

**Privacy Impact**

**Assessment**

Goldsmiths processes significant quantities of personal data. Any processing of personal data carries with it risk of acting contrary to the College’s legal obligations as well as to the rights and freedoms of individuals. It is essential that every effort is made to identify and minimize the risk. Carrying out a Data Protection Impact Assessment helps to identify the risk and assessment the likelihood and severity of any impact on an individual should the risk crystalize.

Staff should complete this form at the start of any major project involving the use of personal data, or if they are making a significant change to an existing process. The final outcomes should be integrated back into the project plan.

Goldsmiths has a legal responsibility to show that it has considered and integrated data protection into its processing activities (“data protection by design and default”). When starting a major project or making a significant change to an existing process, it is important to involve the Data Protection Officer (dp@gold.ac.uk) who can provide advice and guidance.

For any assistance completing this Form, contact the Data Protection Officer (dp@gold.ac.uk).

This Form will need to be submitted to the Data Protection Officer. This can be done by email a copy to dp@gold.ac.uk.

# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
|  |

# Step 2: Describe the processing

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
|  |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
|  |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
|  |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?  |
|  |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
|  |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
|  |

# Step 5: Identify and assess risks

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary.  | **Likelihood of harm** | **Severity of harm** | **Overall risk**  |
|  | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

# Step 6: Identify measures to reduce risk

|  |
| --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** |
| **Risk**  | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
|  |  | Eliminated reduced accepted | Low medium high | Yes/no |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item**  | **Name/date** | **Notes** |
| Measures approved by: |  | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: |  | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: |  | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: |
| DPO advice accepted or overruled by: |  | If overruled, you must explain your reasons |
| Comments: |
| Consultation responses reviewed by: |  | If your decision departs from individuals’ views, you must explain your reasons |
| Comments: |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |