Data Protection Impact Assessment (DPIA) Procedure

Business Assurance
Version: 2.0

1. *Introduction and keypoints*

1.1. This procedure covers when and how to conduct a Data Protection Impact Assessment (DPIA), as well as providing examples of risks and mitigating actions.

1.2. The implementation of this procedure will help to:

- provide support and information to those who need to conduct DPIAs, including advice on how to identify when they arerequired;
- clarify the responsibilities of those involved in conducting a DPIA;
- protect the rights and freedoms of individuals in relation to theirprivacy;
- minimise the university's exposure to legal and regulatory consequences, financial loss and reputationaldamage; and
- demonstrate compliance with data protection legislation by documenting issues considered and decisions made;

1.3. Benefits of conducting a DPIA include:

- Early identification of issues and risks, leading to cost savings and better compliance.
- Increased awareness of data protection issues.
- Improved trust, transparency, and accountability.

1.4 This procedure aligns with the ICO Guidance on Data Protection Impact Assessments.

1.5 It describes roles and responsibilities of individuals involved in conducting a DPIA including: responsible staff members, Information Compliance team members and the Data Protection Officer (DPO).

2. Why Conduct a DPIA?

2.1 A DPIA is a process designed to help you systematically analyse, identify, and minimise the data protection risks of a project or plan. It is a key part of our accountability obligations under the UK data protection legislation, and when done properly helps you assess and demonstrate compliance with our data protection obligations.

2.2 DPIAs are not just a compliance exercise. An effective DPIA allows you to **identify and fix problems at an early stage**, bringing broader benefits for both individuals and the university. DPIAs are fundamental to the Privacy by Design approach. You can use an effective DPIA throughout the development and implementation of a project or proposal, embedded into existing project management or other organisational processes.

2.3 DPIAs are also relevant if you are planning to make changes to an existing system. In this case you must ensure that you do the DPIA at a point when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. **It is vital to integrate the outcomes of your DPIA back into your project plan.**

2.4 By considering the risks related to your intended processing before you begin, you are following sound project planning. You should always consider and mitigate the risks of any activity before

that activity is undertaken. DPIAs are part of this wider risk assessment process.

2.5 Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information you collect where possible and devising more straightforward processes for staff.

2.6 A DPIA does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

3. How and When to Conduct a DPIA

3.1 DPIAs must be completed for new projects or processing activities (or changes to existing ones) which are 'likely to result in a high risk' to the rights and freedoms of individuals (see Appendix 1 for examples).

3.2 A DPIA does not need to be carried out for every processing activity which may result in risks, only those likely (over 50%) to result in risks to the rights and freedoms of individuals. If in doubt, a DPIA should be completed.

3.3 To help you carry out your DPIA, the College has provided a template which covers all the areas you need to think about when undertaking a high-risk processing activity where a DPIA would be mandatory. You should employ the template proportionate to the risk of the processing using this guidance as a starting point. In some circumstances, when onboarding a new supplier for an existing legitimate processing activity for example, the College's Data protection due diligence questionnaire for third parties may be more appropriate. If you are transferring personal data outside the UK/EEA and need to complete a Transfer Risk Assessment please refer to our Guide to International Transfers.

3.4 Proportionality is key: the higher the risk, the greater the checks should be. Relevant factors to consider are included in Appendix 1.

3.5 A DPIA can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing DPIA if it covered a similar processing operation with similar risks. A group of controllers can also do a joint DPIA for a group project or industry-wide initiative.

3.6 DPIAs should be completed as early as possible and before processing of personal data.

3.7 You should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. **You need to keep it under review and reassess if anything changes.**

3.8 The requirements of this procedure must be applied in conjunction with all applicable university policies and procedures, including, but not limited to:

Data Protection Policy
Information Security Policies
Research Data Management Policy

4. Roles and responsibilities

For key definitions please see Appendix 6. For further data protection related definitions, please see the glossary on the Information Compliance intranet pages.

4.1 Staff managing projects to implement new (or update existing) systems or procedures which involve the processing of personal data, are responsible for identifying if a DPIA is required and then completing the form accordingly. They are also responsible for seeking advice on the DPIA from the DPO via the Information Compliance team.

