# **Stage 1**

## **Project Details**

|  |  |
| --- | --- |
| **Project / Process / System Name:** |  |
| **Work Request Reference:**(If applicable) |  |
| **Background / Objectives:**Explain what the project aims to achieve, what are the benefits to the organisation, individuals and other parties |  |
| **Implementation date:** Provide the deadline / milestone dates required for completion |  |

### **Key Officers**

Please identify the key officers involved or with responsibility for this project / system.

If there are multiple, please add more rows as required.

|  |  |  |
| --- | --- | --- |
| **Information Asset Owner(s)** | Name: |  |
| Job Title: |  |
| Service: |  |
| **Project Lead / Manager(s):** | Name: |  |
| Job Title: |  |
| Service: |  |
| **Data Protection/Information Management Officer(s) within the Information Governance Team:** | Name: |  |
| Job Title: |  |
| Service: |  |
| **System Administrator(s)**(if applicable) | Name: |  |
| Job Title: |  |
| Service: |  |

### **Version control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Status(Draft / Final / Revision) | Revision Date | Summary of Changes | Author(s) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **Screening Questions - please complete all the questions below**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Screening questions** | **Yes** | **No** |
| **1** | Will any personal data be processed? (personal data means any information relating to an identified or identifiable natural person)*e.g., names, addresses, bank details, health data.* *For a full list please see* **Section B: Data Protection Impact Assessment *question 1a*** |[ ] [ ]
| **2** | Under UK GDPR a DPIA must be completed for three types of processing. Will any of the following three types of processing be required? [**(see guidance note for definitions)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=3.pdf)• Systematic and extensive profiling with significant effects.• Large scale use of sensitive data.• Public monitoring.  |[ ] [ ]
| **3** | Is the processing ‘high risk’?  [**(see guidance note for definition of high risk)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=3.pdf) |[ ] [ ]
| **4** | Will the processing involve any of the following? **[(see guidance note for definitions and examples of each type of processing)](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note%22%20%5Cl%20%22page%3D4.pdf)*** Innovative technology
* Denial of service
* Large Scale Profiling
* Biometrics
* Genetic data
* Drones
* Facial Recognition including images and videos
* Data matching
* Invisible processing
* Tracking
* Targeting of children or other vulnerable individuals
* Risk of physical harm
 |[ ] [ ]
| **5** | Will the processing utilise automated decision making?  |[ ] [ ]
| **6** | Will the processing involve the contacting of individuals in ways which they may find intrusive? (e.g., marketing)  |[ ] [ ]

**If you answered “yes” to any of the above, then a full DPIA should be carried out.**

There may be circumstances where you feel the personal data identified in Q1 is low risk. If this the case, please contact the Information Governance team before progressing to stage 2 to prevent unnecessary work.

Stage 2 questions 2 – 6 maybe technical but please complete as much as you can before returning it along with accompanying documentation such as mandates and contracts to: infocompliance@leedsbeckett.ac.uk

**If you answered “no” to all the above, then it is likely a DPIA is not required.**

Please return this by email to: infocompliance@leedsbeckett.ac.uk for review and audit trail purposes.

# **Stage 2:** Full DPIA

## **Section A:** New process/Change of System/Project General Details

|  |  |
| --- | --- |
| **Project Type** | [ ]  New process / project (complete sections A & B)[ ]  New system / application (complete sections A, B & C)[ ]  Surveillance equipment (complete sections A, B and Appendix 1)[ ]  Research-Undergraduate (complete sections A, B & if relevant C) [ ]  Research-Postgraduate (complete sections A, B & if relevant C)  |
| **Data Controller(s)**This the organisation(s) that decides what data to collect or what to do with it. |  |
| **Data Processor(s)**This is any organisation who receives, stores, or processes the data but do not have the authority to decide how to do this. |  |
| **Consultation:** Detail any consultation undertaken with the public, partners, internal or external stakeholders |  |
| **Information flow/numbered stages:**Please set out the stages of how data is collected and used from the point of collection to its destruction (an example of an information flow can be found in the DPIA guidance note to use as appropriate) |
|  |

