**Information Technology and Media Services**

**Data Protection Impact Assessment Template**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**
**[Please note that a project in this context is a business change within a set time period. We are not using the word project in accordance with the definition set by the Strategic Portfolio]**

**You must complete a DPIA if the DPIA Screening Checklist for your project identifies that a DPIA is required. You should complete a DPIA at the earliest stage of your project. You can repeat a DPIA at any stage of your project, for example, if the scope of your project changes.**

**If this is the first DPIA for your project, please make sure that Sections 7 and 8 are completed by the SIRO/Director and Information Governance Manager so that your project can proceed beyond Gateway 1.**

|  |  |
| --- | --- |
| Project Title |  |
| Project Manager |  |
| Project Sponsor |  |
| Project DPIA Number (1= first DPIA) |  |

1. **What are the aims of your project?**

|  |  |
| --- | --- |
| Explain broadly what the project aims to achieve. What will be the benefits to DMU, students, staff, other stakeholders or the public?You may include links to other project documentation to support of this section.  |  |

1. **Describe the data processing**

|  |  |
| --- | --- |
| Please describe the proposed data flows (or attach a data flow map).How will you collect, use, store, share and delete data (in line with DMU’s retention policy or guidelines)? Who will have access to the data? Will it be shared with any third parties? If data is shared with a third party, how will the data be shared?Is there a contract/data processing agreement in place between DMU and the third party? If the data is shared with another data controller, is there an Information Sharing Agreement in place for this? |  |
| How many individuals/individual records will the system hold? What category of individual are they (e.g. staff, prospective students, current students, alumni, third parties,)? |  |
| What data items will you be processing (e.g. name, address, date of birth, sex, email address, etc)? Special category dataWill you be processing special category data? If so, what special category data will you be processing? Will it include genetic or biometric data?What is the lawful basis for the processing? (Please specify one lawful basis under Article 6 of the GDPR and one lawful basis under Article 9 of the GDPR).Criminal offence dataWill you be processing criminal offence data? If so, what is the lawful basis for the processing? Is it under an official authority as required under Article 10 of the DPA? (Please specify one lawful basis under Article 6 of the GDPR). Do you have an agreed policy to process criminal offence data, as required under the Data Protection Act 2018? |  |
| Will you be using systematic or extensive profiling or automated decision making? |  |
| Will you be processing data about children or vulnerable adults? |  |
| Will you be processing data that could result in a risk of physical harm in the event of a security breach? |  |
| Would the individuals reasonably expect their data to be processed in this way? How much control will they have? Are there any issues of current public concern that you should factor in?  |  |
| Will you be matching data about individuals with other information systems and for what purpose(s)? |  |
| Will you be applying a pseudonym or encrypting data so that individuals cannot be identified without decryption?  |  |

1. **Have you carried out or will you be carrying out any consultation?**

|  |  |
| --- | --- |
| Who has been or will be consulted, internally and externally (key stakeholders, trade unions etc)? |  |
| How will you carry out the consultation (you should link this to the relevant stages of your project)?Consultation can be used at any stage of the DPIA process. |  |

1. **Identify the privacy risks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Below are some common data privacy risks for projects. They are not exhaustive and will not apply to all projects, so please delete those that do not apply and add other identified risks as necessary, to ensure this section reflects the actual risks of your project. **You should also refer to the GDPR principles included in Appendix A, to help you identify privacy risks.** You can instead attach a copy of a recent relevant risk assessment for your project.  | **Risk to individuals** | **Likelihood x impact of harm to individual(s) (Low, Medium, High)** | **Associated corporate risk (e.g. compliance, financial, operational, reputational) (Low, Medium, High)** | **Likelihood x impact of corporate risk (Low, Medium, High)** |
| Unauthorised access to data (by DMU staff or third party supplier or service provider) |  |  |  |  |
| Information not encrypted in transit between [externally-hosted solution] and DMU |  |  |  |  |
| Information not encrypted at rest in [solution]  |  |  |  |  |
| Information transferred outside EU/EEA (to an adequate country) |  |  |  |  |
| Information transferred outside EU/EEA (to an inadequate country) |  |  |  |  |
| Information transferred to an organization who operate under the Privacy Shield in the USA (please note that whilst Privacy Shield is adequate, the adequacy may be revoked in September by the EC) |  |  |  |  |
| Data held for longer than mandated by DMU retention policy |  |  |  |  |
| Data not returned to DMU should processor go out of business, or termination of contract |  |  |  |  |
| Information excessive for purposes required |  |  |  |  |
| Data subjects unable to access information |  |  |  |  |
| Unable to delete data in response to a right to erasure |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **Mitigation of identified privacy risks**