4.2 The DPO and Information Compliance team are responsible for providing advice on how to complete DPIAs, keeping records of completed DPIAs, and liaising with the Information Commissioner's Office (ICO) if residual risks are outstanding. For mandatory DPIAs the DPO will sign the completed form to show that the DPIA has been carried out correctly and advise on whether the processing should go ahead or not.

4.3 The IT Assurance team are responsible for providing the necessary advice and assistance on any appropriate technical measures which need to be taken to keep personal data secure and prevent unauthorised loss or access.

4.4 The Research Governance Office (RGO) are responsible for advising on research specific DPIAs escalating to the DPO where appropriate.

4.5 You may want to ask a processor to carry out a DPIA on your behalf if they do the relevant processing operation, but again you remain responsible for it.

5. *DPIA Process*

The following steps should be undertaken before processing has started, and these may need to be repeated at various later stages.

Step 1: Identify if a DPIA is needed

- Is personal data being processed? If 'no', no DPIA needs to be completed as data protection law only applies to the processing of personal data. If 'yes', is processing likely to result in a high risk to the privacy of individuals? (see Appendix 1). If 'yes', a DPIA will need to be completed. If 'no', keep a record that no DPIA is required. If in doubt, check with the Information Compliance team.
- A DPIA does not need to be carried out where the specific activity is mandated by law.
- A DPIA may need to be carried out for existing high-risk processing operations.

Step 2: Complete the DPIA form and return this to the Information Compliance team (or the Research Governance Team for research DPIAs)

- The DPIA form can be found at Appendix 4 or Appendix 5 (research only).
- The DPIA must include a description of the proposed or existing processing.
- There should be an assessment of whether the processing is necessary and proportionate to the purposes identified.
- A lawful basis for processing must be identified.
- Any risks to the rights and freedoms of individuals (data subjects) should be identified. See Appendix 2 for examples of risks.

Step 3: Risk assessment and identification of mitigating actions

- The likelihood and severity of the risks may need to be assessed, and then mitigating actions proposed and documented. This can be done through discussions with the Information Compliance team.
- Mitigating actions should be proportionate to the risks. They should ensure that:
  - any processing has identified a lawful basis and has specific, explicit and legitimate purposes;
  - processing is adequate, relevant and limited to the necessary data;
  - personal data has a limited storage duration and clear retention period;
  - the necessary information about the processing is provided to data subjects to ensure transparency;
  - data subjects' rights of access, data portability, erasure, rectification, and objection to processing can be upheld where appropriate; and
  - personal data is held and transferred securely, especially when transfers are international.

Step 4: Implementation of mitigating actions and consultation

- Any recommended mitigating actions should be implemented (where costs are proportionate to risks).
- Consultation with internal stakeholders, external stakeholders and data subjects may be appropriate.
- Appropriate consultation with internal stakeholders might include members of a project team, IT, Procurement, Internal Communications, or senior management, as well as the Information Compliance team. Consultation with internal stakeholders will help to ensure that all the necessary privacy risks are identified, and appropriate mitigating actions put in place to reduce these risks.
- Consultation with external stakeholders may include external experts, data processors (third party service providers) or regulatory authorities.
- The views of data subjects should be sought where appropriate and if advised by the Information Compliance team. If the views of data subjects differ from those of King's, the reasons for deciding whether to proceed should be documented. It is also important to record why a decision is made not to consult data subjects, for example if the effort required would be disproportionate.
- Where the DPIA reveals high residual risks, the DPO will be required to consult with the ICO. Under the College Data Protection Policy the DPO is the university's sole point of contact with the ICO for any issues relating to data processing. This is when sufficient measures to reduce the risks to an acceptable level cannot be found. It is also required when UK law requires the data controller to consult with the relevant supervisory authority in relation to processing for the performance of a task.

Step 5: Sign-off and record keeping

- All the above steps, decisions, actions and mitigations should be recorded to demonstrate compliance, including decisions not to go ahead with the processing of personal data.
- The DPO will advise whether they think processing can proceed or not.
- The ICO recommends that DPIAs are published in whole, or part, although this is not a mandatory requirement.
- If the processing activity is a new one, it should be added to the university's Record of Processing Activities. For further details, contact the Information Compliance team.
- The DPIA should be reviewed by the project lead throughout the various project stages, and when any changes are made the DPIA should be updated accordingly.