## **Section B:** Data Protection Impact Assessment

|  |  |
| --- | --- |
| **Question** | **Response** |
| **Data Types** |
| **1a** | **Personal Data**Please check the information that will be processed  | **Data Type** | **Mandatory** | **Optional** |
|  |  | Name |[ ] [ ]
|  |  | Date of birth |[ ] [ ]
|  |  | Correspondence details (address-term time/non term) |[ ] [ ]
|  |  | Contact details(telephone, email, social media –private/LBU assigned) |[ ] [ ]
|  |  | Personal data history (education, career, work, CV) |[ ] [ ]
|  |  | Proof of residence/address (see gov.uk category 2 list for full list: council tax, utility bill, official government letterheaded correspondence) |[ ] [ ]
|  |  | Third party contact data (emergency contact, guardian, parent, power of attorney) |[ ] [ ]
|  |  | Pseudonymised data (please highlight all those which apply)(Student No, Staff No, UCAS ref, driving licence ref, NI number, payroll no, NHS no, student loan no, bank account no, vehicle registration) |[ ] [ ]
|  |  | Photograph/video footage/audio could be considered sensitive |[ ] [ ]
| **1b** | **Special Category and/or Sensitive Data**Please check the information that will be processed | Racial / Ethnic origin |[ ] [ ]
|  |  | Political opinions |[ ] [ ]
|  |  | Religious / philosophical beliefs |[ ] [ ]
|  |  | Trade union membership |[ ] [ ]
|  |  | Sexual orientation |[ ] [ ]
|  |  | Sexual life |[ ] [ ]
|  |  | Physical health |[ ] [ ]
|  |  | Mental health |[ ] [ ]
|  |  | Medical history |[ ] [ ]
|  |  | Criminal convictions |[ ] [ ]
|  |  | Proof of identification (see gov.uk category 1 data for full list: passport, driving licence, visa, travel cards, NUS card) |[ ] [ ]
|  |  | Location data (IP address, geolocation) |[ ] [ ]
|  |  | Personal finance data (student loan, social economic categorisation, hardship) |[ ] [ ]
| **1c** | **Gender Information** | Gender (inc. non-binary) |[ ] [ ]
|  |  | Titles (Dr, Miss, Mr, Mrs, Mx) |[ ] [ ]
| **1d** | **Other**  | (please specify) - including associated personal data such as vulnerable groups e.g., young persons, elderly, patient groups, campaign groups, learning impairment, ancestry/family connections |

|  |  |
| --- | --- |
| **Processing** | **Issue/Risk Number** |
| **2** | The data of approximately how many individuals will be affected? | [ ]  1 - 9[ ]  10 - 99[ ]  100 - 999[ ]  1,000 - 9,999 [ ]  10,000+  |  |
| **3** | How is the personal data obtained? | [ ]  From client / service user[ ]  From partner agencies [ ]  From third party / other Individuals[ ]  For employment purposes[ ]  Internal services[ ]  Other - please provide detail below:  |  |
| **4** | How are individuals informed of the processing at point of data collection?If none of the items listed are ticked please tick the issue/risk column | [ ]  Privacy notice on leedsbeckett.ac.uk[ ]  Privacy notice on another webpage [ ]  Privacy statement on paper form / leaflet[ ]  Signage[ ]  Verbally as part of documented process |  |
| **5** | Does this project involve any linkage / matching of personal data with data in other collections, or is there significant changes in data linkages / matching? | [ ]  No[ ]  Yes - if so, please provide detail below: |  |
| **6** | Does this project involve any automated decision making/profiling? | [ ]  No[ ]  Yes - if so, please provide detail below and tick the issue/risk column: |  |

|  |  |
| --- | --- |
| **Legal Basis** | **Issue/Risk Number** |
| **7** | What is the legal basis you are relying on for the processing of the personal data? [**(see guidance note for details on each legal basis)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=6.pdf)If none of the items listed are ticked please tick the issue/risk column | [ ]  (a) Consent[ ]  (b) Contract with data subject[ ]  (c) Legal obligation[ ]  (d) vital Interests [ ]  (e) Public task[ ]  (f) Legitimate interests \*consult with IG for undertaking legitimate interest test |  |
| **7a** | If you are relying on legal obligation or public task, please detail which legislation are you relying on? |  |  |
| **8** | If you are processing special category data, what is the legal basis you are relying on? [**(see guidance note for definitions)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=8.pdf) | [ ]  N/A[ ]  (a) Explicit consent[ ]  (b) Employment[ ]  (b) social security/social protection law[ ]  (c) Vital interests[ ]  (d) Not-for-profit bodies[ ]  (e) Made public by the data subject[ ]  (f) Legal claims and judicial acts[ ]  (g) Substantial public interest [ ]  (h) Health or social care[ ]  (i) Public health[ ]  (j) Archiving, research and statistics |  |
| **9** | Will personal data be stored and/or transferred to a country outside the UK? | [ ] No [ ] Yes - if so list which one(s) and tick the issue/risk column |  |
| **9a** | If data is leaving the UK, what legal basis are you relying on for this international transfer? [**(see guidance note for further information on international transfers)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=8.pdf) | [ ]  Adequacy decision[ ]  Appropriate safeguards[ ]  Exemption – explicit consent[ ]  Exemption – public interest[ ]  Exemption – legitimate interest |  |
| If you are using consent for any of the above, please answer Q10 below.If you are not using consent, please proceed to Q11. |  |
| **10a** | How will consent be obtained and recorded?  |  |  |
| **10b** | How will subjects be able to withdraw their consent? |  |  |
| **10c** | How will a subject’s data be removed if required? |  |  |

