DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

POLICY NUMBER & CATEGORY	**QSC/12/APP11**	**Quality & Standards**
VERSION NO & DATE	**1**	**March 2018**
ANTICIPATED REVIEW DATE:	**March 2020**	

CONTENTS

1 SCOPE

1.1 All projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

2 RESPONSIBILITIES

2.1 The Data Protection Lead (DPL) is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA .

2.2 The Board of Trustees and DPL are responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

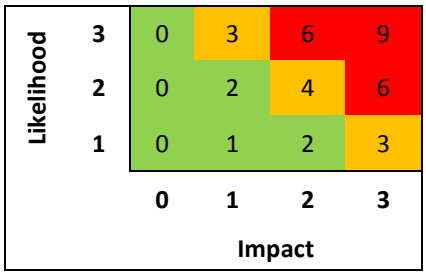
2.3 Risk Owners are responsible for implementing any privacy risk solutions identified.

3 PROCEDURE

3.1 The Data Protection Officer at Focus Learning Trust and the DPL identify the need for a DPIA at the start of each project, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the DPIA tool

3.2 Using the criteria below, following the likelihood and impact matrix, Organisation Name defines the risks to rights and freedoms of data subjects as:

Likelihood and Impact Matrix



Risks to rights and freedoms of data subjects:

Risk Level	From	To	GDPR Assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

3.3 Data processing workbook (data flow)

3.3.1 Focus School Dunstable and Northampton Campus (hereafter the Campus) records key information about all personal data processed for each project in the DPIA Tool workbook. This includes a description of the processing and purposes; legitimate interests pursued by the controller; an assessment of the necessity and proportionality of

the processing; an assessment of the risks to the rights and freedoms of data subjects (as per the matrix and risk level definitions in clause 3.2 above).

3.3.2 The Campus captures the type of processing activity associated with the personal data being processed as part of the project. These are categorised as:

- Collection
- Transmission
- Storage
- Access
- Deletion

3.3.3 The Campus establishes on what lawful basis the data is being processed and its appropriate retention period (in line with the Data Retention Policy)

3.3.4 The Campus identifies the category of data processed, whether it is personal, special or that of a child's, and the format of the data.

3.3.5 The Campus identifies who has access to the data (individuals, teams, third-parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is trans-border processing.

3.4 Identify privacy risks

3.4.1 The Campus assesses the privacy risks for each process activity as described in clause 3.2 above by:

- Identifying and describing the privacy risk associated to that process activity
- Using the likelihood criteria (1 – low, 2 – medium and 3 - high), scoring the likelihood of the risk occurring
- Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 - high) of the risk should it occur
- Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.

3.4.2 In assessing the privacy risks, the Campus considers:

- risks to the rights and freedoms of natural persons resulting from the processing of personal data;
- risks to the organisation (including reputational damage); and
- Its objectives and obligations (both regulatory and contractual).

3.4.3 The Campus identifies solutions to privacy risks, assigns a risk treatment owner and sets a target date for completion.

3.4.4 The Campus prioritises analysed risks for risk treatment based on the risk level criteria established in clause 3.2 above.

3.4.5 The Campus risk owner, in consultation with the DPL, approves and signs off each DPIA for each data processing activity.

3.5 Prior consultation (Article 36, GDPR)

3.5.1 Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, the Campus consults with the supervisory authority (the ICO), using the following method.

3.5.2 When the Campus requests consultation from the supervisory authority it provides the following information:

- detail of the responsibilities of the Campus (controller), and if relevant the data controller/processor/joint controller involved in the processing;
- purpose of the intended processing;
- detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
- contact details of the DPL as recorded;
- a copy of the data protection impact assessment; and
- any other information requested by the supervisory authority.