5 Links to useful resources

- KCL Information Compliance intranet pages
- KCL mandatory data protection training
- ICO data sharing code of practice
- ICO DPIA Guidance
- Article 29 Working Party guidance on high risk processing and DPIAs

6 Contact details for queries in relation to this procedure

Information Compliance team info-compliance@kcl.ac.uk 020 7848 7816

Appendix 1: Examples of Activities that Require a DPIA

Before conducting a DPIA you need to consider whether one is required. The screening question whether the **processing is of a type likely to result in a high risk**. Are there any red flags which point to the potential for high risk?

The ICO has published a list of processing activities which should always require a DPIA:

- Systematic monitoring of a publicly accessible area on a large scale, e.g CCTV in public areas.
- Denial of service: Decisions about an individual's access to a service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
- Biometric or genetic data processing. Processing of patients' genetic or health data including medical research.
- Where innovative or new technologies are being applied, such as facial recognition or AI. Innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you/the university.
- Tracking: processing which involves tracking an individual's geolocation or behaviour. Including systematic monitoring of employees' behaviour e.g. work station activity, internet use.
- Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals. For example, cases of whistleblowing/complaint procedures
- Gathering of public social media data for generating profiles (profiling).
- Direct marketing
- Storage for archiving purposes of pseudonymised personal sensitive data concerning vulnerable subjects of research projects or clinical trials.
- Processing of personal data from patients or clients by an individual physician, lawyer or health care professional.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Implementing existing technology in a new way, such as a new database which consolidates information held by separate parts of King's.
- Policy or strategies which will impact on privacy through the collection or use of information.
- Assessment of the data protection for a technology product e.g. a piece of hardware or software.
- Where a systematic and extensive evaluation of individuals is being carried out based on automated processing, including profiling, which may have significant impacts on the individuals. This might include evaluation of performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, or creation of personal profiles.
- When there is large scale processing of sensitive personal data or special categories, including criminal convictions, racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, processing of genetic data, data concerning health or sex life, or other types of data which may be personal to individuals (such as bank account and salary information).

- Where data is being processed on a large scale with a large number of data subjects, a large volume of data, a long processing duration or large geographicalarea.
- Where datasets containing personal data are being matched orcombined.
- Where data concerns vulnerable subjects including children, ill persons/patients, asylum seekers. Employees and students can also be considered vulnerable individuals due to the employer/employee student/staff power imbalance meaning they cannot easily consent or object to the processing of their data.
- Invisible processing: processing of personal data that has not been obtained directly from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a university tracking real-time location of staff/students;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.

Individual professionals processing patient or client data are not processing on a large scale.

For more guidance on these factors, read the WP29 guidelines (WP248). These guidelines give background on the reasoning for the high-risk indicators, and further examples of processing likely to result in high risk.

You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high risk, but you should document your reasons.

Appendix 2: Examples of Risks

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

To Individuals

- Physical, material or non-material damage, in particular:
- where the processing may give rise to discrimination,
- identity theft or fraud,
- financial loss,
- damage to the reputation,
- loss of confidentiality of personal data protected by professional secrecy,
- unauthorised reversal of pseudonymisation, or
- any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data

Examples of activities that might increase the likelihood of the above risks manifesting:

- Information is inaccurate, insufficient or out of date.
- Information is excessive or irrelevant.
- Information is retained for too long.
- Information is disclosed to unauthorised persons.
- Information is used in ways that are unacceptable or unexpected by the data subjects.
- Information is not kept securely.
- Unjustified intrusion from surveillance.
- Incomplete anonymisation.

Corporate risks

- Reputational or financial risks to King's.
- Loss of business, funding or trust.
- Non-compliance with legislation and consequent fines.

Appendix 3: Examples of Mitigating Actions

- Compliant contracts with data processors (third party service providers) should be in place to ensure personal data is managed securely and appropriately by third parties.
- Data sharing agreements should be in place between joint data controllers.
- Clear and transparent privacy notices must be in place.
- Appropriate lawful basis for processing personal data must be clearly identified.
- Data subjects should be consulted where appropriate.
- Appropriate organisational measures (policies, procedures, training) and technical measures (encryption, access restriction, secure storage) should be put in place to ensure the security of personal data. IT should advise where necessary.
- Data minimisation – processing only the minimum amount of personal data required.
- Pseudonymisation (see glossary) and anonymisation of data as an appropriate safeguard.
- Clearly defined retention periods and secure destruction of data when no longer required.
- Training and guidance for staff.

