**Imperial College London**

**Name of Activity, Project, Process or Initiative**

**Data Protection Impact Assessment**

|  |  |
| --- | --- |
| **Document Information** | |
| Document Status and Version | *Draft / Review / Final V1.0* |
| Author(s) |  |
| Information Asset Owner |  |
| Name of department and faculty or Support Services |  |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version History** | **Version Date** | **Requestor of Change** | **Summary of Changes** |
| *V1.0* |  |  | *Initial Draft* |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| Proposed date for the activity/project/process/initiative commencement |  |

|  |  |
| --- | --- |
| Proposed date for the activity/project/process/initiative completion |  |

Please note that the College may disclose completed DPIAs where it is required to do so by law (including the Freedom of Information Act), by any applicable governmental or other regulatory authority, or by order of a court. For further information as to what to disclose if required under FOIA please contact the Legal Services Officers at [foi@imperial.ac.uk](mailto:foi@imperial.ac.uk).

Completed DPIAs may also be published internally for organisational learning and awareness so please advise the Data Protection Officer of any concerns to ensure these are duly considered/mitigated. The Data Protection Officer can be contacted at [robert.scott@imperial.ac.uk](mailto:robert.scott@imperial.ac.uk)

Before completing this document, please read the Data Protection Impact Assessments Guidance available on <http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/internal-guidance/templates/>

All entries listed in blue are examples and for guidance only

**Part 1 - DPIA Summary**

|  |  |
| --- | --- |
| **Name, job title and contact details of the nominated Information Asset Owner\*** | |
| Information Asset Owner name and job title |  |
| Information Asset Owner contact details |  |

**\*Information Asset Owners**

Any activity, project, process or initiative proposed to involve the processing of personal data[[1]](#footnote-1) should have a designated Information Asset Owner. Information Asset Owners are responsible for assessing information security and privacy risks annually for their information assets and implementing appropriate measures accordingly. Accordingly, the Information Asset Owners are responsible for completing a DPIA in respect of the relevant activity/project/process or initiative (as is applicable).

Information Asset Owners are also responsible for recording the existence and details of their information assets in the College’s Information Asset Register (which is in the process of being rolled out in College).

|  |  |  |
| --- | --- | --- |
| **What scenario best describes the purpose for the DPIA?** | | |
| Activity/Non-research project: *Yes / No* | Supplier: *Yes / No* | Research: *Yes / No* |

|  |
| --- |
| **Outline the project / supplier requirements / research and its objectives (if processing is due to a statutory requirement please explain)?** |
| *Activity/non-research project:*  *If this is not a new process but a change to a current system or technology then describe the current process and how the proposal will effect this*  *Supplier:*  *If a new / renewed supplier please describe the processing that will be conducted by them*  *Research: If a Research Study please advise of the proposal and what processing is expected to be conducted*  *NB also consider the following*  *What are the primary and secondary objectives / activities to be completed*  *What further governance will be needed including but not limited to – creation of a contract, creation of a data sharing agreement, ICT / ICT Security Involvement, Ethics Committee sign off*  *You may find it helpful to refer or link other documentation such as the proposal, ethical guidelines, contract terms etc.* |

|  |  |
| --- | --- |
| **List of stakeholders consulted during the DPIA Process (if pertinent, include names / roles for any persons involved thus far and any actions completed / in transit as a result)** | |
| *Internal Suggestions include:*  *ICT Security*  *Information Governance*  *Legal Services*  *Archives and Corporate Records Unit*  *Data Protection Officer*  *Ethics / Guidance Committee*  *Research Office*  *End users*  *Collaborative Partners*  *Procurement / Purchasing*  *Suppliers of system and/or framework* | *External suggestions include:*  *Data Subjects*  *General public*  *External organisations*  *Regulators* |

