Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Principal	August 2023	1 August 2024

Data Protection Impact Assessment (DPIA) Policy

Updated: November 2022

Purpose

The purpose of this policy is to assist the college in identifying potential data protection risks when processing personal or sensitive data, and to help establish mitigations against those risks prior to the active processing of any data.

A Data Protection Risk Assessment is required to be completed when the processing of data is likely to result in a high risk to the rights and freedoms of individuals.

A failure to complete a DPIA when required under the UK Data Protection Act 2018 may result in a fine of up to £8.7 million or 2% of total global annual turnover, whichever is higher.

Values

Privacy by Design: The college is committed to the protection of its stakeholders' rights in regards to data privacy and the safeguarding of that data. Completion of a DPIA provides the college with the means to safeguard that data and minimise and mitigate against the risk of data breach events by designing solutions with privacy considered from the outset as part of its design.

Scope

This policy applies to all OCA employees who might be involved with the processing of new data, or for data being processed in new ways or contexts.

Any employee who might be responsible for: project initiation; introduction of new (or oversight of existing) processes, systems, applications or services, or for the development and testing of new processes, systems, applications or services must ensure they are familiar with this policy and the circumstances under which they will be required to conduct a DPIA.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Principal	August 2023	1 August 2024

Changes

Since the last version of the policy, the following changes have been made:

- Incorporated references to listed and linked forms as being only for Employees' use.

This policy was reviewed in August 2023, no changes made.

Policies superseded by this document

This policy replaces the *DPIA Policy, v1, 07/06/22*.

Related policies and legislation

This policy references:

- Data Protection and Privacy Policy
- DPIA Form (only available for internal use by OCA employees)
- DPIA Screening Questions (only available for internal use by OCA employees)

  (The DPIA Form and Screening Questions are only available for internal use by OCA employees, through Google Docs Templates, or the College-Wide Templates folder of 'Central Storage')

Policy / procedure

1. Identifying the need to complete a DPIA

1.1. A DPIA is required for data processing that is likely to result in a high risk to individuals. This includes some specified types of data processing.

1.2. As per the General Data Protection Regulations (GDPR) 2018, a DPIA must be undertaken where any initiative will involve:

a. the systematic and extensive evaluation of personal data by automated means, including profiling, resulting in decisions that would have significant effects for those individuals;

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Principal	August 2023	1 August 2024

b. the large scale processing of special category personal data[1] or personal data relating to criminal convictions; or

c. the systematic monitoring of a publicly accessible area on a large scale.

1.3. The screening questions checklist (only available for internal use by OCA employees) should be completed in order to determine whether or not a full DPIA needs to be completed. If more than one answer is yes, a DPIA will need to be completed.

2. Responsibility for completion of Screening Questions and DPIA

2.1. The individual who has initiated or proposed the task or new process must take responsibility for completion of the screening questions and (if required) the DPIA.

2.2. In the case of projects or task groups, the responsibility may be delegated to a suitable member of the project or task group, but a single accountable person must be identified.

3. Responsibility for sign off of the DPIA

3.1. All DPIAs must be submitted to the DPO (dpo@oca.ac.uk) who will make an initial review of the completed DPIA and either request further information to satisfy regulatory requirements or otherwise pass the DPIA to the Senior Management Team (SMT - smt@oca.ac.uk) for approval or rejection with a request for further information.

3.2. In cases where processing of data is urgent, the DPIA must still be completed but may be issued directly to the SMT if the DPO is unable to process the request in the required timeframe. The SMT will review the submission and approve or reject based upon provided knowledge of the declared risks and mitigations put in place.

4. For data processing that is already in place

4.1. Data processing which was already being conducted prior to the implementation of GDPR on 25th May 2018, does not strictly require a

[1] Special Category information is that which may reveal racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions.

retrospective DPIA process to be followed. However, the DPIA process (including Screening Questionnaire) should be followed at the next review point for any services that process personal data.

4.2. At each review period for any data processing service for which a DPIA already exists, the review should consider whether there have been any changes to data processing scope, method or processing partners by the service, and whether any notice of that change has been received during the intervening period.

4.3. If a data processor makes changes to its processing of personal data controlled by the college, the DPIA process should be followed in order that any objections to the changes might be raised with the data processor.

5. Undertaking the completion of a screening questionnaire

5.1. Prior to its completion and submission, any relevant stakeholders to the initiative must be consulted to ensure all aspects of the processing are collated and understood.

5.2. Where any uncertainty exists during completion of the screening questionnaire, assistance should be sought from the college's DPO who may either respond directly with advice or escalate the query to the SMT.

5.3. In cases where the outcome from the screening questionnaire is that a DPIA is not required, the reason for this must be documented and included with the questionnaire when submitted to the DPO.

6. Undertaking the completion of a DPIA

6.1. Where a DPIA is to be completed, the DPIA template (only available for internal use by OCA employees, through Google Docs Templates, or the College-Wide Templates folder of Central Storage) must be used. Where a section is considered non-applicable to the context, the reason for this must be provided.

6.2. All relevant stakeholders to the processing must be consulted as part of the DPIA's completion. This may involve college employees, students or Third Party data processors. In the case of Third Parties, an expectation of their

assistance in the completion of such forms should be made part of any contracts where possible.

6.3. In the event that a Third Party refuses to cooperate in providing information required for the processing of a DPIA, that refusal must be documented and considered as part of its next Review process.

6.4. Where external consultation is required in order to complete the DPIA adequately, that request must be made to the SMT to be reviewed at the next SMT meeting.

7. In the event of a High Risk outcome

7.1. In most situations where there is a high risk outcome despite identified mitigations and safeguards, the college will work to ensure that these risks can be reduced in order to allow processing to commence. However, where the college cannot achieve this within its own resources, consultation with the Information Commissioner's Office (ICO) must be sought by the college's DPO.

7.2. Where consultation with the ICO is sought, the request together with existing documentation relating to it must be issued to dpiaconsultation@ico.org.uk to await an outcome. ICO consultation requests will usually be processed within 8 weeks of receipt, but may take as long as 14 weeks in some instances. The ICO's recommendations should be followed, and incorporated into a new DPIA submission which will go through the same process as previously.

7.3. In a small number of cases the ICO may recommend that processing should not commence. This advice should be taken on board and alternative processing methods or additional mitigations should be considered in light of that advice.

Implementing the policy

Implementation of the Policy is incorporated into the college's Project Initiation Documentation template and the need for a DPIA is emphasised as part of the college's Data Protection E-Learning package which is completed annually by all employees.

Employees are required to complete first the Screening Questionnaire, followed by the DPIA form if required (the Screening Questionnaire and DPIA form are only available for

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Approved	Paul Vincent	OCA Principal	August 2023	1 August 2024

internal use by OCA employees, through Google Docs Templates, or the College-Wide Templates folder of Central Storage) .

Compliance Measurement

The college will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

There are no exceptions to this policy; cases where a DPIA is not required are incorporated as an aspect of the policy.

Non-Compliance

Any employee found to have violated this policy may face repercussions, up to and including termination of employment.

Support for the policy

For support in completing a DPIA or the Screening Questionnaire, please contact the college's Data Protection Officer at dpo@oca.ac.uk.