

**DN COLLEGES GROUP**

**Data Protection Impact Assessment**

**Effective from:**

**Version Number: VI**

|  |  |  |
| --- | --- | --- |
| **1.** | **Purpose** | |
| 1.1  1.2  1.3  1.4 | The purpose of the Data Protection Impact Assessment (DPIA) process is designed to describe the processing of personal data, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. A DPIA must be completed at the point of considering a change in process, product or service. This will determine whether a DPIA is required.  GDPR Article 35 makes DPIAs a mandatory requirement for the controller to carry out DPIAs prior to the processing, where the processing is likely to result in a high risk to the rights and freedoms of natural persons.  The purpose of this document is to set out the procedure for completing a DPIA to identify and manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.  The DPIA must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled. This must be done prior to the processing via a Data Protection Impact Assessment and **this should be started as early as practical in the design of processing operations**. The DPIA will assess issues affecting personal data, which need to be considered before a new product/service/process is rolled out. The process is designed to:   * Describe the collection and use of personal data; * Assess its necessity and its proportionality in relation to the purpose; * Assess the risks to the rights and freedoms of individuals; and * The measures to address the risks * Where the risks revealed are not appropriately mitigated, you must contact the DPO [dataprotection@dncolleges.ac.uk](mailto:dataprotection@dncolleges.ac.uk) | |
| **2** | **The Procedure** | |
| 2.1  2.2 | A procedure should incorporate the following steps to identify the need to complete a DPIA:  Where the Group is launching or proposing to adopt a new process, product or service that involves personal data, the DPIA should be completed as part of the project initiation process.  Complete a DPIA Form (*please note: if you complete section 1 and do not meet the criteria to complete a DPIA, do not continue with this process)*  The request can be made to any member of staff, once completed the DPIA must be reviewed by the line manager, prior to submission to the DPO at [DPA@dncolleges.ac.uk](mailto:DPA@dncolleges.ac.uk) for verification and advice to proceed.  Describe the processing (nature, scope, context and purpose)  Consultation process (How stakeholder will be consulted)  Assess necessity and proportionality (Describe compliance and proportionality measures)  Identify and assess risks (risk to individual, privacy, organisation, and compliance)  Identify measures to reduce risk (controls and counter measure to mitigate/manage risk)  Submit to the DPO at [dataprotection@dncolleges.ac.uk](mailto:dataprotection@dncolleges.ac.uk) – please note the request can be denied or further information requested to support the DPIA  The DPO / Acting DPOs will assess the DPIA with relevant staff and advise whether this can be processed or a response as to why this will be declined  The DPO / Acting DPOs will verify the DPIA and log on the DPIA log  The DPO records the date that the DPIA checks were conducted and the approval date  The DPO will inform the staff member of the outcome and advise action required  The DPO/Acting DPO’s revise privacy notices if required, (subject to the DPIA requirement)  Staff member to implement new process  Staff member to keep new process under review through implementation  **This procedure is to be followed in the following circumstances:**   * Use systematic and extensive profiling with significant effects; Process special category or criminal offence data on a large scale; or Systematically monitor publicly accessible places on a large scale. * Introduction/use of new technologies; * Update or revision of a system that might alter the way in which the organisation uses, monitors and reports personal information; * Use profiling or special category data to decide on access to services; Profile individuals on a large scale; * Process biometric data or genetic data; * Match data or combine datasets from different sources; * Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing'); * Track individuals' location or behaviour; * Profile children or target marketing or online services at them; * Process data that might endanger the individual's physical health or safety in the event of a security breach; * Plans to outsource business processes involving storing and processing personal data; * Plans to transfer services from one provider to another that include the transfer of information assets; * Any change to or introduction of new data sharing agreements * Data sharing initiative where two or more organisation’s seek to pool or link sets of personal data; * Any change to access of an information asset that involves an external organisation; Changes in legislation, policy or strategies which will impact on privacy through the collection of or use of information, or through surveillance or other monitoring, e.g. CCTV cameras * The introduction of an IT system which processes large amounts of personal data.   Any person who is responsible for introducing a new or revised service or changes to an existing system, procedure or information asset is responsible for ensuring the completion of a DPIA and therefore must be effectively informed of these procedures. | |
| **3** | **Relevant Policies and Procedures** | |
| 3.1 | Data Protection Policy  Data Protection Impact Assessment Template | |
| **4** | **Who to contact with Queries** | |
| 4.1 | Data Protection Officer (Jo Garrison) – [dataprotection@dncolleges.ac.uk](mailto:dataprotection@dncolleges.ac.uk)  Acting DPO’s - [Jason.barnard@northlindsey.ac.uk](mailto:Jason.barnard@northlindsey.ac.uk) or terry.hutchinson@don.ac.uk | |
| **5** | **Communication** | |
| 5.1 | This procedure will be provided to all staff, who are required to complete a Data Protection Impact Assessment. The procedure and DPIA form will be placed on the intranet site and website of Doncaster College, North Lindsey College and DN Colleges Group. | |
| **6** | **Authorisation** | |
| Procedure Holder: | | J Garrison, Data Protection Officer |
| Committee Group: | | GDPR Core Group |
|  | |  |
| Authorisation Date: | | 01 December 2019 |
| Next Review Date: | | 01 December 2021 |

|  |
| --- |
| **7 Version Control** |

|  |  |  |
| --- | --- | --- |
| Version Number | Effective From | Review Date |
| Version 1 | 01 December 2019 | 01 December 2021 |
|  |  |  |