information Security Group (ISG) and The Data Protection Officer (DPO) are responsible for handling data breaches. If you believe there has been a breach of personal data you must complete the **form** and send it to ISG **isg@ucl.ac.uk** or (0)20 7679 7338 (internal 37338).

If the breach relates to electronic records you should also notify your local computer representative.To identify and assess the nature of the breach, you should provideISG with the following information:

- full details as to the nature of the breach;
- an indication as to the volume of material involved;
- the sensitivity of the breach; any timeframes that apply.

What happens next?

Once ISG has been notified, they will work with the DPO to undertake an assessment of the breach and carry out an investigation. Where there is evidence of a breach it is important to ensure that processes and practices are in place to ensure it does not reoccur.

The key considerations will include:

- the potential harm to the data subjects(s);
- the sensitivity of the data;
- the volume of data.

ISG and the Data Protection Office will notify the ICO of all data breaches. You should ensure that you record all breaches.

Key points to consider

- Compliance with the GDPR is NOT optional;
- Report any loss of personal data to the Information Security Group immediately;
- Advise staff and students on the implementation of and compliance with the UCL Data Protection policy and any associated guidance/codes of practice;
- Ensure appropriate technical and organisational measures are taken to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- Support UCL's notification with the ICO by maintaining a register of holdings of personal data, including databases and relevant filing systems, and the purposes of processing.
- Undertake the current **DPA and ISG training**

Click here to return to Index page

Art. 6 GDPR Lawfulness of processing

1. [1]Processing shall be lawful only if and to the extent that at least one of the following applies:

    1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    3. processing is necessary for compliance with a legal obligation to which the controller is subject;

    4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

    [2]Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. [1]The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

    1. Union law; or

    2. Member State law to which the controller is subject.

4. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [3]That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the

types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

5. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

    1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

    2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

    3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

    4. the possible consequences of the intended further processing for data subjects;

    5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Suitable Recitals

(39) Principles of data processing (40) Lawfulness of data processing (41) Legal basis or legislative measures (42) Burden of proof and requirements for consent (43) Freely given consent (44) Performance of a contract (45) Fulfillment of legal obligations (46) Vital interests of the data subject (47) Overriding legitimate interest (48) Overriding legitimate interest within group of undertakings (49) Network and information security as overriding legitimate interest (50) Further processing of personal data (171) Repeal of Directive 95/46/EC and transitional provisions

Click here to return to Index page

Statement of Tasks in the Public Interest

1. Introduction

Whenever UCL uses personal data, it needs to establish a legal basis for doing so in line with the General Data Protection Regulation (GDPR).

One of these legal bases is the 'public task' ground. This will apply where the processing of personal data is necessary in order to perform a task in the public interest which is laid down by law, or in the exercise of official authority laid down by law.

Universities are classed as public authorities for the purposes of data protection law. Current guidance issued by the UK Information Commissioner's Office (ICO) indicates that the 'public task' ground for processing is likely to apply to much of the processing of personal data carried out by universities, depending on the detail of their constitutions and legal powers. However, the ICO also states that where a university's processing is separate from its tasks as a public authority, other legal bases may be more appropriate.

UCL processes personal data in relation to a wide variety of activities and not all of those activities will be undertaken in UCL's capacity as a public authority. This statement looks to clarify when UCL will be carrying out tasks in the public interest in its capacity as a public authority and therefore can rely upon the 'public task' ground for processing personal data set out in the GDPR.

This statement draws upon UCL's Charter and Statutes, which establish the purposes for which the University was incorporated and its related powers, and UCL's 2034 strategy.

2. Establishing a legal basis for processing

Where UCL processes personal data in connection with the carrying out of tasks in the public interest in its capacity as a public authority, UCL should rely on the 'public task' ground as its lawful basis for processing that personal data.

Where the processing of personal data by UCL is separate from UCL's tasks as a public authority, a basis for processing that personal data other than the 'public task' ground is likely to be the most appropriate one to use.

Please note that where UCL processes 'special categories of personal data' or criminal convictions data in its capacity as a public authority then a legal basis for processing that personal data will need to be found in line with the GDPR in addition to the 'public task' ground.

Further guidance on the topic of establishing a legal basis for processing personal data is available on UCL's GDPR website.

3. Circumstances in which UCL acts in its capacity as a public authority

A. UCL's core purposes

UCL will be carrying out tasks in its capacity as a public authority when it carries out the following tasks.