**Part 2 - Identifying the need for a DPIA**

The following screening questions are intended to help you decide whether a full Data Privacy Impact Assessment (DPIA) is necessary. Answering yes to any of the below listed questions means that a full DPIA is necessary and therefore, you must complete all of Parts 3 through 9 (inclusive) of this document. If a full DPIA is **not** required please progress to Part 9.

|  |  |
| --- | --- |
| **Activity** | **Yes or No** |
| Will you be processing / collecting special categories of personal data[[2]](#footnote-2) or data which is likely to raise privacy concerns e.g. criminal records, health records? |  |
| Will you be evaluating, scoring, profiling or predicting individuals’ behavior? |  |
| Will there be automated decision making about individuals with legal or similar effects?[[3]](#footnote-3) |  |
| Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? |  |
| Will the project include systematic monitoring, observing or controlling personal data? |  |
| Will you be carrying out large scale processing of personal data? (This could include large volumes of data, large population of data subjects, length of processing or geographical extent of data) |  |
| Will you be combining or matching datasets or collecting and creating new information about individuals? |  |
| Will you be collecting the personal data of vulnerable individuals? |  |
| Will you be deploying a new or innovative use of technology to process personal data? |  |
| Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support? |  |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. |  |
| Is data likely to be transferred outside of the European Union? |  |
| Will the project compel individuals to provide information about themselves, without which an individual cannot use a service or contract? |  |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |  |
| Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |  |
| Will the project require you to contact individuals in ways which they may find intrusive? |  |
| Will the project involve the processing of personal data by third parties (third parties would include all cloud based services, webinar platform providers etc.)? |  |
| Will the project expose personal data to elevated levels of security risks? |  |
| Are stakeholders likely to have privacy concerns about the project? |  |

Once these questions have been completed please contact the College’s Data Protection Officer at [robert.scott@imperial.ac.uk](mailto:robert.scott@imperial.ac.uk) for review and guidance.

**Parts 3 – 9 must be completed if a full DPIA is required**

**Part 3 - Describing the Data Processing**

|  |
| --- |
| Describe the scope of the processing: |
| *What types of personal data will be collected/processed/stored? Will it include and special categories of data? If so, what are these? How long will it be kept for? How will it be deleted? Approximately how many persons’ data will be collected?* |

|  |
| --- |
| Describe the processing: How has the data been collected/ will be collected? |
| *What is or will be the source of the data? Are persons aware of the processing? Is children’s data collected (under 13’s) or other vulnerable persons? Is this new technology? Are any code of conducts/guidelines being followed? What will the benefits of the processing be? Will a new Privacy Notice need to be created or will an existing College Privacy Notice be appropriate and sufficient?* |

**Part 4 - Legal basis for processing**

|  |  |
| --- | --- |
| **Legal basis for processing ‘Personal Data’ – list ‘Y’ where applicable** | |
| Data subject has given **consent** (must be unambiguous and auditable) |  |
| Necessary for the performance of a **contract** (includes during negotiation of said contract such as purchase of services, registration, contract to staff/students) |  |
| Necessary for compliance with a **legal obligation** (e.g. HMRC, does not include contractual obligations) |  |
| Necessary for the performance of a task carried out in the **public interest** or in the exercise of an **official authority** vested in the controller (examinations, assessments, transcripts etc.) |  |
| Necessary for the purpose of the **legitimate interests** pursued by the controller or by a third party (if such then a **Legitimate Interests Assessment**, LIA, must be conducted[[4]](#footnote-4) and this cannot be cited for processing in accordance with acts carried out by public authorities i.e. teaching) |  |

|  |  |
| --- | --- |
| **Legal basis for processing ‘ Special Categories of Personal Data’ – tick where applicable** | |
| Data subject has given **explicit consent** |  |
| Necessary for carrying out obligations **under employment**, **social security** or **social protection law**, or a **collective agreement** |  |
| Processing relates to data **manifestly made public** by the data subject |  |
| Processing is necessary for the purposes of **carrying out obligations** as set out by the College in its official capacity |  |
| Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems |  |
| Processing is necessary for archiving purposes in the public interest, **scientific or historical research purposes or statistical purposes** |  |