Department of Business Assurance
Information Compliance
Tel: 020 7848 7816
Email: info-compliance@kcl.ac.uk

DATA PROTECTION IMPACT ASSESSMENT

This document is designed to identify privacy and data protection risks. Please complete with as much detail as possible and return the document to the Information Compliance team for review.

Screening Questions – Do I need a Data Protection Impact Assessment?

Question	Y/N
Are you going to be collecting information about vulnerable data subjects? (e.g. children, vulnerable adults, patients)	
Will the information be disclosed to organisations or people who have not previously had access to the information? (e.g. a research partner or institution, another department within King's)	
Will the information be used in a way that it is not currently used? (e.g. to send text messages about revision sessions)	
Will you make decisions about individuals or act against them as a result of collecting or using the information? (e.g. to decide whether to offer an additional tutoring service based on exam results)	
Are you using new technology that could be intrusive? (e.g. biometrics or facial recognition)	
Is the information that you are collecting or using sensitive information (e.g. health records, criminal records, religious beliefs – see definitions in procedure for full list) or information that may be perceived as sensitive to individuals (e.g. salary, bank account details, copies of passports)?	
Will you contact the individuals in a way they might find *intrusive* (e.g. telephone calls, emails to personal email addresses)	
Is the processing of personal data 'large scale'? Are many data subjects involved? Does the project cover a large geographical area? Does it cover a very long period? Is there a variety of different types of data being processed?	

Is more than one dataset containing personal data being matched or combined?	
Will systematic monitoring of individuals be taking place? (e.g. CCTV)	
Is the processing otherwise likely to result in a high risk to the freedoms or rights of individuals? Will the processing prevent data subjects from exercising their rights? See guidance on data subject rights	
Will personal data be transferred out of the EU/EEA?	

If your answer to any of these questions is 'yes' a full assessment will usually be required. If not, but personal data is still being processed, please contact Information Compliance with a summary of your project for further advice.

Step 1: Why do I need a Privacy Impact Assessment?

Project Summary/Description of Processing
Please provide a summary of your project. You can attach a brief proposal or other document if available. Please state if more than one processing activity is covered by this DPIA. Please include the nature, scope, purposes and context of the processing and describe any relevant hardware, software, networks or people who may be relevant. Please also include reference to any relevant codes of practice, legislation or funding contracts which may be relevant. What are the projected outcomes of the project?
Screening Questions
Please provide more details about the 'Yes' responses to the screening questions
Example of Dataset
Please provide an example of your dataset, including all the categories of personal data that will be processed.

Step 2: The Data Flow

Collection of Data	
What data will be collected and from whom? How many individuals?	

Why is this data collection necessary?	
Who will be collecting the data?	
What method of collection will you use?	
Will you be obtaining consent? If so, how will this be captured and documented?	
What information will be provided to the data subjects about how their personal data is handled? *Please attach any privacy notices you intend to use*	
What is the lawful basis for processing the personal data? E.g. necessary for a contract, necessary for our public task, consent, etc	
How many individual datasets will you collect?	
Use of Data	
What decisions/actions will be taken using the data?	
Who will have access to the data?	
Will the data be transferred to third parties? Is so, are any of these third parties outside of the EEA? Are there any data sharing agreements, or contracts with data processors in place? Please see the guide to data sharing. Will a third party be making decisions about the data?	
How will any third parties process the data?	
Who will be responsible for accuracy and corrections, or considering deletion of personal data if requested in line with the rights of the data subjects?	
How will you handle any objections to processing or, where relevant, withdrawal of consent?	
Will data portability be possible?	
Storage, Access (including third party providers)	
Where will the data be stored?	
How will access be restricted?	