|  |  |
| --- | --- |
| **Records Management**  | **Issue/Risk Number** |
| **11** | Does this project relate to an existing information asset listed on your local information asset register? If you are unsure, please check with infocompliance@leedsbeckett.ac.uk  | [ ] No[ ] Yes - if so, please provide detail below: |  |
| **12** | What processes are in place for checking data quality at the point of collection?If there is no data quality, please tick the issue/risk column | [ ] Peer checking[ ] Validation[ ] Other – please provide detail below: |  |
| **13** | How will the information being processed be kept up to date and checked for accuracy and completeness? |  |  |
| **14a** | Where will the information be stored / accessed? If you are unsure you may need to contact an appropriate person(s) within IT Services.If data is stored in multiple places, please tick the issues/risk column | Unstructured Electronic:[ ]  Shared network drive (H)[ ]  Personal network drive (P)[ ]  Personally allocated cloud storage (e.g. google drive, one drive, adobe cloud, drop-box)[ ]  collective cloud storage (e.g. share-point, microsoft teams, case handling system, EDRMS)[ ]  Email client (LBU outlook, external org email client, personal email client)Structured Electronic[ ]  Internal system / application[ ]  External – third party application[ ]  External – cloud hostedOther:[ ]  Paper filing system [ ]  Removable media [ ]  Other – please specify: |  |
| **14b** | Please give details of the storage solution. (e.g., application name, site, file path) |  |  |
| **15a** | Does this data follow an existing retention entry listed on the [**LBU retention schedule?**](https://www.leedsbeckett.ac.uk/our-university/public-information/information-compliance/information-management-and-compliance/) | [ ]  No - please complete 15b and tick the issues/risk column[ ]  Yes - if so, provide details of which entry below: |  |
| **15b** | How long will this information be kept for, and from what date? |  |  |
| **16** | How will the information be destroyed when it is no longer required?If unknown, please tick the issues/risk column |  |  |
| **17** | Will the destruction of information be certified?  | [ ]  No[ ]  Yes - if so, please provide details below: |  |

|  |  |
| --- | --- |
| **Sharing / Processing** | **Issue/Risk Number** |
| **18** | Will any of the information be processed by or shared with other University services/schools?  | [ ]  No[ ]  Yes - if so please provide details below: |  |
| **18a** | Will any of the information be processed by or shared with other external organisations? | [ ]  No[ ]  Yes - if so, please provide details below: |  |
| If the answer to both questions 18 and 18a are ‘no’ proceed to Governance Section.If the answer to either question 18 or 18a was ‘yes’ please answer questions 19-21 below. |  |
| **19** | What is the legal basis for sharing? [**(see guidance note for further details relating to legal basis)**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=7.pdf) | [ ]  (a) Consent[ ]  (b) Contract with data subject[ ]  (c) Legal obligation[ ]  (d) vital Interests [ ]  (e) Public task[ ]  (f) Legitimate interests |  |
| **20** | Will there be an agreement in place setting out the requirements and expectations when sharing data?If no please tick the issues/risk column | [ ]  No[ ]  Yes – in a contract[ ]  Yes – in a sharing agreement / data processing agreement |  |
| **21** | Which method will be used to transmit / transport information?  | Digitally[ ]  Email[ ]  Encrypted Email[ ]  File transfer service (e.g. Zend To, One Drive)[ ]  Social media [ ]  Providing access via University systems Verbally[ ]  In person[ ]  By telephonePhysically[ ]  By hand[ ]  Via courier[ ]  Via external post[ ]  Removable media[ ]  Other (please give details): |  |

|  |  |
| --- | --- |
| **Governance** | **Issue/Risk Number** |
| **22** | Are there any written processes in place specifying any of following: (tick multiple boxes if applicable)If no please tick the issues/risk column | [ ]  Which users / services / agencies are granted access?[ ]  How information is handled[ ]  How information is disclosed[ ]  When information is disclosed[ ]  That recipients of information become Data Controllers of the copy disclosed |  |
| **23** | Are there auditing processes available to ensure compliance any of the following: - disclosure, production, access, handling receipt, storage, disposal, migration/transfer If no please tick the issues/risk column | [ ]  No[ ]  Yes – if so, please list which elements can be audited: |  |
| **23a** | When will any audits be undertaken? | [ ]  As required / requested [ ]  On an ad hoc basis[ ]  On a regular basis. If so, how often?: [ ]  Daily [ ]  Weekly [ ]  Monthly [ ]  By Academic Term or Semester [ ]  Annually |  |
| **24** | Is there a business continuity and a disaster recovery plan in place? If no please tick the issues/risk column | [ ]  No[ ]  Yes – if so, please provide detail below: |  |

