## ico_master_blue_rgb_Sample DPIA (Data Protection Impact Assessment)

This template is an example of how you can record your DPIA process and outcome. Please see the [Guidance on Data Protection Impact Assessments](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) from the Information Commissioner's Office.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

# Submitting controller details

|  |  |
| --- | --- |
| Name of controller |  |
| Subject/title of DPO |  |
| Name of controller contact /DPO (delete as appropriate) |  |

# 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. |
| *I’m a…, Get me out of here* is a group of online enrichment activities, which includes *I’m a Scientist, I’m an Engineer, I’m a Mathematician,* and others.  The activity connects school students with working STEM professionals online. It consists of a secure, moderated website where groups of students take part in live text-only chats with STEM professionals. They are able to submit follow-up questions, and comment on the answers given.  In order to gain secure access students need to create an account on the site. They need to provide their:   * Name, so teachers can identify them. * Email address, so the students can recover passwords, be notified of answers to their questions, and be given updates on the activity.   Students choose a display name to appear on the site. This is the only information that is visible to the STEM professionals taking part.  Student data is processed for the sole purpose of delivering the activity. Data is stored on a secure server in the UK and is not shared with any other party.  This DPIA is provided under a precautionary principle even though the data risk is viewed as low. |

# 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? |
| Name and email address are entered by students as they create their account on a page provided by their teacher.  The data is stored for the duration of the activity and deleted after 6 months or at the end of the academic year (whichever is sooner).  Student data is stored on a secure server based in the UK. It is not shared with any other party. There is no high-risk processing. |

|  |
| --- |
| **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? |
| Student data consists of name and email address only. There is no special category data.  The data is collected once at the time of account creation.  The data is stored for the duration of the activity and deleted after 6 months or at the end of the academic year (whichever is sooner). |

|  |
| --- |
| **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)? |
| Students are requested to create an account by their teachers.  A short, clear, and simple to read privacy policy, along with human-readable terms of use, are provided and designed for all students to understand.  Over-16’s are asked to give consent to the terms of use. For students under this age, teachers provide consent on their behalf.  The activity is provided by a company that has been delivering online activities to schools since 2003. There are no concerns over the technology. |

|  |
| --- |
| **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? |
| The processing is required to run the activity and to allow teachers to safely and securely know which students are participating.  The benefits of processing are a demonstrable increase in motivation to study STEM. |

# 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? |
| The school should consider notifying parents and carers about their children’s participation in the activity.  This may be even more relevant if students are taking part from home, which might be the case under certain circumstances. |

# 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? |
| The processing of data is lawful and is necessary for the successful delivery of the activity, which is in students’ and the public’s interest.  Consent is given by teachers or students (depending on the age of the students).  Minimal data is requested. Students can unsubscribe and request account deletion. Data is kept for a short period. Data is stored on a single UK-based server. |

# 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** |
| Data breach of student names and email addresses. | Remote | Minimal | Low |

# 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** |
| Data breach | Access to data is tightly restricted to the Data Processor’s DSO. | Reduced | Low | Yes/no |

# Step 7: Sign off and record outcomes

|  |  |  |
| --- | --- | --- |
| **Item** | **Name/position/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 |