Will data be anonymised? *Please see the ICO code of practice on anonymisation*	
Who is the data controller (who determines the manner and purpose of the processing)?	
Retention and Deletion	
Estimated length of data cycle	
For how long will you keep the data? Please include justification	
How will it be destroyed?	
Security	
What measures will be in place to keep the data safe and secure?	
Will the data be transferred outside the EU/EEA? If so under what grounds?	
Will children's data (generally under 13 years old) be collected as part of the project? If 'yes', how will consent be obtained from a parent/guardian?	
Will the data of other vulnerable individuals be processed? If so what measures will be in place to protect them?	

Step 3: Consultation

Should any other persons/departments be consulted about this project? Please list all relevant stakeholders who will be affected by this processing.

Please enter the comments of any persons here

Have any data subjects been consulted for their views on this processing?

Please enter the comments of any persons here

Has an Equality Analysis been completed for this project?

King's has a responsibility to consider the impact of decisions on individuals beyond how we process personal data. We have an obligation to demonstrate our considerations for protected groups. Please enter the summary from a completed Equality Analysis or explain why it is not relevant to the processing.

Step 4: Identifying the data protection risks and mitigating actions

Data protection issues/risks identified *See Appendix 2 for examples and consult the Information Compliance team*	Recommended actions to mitigate the risks *See Appendix 3 for examples and consult the Information Compliance team*	Residual risks *Are the initial risks eliminated, reduced or the same? If reduced, what risk remains?*	Date actions implemented/ to be implemented

Step 5: DPO advice

The DPO has reviewed this DPIA and advises that the processing can proceed as outlined, subject to the above actions being implemented.

DPO signature, date and comments

OR

The DPO has reviewed this DPIA and advises that the processing should not proceed as outlined due to the high residual risks. Processing cannot proceed without consulting the ICO first.

DPO signature, date and comments

Research Governance Office

57 Waterloo Road
London
SE1 8WA

RESEARCH: DATA PROTECTION IMPACT ASSESSMENT

Every researcher who collects, stores, shares, and otherwise uses personal data from research project participants is responsible for ensuring that these data are processed lawfully.

The Information Commissioners Office (ICO) provide a list of criteria where the data processing is 'likely to result in high risk' to the data subjects (your research participants) and a DPIA is required. Please consult this list and complete the DPIA if any of the criteria apply to your project.

This document is designed solely to identify privacy and data protection risks for research projects which are subject to Research Ethics approval. For all other processing activities, or if you are unsure which DPIA to complete, please review this guidance on the Information Compliance DPIA webpage.

Please complete this form with as much detail as possible and return it to the Research Governance Office for review rgo@kcl.ac.uk

For further information and advice on research DPIAs, please see the Research Governance Office webpages: RGO - DPIA

ICO Criteria

i.	Please select the ICO DPIA criteria that apply to your project
	A DPIA is only mandated if certain criteria are met. Please summarise below which of the ICO's criteria apply to your project. The ICO criteria can be seen on the 'When do we need a DPIA?' section on the ICO website. **Please note – if you do not meet the ICO criteria then you do not require a DPIA for your project.**

Part 1: Description of processing

ii.	Project Summary
	Please provide a summary of your project's data processing below including your research objectives. Attach relevant supporting documentation (draft or final versions) including your PIS and/or supplementary privacy notice, Research Data Management Plan, and any contracts/data-sharing agreements.

iii. Collection of Data	
What personal data types will be collected and from whom?	
How many individuals will data be collected from?	
If you are processing special category data, please state how this data processing is tied to your research objectives	
Who will be collecting the data?	
What method of data collection will you use? *If this involves use of new technology, please outline this here*	
Is more than one dataset containing personal data being matched or combined?	
What information will be provided to the data subjects about how their personal data is handled? *Please attach any PIS or privacy notices you intend to use. PIS should link to Statement on Use of Personal Data in Research notice.*	
iv. Use of Data	
Who is the data controller (who determines the manner and purpose of the processing)? *If this is not KCL, please provide additional details of the Data Controller*	
Who will have access to the data?	
What decisions/actions will be taken using the data?	
Will the data be transferred to third parties? *This includes storing data on third party platforms, sending to transcription/ translation services etc. If 'no' please jump to the Storage and Security section.*	
Are there any data sharing agreements, or contracts between parties in place?	