Category	Description
Education Core Purpose	
Education	Providing courses of education at undergraduate and postgraduate level, engaging with and providing educational opportunities and resources to the wider public, demonstrating academic leadership and making UCL a global educational establishment. This includes: • providing educational courses in a variety of forms, such as online, face-to-face and distance learning • teaching on undergraduate and postgraduate courses • arranging and facilitating student placements and exchanges • running summer schools • providing continuing professional development • providing executive education • providing a range of personal learning courses • carrying out cross-disciplinary educational activities • carrying out ancillary activities to facilitate the provision of educational courses, such as teacher development
Qualifications	Awarding recognised forms of undergraduate and postgraduate level educational qualifications such as degrees, diplomas and certificates. This includes where UCL cooperates with other institutions to award joint degrees and other qualifications.
Awards and prizes	Founding and awarding scholarships, bursaries, studentships, medals and prizes.
Publication of educational material	Providing, publishing and distributing educational material in a variety of forms, including to members of the public.
Research Core Purpose	
Research	Facilitating and carrying out research in any field and encouraging and carrying out research that looks to address global challenges and provide long-term benefits to humanity. This includes: • research carried out by students at both undergraduate and postgraduate level • research carried out by UCL staff • research carried out jointly with third parties • supervising research students • encouraging and facilitating cross-disciplinary research • carrying out ancillary activities to facilitate and support research, such

Category	Description
	as purchasing research-specific technology • publishing research papers, articles, books etc. It may include research which is entirely funded by private companies.
Innovation Core Purpose	
Innovation	UCL sees innovation in the fields of education and research, including the commercialisation of UCL's research, as part of its core purposes. This includes: • knowledge exchange and enterprise activities • developing research and innovation excellence across UCL • finding creative solutions to global social issues • showing academic leadership in the field of innovation • the creation of 'innovation clusters' around UCL • providing relevant skills and training to students and staff • providing advice and mentoring, encouraging start-ups and the creation of spin-offs • supporting student entrepreneurship societies • the activities of UCLB • the activities of UCL Innovation and Enterprise

B. Ancillary activities linked to furthering UCL's core purposes

UCL will be carrying out tasks in its capacity as a public authority when it carries out the following tasks, which are seen as being carried out to further UCL's core purposes of education, research and innovation.

Category	Description
Facilities	
Facilities	The provision and maintenance of facilities such as libraries, museums, labs, classrooms, residential accommodation, club premises, sports fields, lands, furniture, apparatus, equipment and books, in addition to IT services and facilities.
Goods and services	The procurement of goods and services to facilitate or further UCL's core purposes.
Governance	
Governance	The governance of UCL, including the exercise of the powers and duties of the Council, the Academic Board and other individuals involved in the governance of UCL.
Planning	

Category	Description
Planning	This includes UCL's strategic and operational planning and coordination activities, including those activities undertaken as part of the implementation and delivery of UCL 2034.
Staff	
Management of UCL staff	This includes establishing or abolishing both academic and non-academic posts, appointing candidates to roles, removing staff from roles and determining the terms of employment contracts, staff pay and benefits.
Payment of salaries, pensions and benefits	The payment of staff members' salaries and pensions, including to employees' widows or widowers and dependants, and the provision of benefits to staff members.
Financial	
Grants	Soliciting, receiving and administering grants, donations, gifts and loans of all types of property (including IP).
Trustees	Acting as trustees or managers of property, endowments etc. for the purposes of education or research.
Investment	Investing money in accordance with UCL's Charter and Statutes.
Fees	Demanding and receiving fees, subscriptions and deposits.
Guarantees	Giving guarantees to financial and commercial institutions.
Raising funds	Borrowing and raising money, including the charging of UCL's assets as security. Building UCL's endowment funds in order to support students from low income backgrounds, including as part of UCL 2034.
Property	
Property	Acquiring, constructing, maintaining and managing real and other property. This includes working on projects to create educational, research and cultural hubs both in the UK and overseas.
Insurance	
Insurance	Making appropriate insurance arrangements. This includes putting in place insurance for Council members in respect of criminal prosecution brought against them in the course of carrying out their roles.

Category	Description
Third party relationships	
Relationships with other educational institutions	Maintaining and developing UCL's relationships with other educational institutions. This includes developing relationships with schools and higher educational institutions around the world to promote education, research and innovation and to establish UCL as London's Global University.
Charities	Subscribing to charities and granting charitable donations.
Amalgamation	Amalgamating with educational or research institutions with the same or similar charitable purposes.
Strategic partnerships	Building and maintaining strategic partnerships with third party organisations such as the NHS, private businesses and government agencies.
Students' Union	
Students' Union	This includes activities in relation to the Students' Union.
Student recruitment and experience	
Student recruitment	This includes working with schools to raise aspirations and to help recruit students from under-represented groups at UCL.
Student experience	Working to achieve high levels of student satisfaction and to become a world leader in the use of technology to enhance student experience and the quality of learning. This also includes the provision of student support services.
University of London	
Exercise of University of London powers	UCL is a member of the University of London. This category includes exercising the powers of the University of London as authorised by the University of London.

4. Further information

If you have any questions on this statement, please contact the data protection team at data-protection@ucl.ac.uk.

Click here to return to Index page

'Legitimate interests' as a lawful basis for processing personal data

The focus of the guidance is on using the 'legitimate interests' basis for processing personal data.

Scope

This guidance applies to UCL employees who are looking to process *personal data*, i.e. information relating to an identified or identifiable living person, and are looking for a lawful basis to do so.

