The Gosforth Federated Academies Limited

North Gosforth Academy

Data Protection Impact Assessment (DPIA) Policy and Procedure

1. Introduction

1.1 Data Protection Impact Assessments (DPIA) (also known as Privacy Impact Assessments PIA)) are an integral part of taking a 'privacy by design' approach.

1.2 A DPIA is a process which minimises the privacy risks of new projects or work activities by considering the impact that the proposed project or activities will have on the individuals involved to ensure that the potential problems are identified at the outset.

1.3 This policy and procedure is based on comprehensive guidance produced by the Information Commissioner's Office, which can be accessed at:

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

1.4 It has also been developed to meet requirements of the General Data Protection Regulation (GDPR)

2. When is a DPIA required?

2.1 The Academy is obliged to carry out a DPIA whenever it is implementing a new (or making a change to an existing) process, system, project, or work activity that could have an impact on the privacy of individuals.

3. Stages of a DPIA

3.1 Stage 1 – the initial screenings questions

3.1.1 This section is to be completed by the staff member or project lead responsible for delivering the proposed change. The purpose of the screening questions (Appendix A) is to assess whether a further DPIA assessment is required and ensure that the investment in the Academy is proportionate to the risks involved.

3.1.2 If the answers to the questions are 'no', the screening process has not identified any DPIA concerns and the process is complete.

3.1.3 If response to any of the questions is 'yes', then an initial DPIA must be undertaken.

3.1.4 It is important to get this stage right. If the Academy is challenged by the Information Commissioner's Office a decision about why a DPIA was or wasn't undertaken must be defendable.

3.2 Stage 2 – Data Protection Impact Assessment

3.2.1 The responses to the screening questions will give an indication as to the appropriate scale of the DPIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

3.2.2 The DPIA (Appendix B) must be completed by the staff member or project lead responsible for delivering the proposed change. A copy of the completed form must be sent to the Data Protection Officer in order to provide further guidance if necessary.

3.2.1 There are three possible outcomes to the initial DPIA:

- The initial DPIA is incomplete and will have to be repeated or further information obtained;
- The initial DPIA is complete and no privacy risks have been identified;
- The initial DPIA has identified a privacy risk.

3.3 Stage 3 – identifying compliance risks

3.3.1 Identifying compliance risks (Appendix C) will be necessary where there are any significant information governance risks identified. The checklist reviews the Data Protection Principles in order for each to be considered and must be completed by the project lead. A copy of the completed form must be sent to the DPO in order to provide further guidance if necessary.

3.3.2 An action plan must be developed by the project lead, on how the risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities, and timescales.

4. Measures to reduce the risk

4.1 It is important to remember that the aim of a DPIA is not to completely eliminate the impact on privacy. The purpose of the DPIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented.

4.2 Examples of measures:

- Obtaining the data subject's consent;
- Deciding not to collect or store particular types of information;
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information;
- Implementing appropriate technological and organisational security measures;
- Ensuring that staff are properly trained and are aware of potential privacy risks;
- Developing ways to safely anonymise the information, when it is possible to do so;
- Producing guidance for staff on how to use new systems and how to share data if appropriate;
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests;

- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the Academy for assistance if necessary;
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on the Academy's behalf;
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and with whom it will be shared.

5. Integrating DPIA outcomes into the project plan

5.1 The DPIA findings and actions should be integrated with the project plan. The person responsible for the DPIA and the overall project should ensure that the steps recommended are implemented and return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

5.2 If the DPIA generates actions that will continue after the assessment has finished, the person responsible should ensure that these are monitored and that all lessons learned from the DPIA are recorded for future projects.

APPENDIX A

The Gosforth Federated Academies Limited

North Gosforth Academy

DATA PROTECTION IMPACT ASSESSMENT (DPIA) INITIAL SCREENING FORM

Project name:	
Brief outline of the project:	
Project lead:	
Project dates (from – to):	

SECTION 1: DPIA screening questions

These questions are intended to help the Academy decide whether the DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

Once completed please forward to the Data Protection Officer for review.

Question	Yes (✓)	No (✓)	Notes
Will the project involve the collection of new information about individuals?			
Will the project compel individuals to provide information about themselves?			
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?			
Are you using information about individuals for a purpose which it is not currently used, or in a way not currently used?			
Does the project involve you using new technology which might be perceived as being privacy intrusive, for example, the use of biometrics or facial recognition?			

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?			
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? This might include, for example, health records, criminal records, or other information that people would consider to be particularly private.			
Will the project require you to contact individuals in ways which they may find intrusive?			

SECTION 2: Data Protection Officer (DPO) feedback/decision

APPENDIX B

The Gosforth Federated Academies Limited

North Gosforth Academy

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Project name:	
Brief outline of the project:	
Project lead:	
Project dates (from – to):	

SECTION 1: Identify the need for the DPIA

Explain what the project or process aims to achieve; what the benefits will be to the Academy, to individuals and to other parties. You may find it helpful to link other relevant documents related to the project, for example a project proposal. Also, summarise why the need for a DPIA was identified (this can draw on your answers to the DPIA initial screening questions)

SECTION 2: Describe the information flows

The collection, use and deletion of personal data should be described here. Include detail of which individuals and how many are likely to be affected by this new project or change.

SECTION 3: Consulting on the information flows

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who will be consulted, internally and externally? How will you carry out the consultation?

SECTION 4: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Please refer to Appendix C to help identify the DPA related compliance risks

Privacy issue	Risk to individuals	Compliance risk	Corporate risk

SECTION 5: Identify privacy solutions

Describe the actions you could take to reduce risks and any future steps which would be necessary, e.g. the production of new guidance or future security testing for systems

Risk	Solution(s)	**Result:** is the risk eliminated, reduced , or accepted	**Evaluation:** is the final impact on individuals after implementing solutions justified, compliant and proportionate to the aims of the project

SECTION 6: Record of DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

SECTION 7: Integrate the DPIA outcomes into the project plan

Who is responsible for integrating the DPIA outcomes into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Actions to be taken	Date for completion of actions	By whom

APPENDIX C

The Gosforth Federated Academies Limited

North Gosforth Academy

DATA PROTECTION IMPACT ASSESSMENT (DPIA) – Identifying compliance risks

Project name:	
Brief outline of the project:	
Project lead:	
Project dates (from – to):	

Answering the below questions during the DPIA process will help to identify where there is a risk that the project or activity will fail to comply with the Data Protection Principles as outlined in the General Data Protection Regulation, the Data Protection Act 2018, or any other relevant legislation.

Data Protection Principles	Question	Answer
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals	Has the purpose of the project been identified?	
	How will individuals be told about the use of their data?	
	Do the privacy notices need to be amended?	
	Have conditions for processing been established?	
	If 'consent' is required, how will this be collected, withheld or withdrawn?	
Personal data shall be collected for specified, explicit and legitimate purposes…	Does the project cover all of the purposes for processing personal data?	
	Have potential new purposes been identified as the scope of the project expands?	

Data Protection Principles	Question	Answer
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	Is the information of good enough quality for the purposes it will be used?	
	Which data could not be used, without compromising the needs of the project?	
Personal data shall be accurate and kept up to date…	Does any new software or process allow the amendment of data when necessary?	
	How will the Academy ensure the accuracy of data obtained from individuals or other organisations?	
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary…	What retention periods are suitable for the personal data being processed?	
	Will the procured system allow deletion of information in line with retention periods?	
Personal data shall be processed in a manner that ensures appropriate security of the personal data…	Will new systems provide protection against any identified security risks?	
	What training and instructions will be given to staff to operate new systems and keep data secure?	