**Part 5 - Data flow mapping**

Data flow charts pinpoint the data lifecycle from collection, processing, dissemination to destruction/conclusion and will identify whom will have access to the data, why, how and under what legal basis. They can also help identify points of potential risk for investigation and mitigation

When creating your data flow diagrams you may find it easier to use the below examples which can be copied, pasted and edited according to your needs

Data Flow Chart Example

Retention Period

Data destruction / End

Data Collection

Data Processing

Completion / storage

Start

Decision Making

Manual Input

Data shared internally / externally to Imperial

Data processed by ‘Third Party Company’. Contract in place

**Part 6 - Data processor / contractor requirements**

|  |  |
| --- | --- |
| Will a third party company/contractor be utilised? (if yes, please complete) | Yes / No |
| *The College will most commonly be a ‘data controller’, meaning we determine the purpose and means by which data is processed. Another company/contractor may be involved as a data processor, as such they process data on our behalf however to do so the following must be followed* | |
| Has a written contract been agreed/signed which includes relevant data processing clauses? Alternatively, has a data processing agreement been agreed/signed? |  |
| Are sufficient guarantees in place regarding access/use of data and security measures to prevent misuse? |  |
| Has the data processor agreed to replicate the same level of data protection compliance as stipulated within the aforementioned contract? |  |
| Have confidentiality clauses been included where deemed appropriate? |  |
| If off-site, have the data processor/contractor agreed for relevant inspections/audits to be undertaken to provide assurance of relevant security measures being in place? |  |
| If data is to be stored outside of the EEA, has demonstration of Data Protection Adequacy been achieved? |  |

**Part 7- Identify and assess risks (examples in blue)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ref | 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 / Probably) | **Potential impact on individuals** | **Compliance impact** |
| 1 | ***Data intercepted in transit:*** *Information entered into or retrieved from the student record system will need to traverse the internet between the user’s PC or mobile device and the supplier’s datacentre. This will involve transmission over parts of the internet over which neither the College nor the supplier have control. There is a risk that the information could be intercepted in transit, revealing personal information to third parties.* | *Possible* | *Personal, sensitive or confidential information may be used for unauthorised purposes or disclosed inappropriately* | *College might be in breach of GDPR principle 6.*  *Reputational damage, cost of defending prosecution, possible fines.*  *College information may be used for unauthorised purposes or disclosed inappropriately* |
| *2* | *Los of data due to cyber attack* | *Possible* | *High impact on data subjects if data stolen or placed in public domain* | *College might be in breach of GDPR principle 6.*  *Reputational damage, cost of defending prosecution, possible fines.*  *College information may be used for unauthorised purposes or disclosed inappropriately* |
|  |  |  |  |  |
|  |  |  |  |  |

**Part 8 - Identify measures to reduce risk (examples in blue)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Identify measures to reduce / eliminate risks identified in 6 | | | | | |
| Risk ref | Solutions to reduce / eliminate risk | Effect on risk  (Eliminate / reduce / accepted) | Residual risk ( Low / Medium / High) | Measure approved (Yes / No) | Completed (Yes / No) |
| 1 | The supplier’s data centre has a direct connection to the Janet network.  2. The traffic between the client device and the servers is encrypted using https. | The risk is reduced to the level where it is accepted | Low | Yes | Yes |
| *2* | *Penetration testing in place, appropriate anti-cyber-attack measures implemented.*  *Location reviewed/audited and deemed acceptable*  *Contract dictates the process to be followed if incident occurs including contacting relevant personnel within College* | *Reduced* | *Low* | *Yes* | *Yes* |
|  |  |  |  |  |  |

**Important**

The Data Protection Impact Assessment identifies several risks and subsequent countermeasures to reduce risk to a level deemed justified/accepted to allow for processing to occur. Following completion of the assessment the Information Asset Owner is accountable to ensure that ongoing consideration is given to any further risks and impact plus to ensure the counter measures are adhered to.