Note that 'processing' means any operation - collecting, storing, using, transferring, disclosing or destroying - performed on personal data.

Legal basis for the processing of personal data

Before processing any personal data, an appropriate legal basis must be identified.

Article 6(1) of the GDPR sets out the following six possible legal bases for processing personal data:

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

As a public authority, most of UCL's processing will be undertaken using Article 6(1)(e) above, the 'public task' condition. This applies when the processing is necessary for UCL to perform a task in the public interest. Examples include most of UCL's research, teaching and learning activities – we can clearly demonstrate a 'public task' basis for these because performing such tasks is a core part of UCL's Charter and Statutes.

It is important to understand where UCL's processing falls under the 'public task' condition because you can only rely on 'legitimate interests' at Article 6(1)(f) above if you are processing for a legitimate reason other than performing UCL's tasks as a public authority. UCL has produced a **Statement of Tasks in the Public Interest,** which sets out when the 'public task' condition can be used as a basis for processing.

Please note that you cannot rely upon either the 'public task' basis or the 'legitimate interests' basis alone when processing: (a) special category personal data (e.g. data relating to ethnicity, health, religion etc.); or (b) personal data relating to criminal convictions or offences. If you are processing data of this kind, you will need to establish an additional lawful condition under either Article 9 or Article 10 GDPR (as applicable).

Legitimate interests

Legitimate interests is the most flexible lawful basis for processing, but if you choose to rely on it, you are taking on extra responsibility for considering and protecting people's rights and interests, including privacy rights.

There are three elements to the legitimate interests basis and a corresponding three-part test:

1. Identify a legitimate interest: what interest are you pursuing?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interest?

You should avoid relying on 'legitimate interests' if you plan to use personal data in ways people do not understand and would not reasonably expect, or if you think people would object after it was explained to them. You should also avoid 'legitimate interests' for processing that could cause harm.

Identify a legitimate interest

The first stage is to identify a legitimate interest.

An 'interest' can be understood widely. It can be a broad stake that UCL or any third party may have in the processing or the benefit to be derived from the processing. An interest must be *real and present*, something that corresponds with current activities or benefits in the very near future and not vague or speculative; be *sufficiently clearly articulated* to allow for a balancing test to be carried out; and be *lawful*. Interests can be commercial, individual or even broader societal benefits.

Some interests are likely to be 'legitimate' because they are necessary for an administrative function or compliance issue. This is often the case when the processing is not required by law, but the processing is essential to ensure UCL meets external or internal governance obligations, for example, the provision of physical or network security or holding marketing suppression lists to prevent spamming.

Other interests are considered legitimate on the basis that while they do not fall within scope of the 'public task' condition, they support UCL's core business functions, for example activities around graduation and the provision of an alumni newsletter.

Interests are more likely to be legitimate interests when:

i. there is a relevant and appropriate relationship between UCL and the individual, for example between UCL and its alumni, and

ii. the processing is within the reasonable expectations of the individual.

Necessity test

The second stage is to carry out a necessity test.

You will need to consider whether the processing of personal data is 'necessary' for achieving the objective. 'Necessary' in this context means that the processing should be a targeted and proportionate way of achieving your objective.

It is useful to ask, 'Is there another way of achieving the identified interest?' If there is no other way, then clearly the processing is necessary. 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 Data Privacy Impact Assessment (DPIA) can be used to identify the least intrusive processing activity. Guidance on PIAs can be found here: https://www.ucl.ac.uk/legal-services/research/data-privacy-impact-assessment

If the processing is not necessary, then 'legitimate interest' cannot be relied on as a legal basis for that processing activity.

Balancing test

The third stage is to balance the legitimate interest against the rights and freedoms of the individuals whose personal infirmation you are proposing to process.

This balancing test must 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 UCL's legitimate interest, including:

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

i. the nature of the interests includes:

- the reasonable expectations of the individual: would they expect the processing to take place? If so, then the impact of the processing is likely to have already been considered by them and accepted. If they have no expectation that any processing would take place, then the impact is greater and is given more weight in the balancing test

- the type of data: children's personal data or data where there is more expectation of privacy, e.g. salaries, should be consider in a balancing test, and

- the interests of UCL (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?

ii. the impact of processing includes:

- any positive or negative impacts on the individual, any bias or prejudice to UCL, third party or to society of not conducting the processing

- the impact on children. Data protection legislation obliges UCL to consider the interests of children in particular so consider carefully what impact your proposed processing will have on them

- 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?

iii. 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 DPIA, for example:

- data minimisation;
- de-identification;
- additional layers of encryption;
- data retention limits;
- restricted access opt-out options;
- pseudonymisation or anonymisation;
- encryption, hashing, salting.

When UCL 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.

Further guidance and template download

We hope that you find this guidance helpful. If you require any further information on the issues raised in this document, please contact the data protection team at **data-protection@ucl.ac.uk**.
Download the Legitimate Interests Assessment template

Legitimate Interests Assessment (.docx)


Legitimate Interests Assessment (.docx)

Click here to return to Index page