## **Section C:** New System

The below section should only be completed if you are implementing a new system / application.

|  |  |
| --- | --- |
| System (To be considered in conjunction with IT services if required) | **Issue/Risk Number** |
| C1 | Can the system export the data at a client / user level? | [ ]  Yes[ ]  If not please outline how will data be collated for Subject Access Requests below: |  |
| C2 | Can the system quarantine information / restrict processing? If no please tick the issues/risk column | [ ]  No[ ]  Yes - if so, please provide detail below: |  |
| C3 | Does the system enable you amend or add notes to data / information at a single data field level? | [ ]  Yes[ ]  No |  |
| C4 | Can the information be deleted at a singular data field level? | [ ]  Yes[ ]  No  |  |
| C5 | Is there an access control policy in place?If no please tick the issues/risk column | [ ]  No[ ]  Yes- if so, please provide summarise detail below: |  |
| C6 | Is there an ability to audit:- access to the information?* Destruction?
* Modification?
* import/Export?
* metadata even once information asset has been deleted?
* users disabled?
 | [ ]  No If no please tick the issues/risk column[ ]  Yes - if so, please list which elements can be audited: |  |
| C7 | What security measures have been implemented to secure access and limit the use of personal information? (e.g. encryption, role based permissions, multi factor authentication) |  |  |
| C8 | Does this project involve privacy invasive technologies (e.g. trackers, GPS, recording) | [ ]  No[ ]  Yes – if so, please provide detail below and please tick the issues/risk column |  |
| C9 | Is there a documented policy/procedure for managing privilege users?If no please tick the issues/risk column | [ ]  No[ ]  Yes |  |
| C10 | Which country(ies) are the system servers located/hosted? |  |  |
| C11 | What is the registered address of the company with whom we are entering a contractual relationship? |  |  |
| C12 | For personal data - does the system ‘look-up’ data held in another system? | [ ]  No[ ]  Yes |  |

# **S****tage 3:** Identify the information, privacy and related risks / issues

From the assessment above identify the key risks and issues using the [**risk matrix contained within the guidance note**](https://www.leedsbeckett.ac.uk/-/media/files/our-university/public-information/information-compliance/dipa-guidance-note#page=14.pdf)to identify the risk rating.

Describe the actions you could take to reduce the risks and any necessary future steps (e.g., the production of new procedures or future security elements for systems).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Describe the source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm**(Remote, Possible or Probable) | **Severity of harm**(Minimal, Significant or Severe) | **Overall risk**(Low, Medium or High) | **List the action(s) required to reduce or eliminate the risk** | **Likelihood of harm**(Remote, Possible or Probable) | **Severity of harm**(Minimal, Significant or Severe) | **Overall Risk level after mitigation** (Low, Medium or High) | **Outcome** (i.e mitigation to be implemented or risk accepted) |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Sign Off and Outcomes – The Information Governance Team will aim to assess all DPIA’s within 5 working days of receipt.**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name / Date** | **Notes** |
| **Risk mitigation measures approved by Information Asset Owner:**  |  | Integrate actions back into project plan, with date and responsibility for completion. |
| **Residual risks remaining after mitigation actions approved by Information Asset Owner:** |  | If accepting any residual high risk (risk remaining high following the implementation of all mitigating actions) the university will need to consult the ICO before going ahead and it is unlikely these will be signed off by the Data Protection Officer (DPO). |
| **Data Protection Officer (DPO) advice given by:** |  | DPO should advise on compliance, risks assessed and whether processing can proceed. |
| **Summary of DPO advice:** |
|  |
| **DPO advice accepted or overruled by:** |  | If overruled, you must explain your reasons in the comments below. |
| **Comments:** |
|  |

**NEXT STEPS**

**RECORDING OF RISKS -** Subject to approval and finalisation of the DPIA any identified risk that have been considered medium to high risk should be transferred to either the System Information Asset Register or the Information Asset Register so that these risks can continually be monitored by the Information Asset Owner.

**RETENTION OF DPIA** - The final version of this DPIA will be stored by the Information Governance Team for the required record retention period.

**SIGNIFICANT CHANGES TO PROJECT AND REVIEW -** This DPIA should be reviewed where there is any significant change to the project, personal data, processing, or other processors involved this DPIA should be reviewed and updated. Otherwise, the DPIA should be reviewed 3 years after its original approval against the project’s operation.