**Part 9 - Sign off / Approvals**

At the end of the assessment, the DPIA with the proposed solutions should be signed off as follows:

***Sign off by the Information Asset Owner:***

1. where only the screening questions in Part 2 have been completed; or
2. where the full DPIA has been completed and satisfactory solutions are found to any identified risks;

and, in each case, (i) no sensitive personal data is proposed to be processed as part of the activity/project/process or initiative (as applicable) and (ii) the activity/project/process or initiative will not involve the processing of personal data about 250 or more individuals, the Information Asset Owner is authorised to sign off the completed DPIA in consultation with the local Data Protection Co-Ordinator (if one has been nominated).

Where the Information Asset Owner is uncertain as to whether he/she is able to sign off on a given DPIA or uncertain about any GDPR compliance aspects, he/she should contact the College’s Data Protection Officer for further guidance.

***Sign off by the Information Asset Owner, the College’s Data Protection Officer and the Compliance and Information Governance Manager:***

1. where sensitive personal data is proposed to be processed as part of the activity/project/process or initiative (as applicable); and/or
2. where the Information Asset Owner is not able to identify satisfactory solutions to any identified risks or is uncertain as to whether any solutions appropriately address the identified risks; and/or
3. where the activity/project/process or initiative (as applicable) will involve the processing of personal data about 250 or more individuals,

the Information Asset Owner should approve the completed DPIA herself/himself and then seek a further sign off on the DPIA from the College’s Data Protection Officer and the Compliance and Information Governance Manager.

|  |  |  |
| --- | --- | --- |
| **Information Asset Owner** | **Data Protection Officer** | **Compliance and Information Governance Manager** |
| **…………………………………….**  **Signature**  **…………………………………….**  **Name**  **…………………………………….**  **Date** | **…………………………………….**  **Signature**  **…………………………………….**  **Name**  **…………………………………….**  **Date** | **…………………………………….**  **Signature**  **…………………………………….**  **Name**  **…………………………………….**  **Date** |

**Part 10 – Record keeping**

There should be a permanent record of who signs off any DPIA and when this took place. Accordingly, each Information Asset Owner must:

* retain a copy of the final completed DPIA for his/her records (regardless of whether only the screening questions have been completed or the full DPIA has been completed); and
* send a copy of the final completed DPIA to the local Data Protection Co-Ordinator (if one has been nominated) (regardless of whether only the screening questions have been completed or the full DPIA has been completed); and
* send a copy of the final completed and approved DPIA to the College’s Data Protection Officer (regardless of whether only the screening questions have been completed or the full DPIA has been completed).

If any approval is granted on the basis that certain actions are to be taken by a set deadline and those actions are not completed by that deadline, the Information Asset Owner should bring this to the attention of the approvers and suggest appropriate remedial action.

**Part 11 – Further information / guidance**

For more information / guidance on the creation and use of DPIA’s please contact the Data Protection Officer and/or view the following:

Information Commissioner’s Office - [Guide to the General Data Protection Regulation (GDPR)](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf) page 100

Information Commissioner’s Office - [Data Protection Impact Assessments (DPIAs) guidance](https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/)

Article 29 Working Party - [Guidelines on Data Protection Impact Assessments](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

1. For the definition of personal data please see this website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/> or the Data Protection Impact Assessments Guidance, available on <http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/internal-guidance/templates/> [↑](#footnote-ref-1)
2. For the definition of sensitive personal data or special categories of data please see this website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/> or the Data Protection Impact Assessments Guidance, available on <http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/internal-guidance/templates/> [↑](#footnote-ref-2)
3. For guidance on what automated decision making is please see the information on this website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/> [↑](#footnote-ref-3)
4. Use the following link for [guidance on using the legitimate basis for processing](https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf) and the template available on <http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/internal-guidance/templates/> to document your legitimate interests analysis [↑](#footnote-ref-4)