Have your data-sharing agreements been reviewed by the Research Contracts team?	
Are any of these third parties outside the EEA?	
How will these third parties process the data?	
Will a third party be making decisions about the data?	
Who will be responsible for accuracy and corrections, or considering deletion of personal data if requested in line with the rights of the data subjects?	
How will you handle any objections to processing or, where relevant, withdrawal of consent?	
Will data portability be possible?	
v. Storage and Security	
Where will the data be stored during and after the research? *E.g. will it be stored on King's systems such as OneDrive, SharePoint, KORDS etc. or on external software? Where multiple storage solutions apply please list themall here.*	
How will access be restricted?	
Will there be any connection of external software to King's IT infrastructure? *Connections to King's IT infrastructure should be flagged with itassurance@kcl.ac.uk*	
Will data be anonymised? At what point will anonymisation of the data take place? *Please see the ICO code of practice on anonymisation*	
vi. Retention and Deletion	
Estimated length of data collection cycle	
How long will identifiable/pseudonymised data be retained? *Please check the Research section of King's Records Retention Schedule*	

How will the data be destroyed?	
vii. Security	
What measures will be in place to keep the data safe and secure?	
Will children's data (generally under 13 years old) be collected as part of the project? If 'yes', how will consent be obtained from a parent/guardian?	
Will the data of other vulnerable individuals be processed? If so what measures will be in place to protect them?	
viii. Additional Governance	
Has the project a Research Data Management Plan? (If 'yes', please attach)	
Has the project received Research Ethics Committee (REC) approval?	
REC name (if relevant)	
Ethics application/ approval reference (if relevant)	
Has the project been added to King's Data Protection Register? *Please note, you only have to register on KDPR if you did NOT receive ethical approval through REMAS,*	
Do you have measures in place to ensure you are able to comply with your funder/sponsor data-sharing or Open Access obligations?	

Part 2: Risk Table: Data protection risks and mitigating actions

Data protection issues/risks identified *See Appendix 2 of the DPIA Procedure for examples*	Recommended actions to mitigate the risks *See Appendix 3 of the DPIA Procedure for examples*	Residual risks *Are the initial risks eliminated, reduced or the same? If reduced, what risk remains?*	Date actions implemented/ to be implemented

Part 3: RGO review

☐	The RGO has reviewed this DPIA and advises that the processing can proceed as outlined, subject to the above actions being implemented. The RGO have determined that DPO sign off is not required.
☐	The RGO has reviewed this DPIA and advises that the processing can proceed as outlined, subject to the above actions being implemented. The RGO have determined that DPO sign off is required.
☐	The RGO has reviewed this DPIA and advises that the processing should not proceed as outlined due to the high residual risks. Processing cannot proceed without consulting the DPO first.
RGO signature, date and comments	

Part 4: Where DPO sign off is required

☐	The DPO has reviewed this DPIA and advises that the processing can proceed as outlined, subject to the above actions being implemented.
☐	The DPO has reviewed this DPIA and advises that the processing should not proceed as outlined due to the high residual risks. Processing cannot proceed without consulting the ICO first.
DPO signature, date and comments	

Appendix 6: Key Definitions

6.1 **Personal data**: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including name, ID number, location data or online identifier.

6.2 **Sensitive personal data**: special categories of personal data that could cause harm or distress to an identifiable individual if released, including information relating to an individual's:

6.2.1 racial or ethnic origin;
6.2.2 political opinions;
6.2.3 religious or philosophical beliefs;
6.2.4 trade unionmembership;
6.2.5 physical or mentalhealth;
6.2.6 sex life or sexual orientation;
6.2.7 genetic data;
6.2.8 biometric data where processed to uniquely identify an individual; and
6.2.9 criminal record

6.3 **Data subject**: the person about whom the data concerns.

6.4 **Data controller**: a person (this could be an individual or an organisation) who determines the purposes and means of the processing of personal data. If you do this as part of your role at King's, King's College London is the data controller rather than you as an individual.

6.5 **Data processor**: a person (this could be an individual – other than an employee of the data controller – or an organisation) who may be instructed to process personal data on behalf of the data controller. The data processor might determine the method of processing but will never determine the purpose. There should always be a contract in place between a data controller and a data processor.

6.6 **Data Protection Officer (DPO)**: the DPO advises an organisation about their obligations under UK Data Protection Legislation and monitors compliance to ensure that they are meeting those obligations. The DPO reports to the highest level of management in the organisation and operates independently.