|  |
| --- |
| For each of the privacy risks identified above, describe the actions you could take to mitigate against the risks. You may generate multiple potential solutions for each risk in order that the appropriate responsible person can make an informed decision based on risk appetite, available funding and resources etc.  |
| **Risk** | **Solution(s)**  | **Anticipated result: is the risk eliminated, reduced, or accepted?** | **Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Agreed solutions for mitigation of the above identified privacy risk(s)**

|  |
| --- |
| Which of the solutions identified above are approved for each of the risks identified?  |
| **Privacy risk** | **Agreed solution(s)** | **Approved by**  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **How will the above agreed solutions be integrated into your project plan?**

**Please ensure your SRO or Director approves the below proposals and include their details below.**

|  |
| --- |
| Which of the above solutions will be integrated into your project plan and who is responsible for ensuring that they are actioned? Who is the officer on your project group who can be contacted about any privacy issues that may arise? |
| **Action to be taken** | **Date for completion of actions** | **Responsibility for action** |
|  |  |  |
|  |  |  |
|  |  |

**Name (SIRO or Director) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_/\_\_\_\_/20\_\_ Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**8. This section is to be completed by the Information Governance Manager**

|  |  |
| --- | --- |
| Is the intended use of personal data necessary and proportionate to the proposed aim of the project? |  |
| Has the DPIA identified an unmitigated high risk(s) to the data subjects?  |  |
| What risks remain after the proposed mitigations and are they acceptable risks (within tolerance)?  |  |
| Have key stakeholders and/or unions been consulted? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| The project is compliant with data protection requirements | **Yes** |  | **No** |  |

**Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_/\_\_\_\_/20\_\_ Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Appendix 1 – GDPR Principles – the below principles from the GDPR should be considered when identifying your privacy risks**

**Principle – Lawfulness, fairness and transparency**

|  |  |
| --- | --- |
| Have you identified the need for the processing and is your project a proportionate response? |  |
| How will individuals be told about the use of their personal data? |  |
| Do you need to amend your privacy notices (e.g. [How We Use Student Data](https://www.dmu.ac.uk/documents/about-dmu-documents/quality-management-and-policy/information-security/policies/how-we-use-student-data.pdf), Student Regs & handbooks, [ICO DPA notification](https://ico.org.uk/ESDWebPages/DoSearch?reg=524743), or those provided on webforms?) |  |
| Have you established the legal basis for the processing? |  |
| If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? |  |
| Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act or the Common Law Duty of Confidentiality? |  |

**Principle - Purpose limitation**

Personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);"

|  |  |
| --- | --- |
| Is the processing necessary for the purpose?  |  |
| Are your processing only the minimum personal data needed for the purpose? |  |
| How long will you need to retain the personal data for the purpose? |  |
| Can the data be pseudonymised or encrypted for the purpose? |  |

**Principal - Data minimisation**

Personal data shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);"

|  |  |
| --- | --- |
| Is the information you are using of sufficient quality for the purposes for which it is used? |  |
| Which personal data could you not use, without compromising the needs of the project? Could you consider anonymisation or psuedonymisation of personal data? |  |

**Principle - Accuracy**

Personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);"

|  |  |
| --- | --- |
| If you are procuring new software, does it allow you to amend data when necessary? |  |
| How are you ensuring that personal data obtained from individuals or other organisations is accurate? |  |
| Will the project result duplication of data already held, and if so, how will data integrity be maintained? |  |
| Can you delete personal data if required to do so? |  |

**Principle – storage limitation**

Personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);"

|  |  |
| --- | --- |
| How long do you intend to retain the personal data?  |  |
| Are you procuring software which will allow you to delete information in line with the retention period(s)? |  |

**Principle – integrity and confidentiality of data**

Personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)."

|  |  |
| --- | --- |
| Does the new system or process provide protection against the security risks you have identified? |  |
| What instructions or training are needed so that staff know how to operate the new system securely? |  |
| Is the system accessible from outside of DMU, and if so, how will it prevent unauthorised access? |  |
| Does the system allow for configuration so that access to personal data is kept to the minimum required by an individual to carry out their role? |  |

**Principle - Accountability**

|  |  |
| --- | --- |
| Who will be responsible for the data processing on a day to day basis and ensure that the other principle are complied with? |  |
| What policies and procedures, guidance, training, contracts or agreements are in place to ensure compliance with data protection principles? |  |
| Is this system or process included in the DMU’s Information Asset Register or Record if Data Processing Activities? |  |