Grange
Primary
School

*Growing the seeds*

*for Lifelong learning*

# Data Protection Impact Assessment Procedure

npw

Services for schools, owned by schools

## Overview

Data Protection Impact Assessment (DPIA) is the term the General Data Protection Regulation (GDPR) utilises for the risk-based approach and pre-assessments for high-risk processing.

DPIAs are a requirement of the GDPR and a tool that can assist those with data protection obligations in identifying risks associated with data processing and posed to data subjects. It enables a pre-emptive approach to assess the risks and apply corrective actions and mitigating controls before a breach occurs.

The overall aim of the DPIA is to apply solutions and mitigating actions where a processing activity is deemed likely to cause a high risk to one or more individuals. The mitigating actions are then implemented into the project plan and then reassessed to ensure that the risk(s) has been eliminated or reduced to an acceptable level. The overall scope of the risk solutions is to either: -

- **Transfer** the risk to another party
- **Tolerate** the risk by acceptance
- **Terminate** the risk by not proceeding with the proposed change
- **Treat** the risk by implementing solutions to reduce likelihood or impact

Where a DPIA indicates that the processing involved will or is likely to, result in a high risk to an individual and it is not possible to mitigate such risk with appropriate measures or controls, the School will consult the Information Commissioner's Office (ICO) prior to the processing taking place.

## Responsibilities

All staff, contractors and temporary staff are required to inform the Data Protection Officer (DPO) of any planned projects which involve personal data.

The DPO is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

Under guidance from the DPO, the School is responsible for checking that appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and the subsequent decision to proceed with processing.

## DPIA Procedure

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the School or any 3rd parties. When the risks of processing are high, the School employ the use of DPIAs to assess the risk, the impact and the likelihood, and to document the origin, nature, and severity of that risk, along with the processing purpose, reasons and mitigating measures and/or proposed solutions.

## Identify if a DPIA is required

A DPIA is required whenever there is processing that is likely to result in a high risk to the rights and freedoms of individuals.

In particular, the GDPR specifies that a DPIA must be conducted if the School plans to…

- Use systematic and extensive profiling with significant effects
- Process special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale

The ICO also requires you to conduct a DPIA if you plan to…

- Use new technologies
- Use profiling or special category data to decide on access to services

- Profile individuals on a large scale
- Process biometric data
- Process 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 services at them
- Process data that might endanger the individual's physical health or safety in the event of a security breach

The School will inform the DPO of any proposed changes which may result in the need for a DPIA. The DPO will ascertain if a DPIA is required by the use of screening questions (see Appendix 1).

## Completing the DPIA

The DPO will complete the DPIA Form (see Appendix 2) using appropriate tools and with support from the School. The details required will include a description of the proposed process and its purpose and an assessment of the risks to the rights and freedoms of data subjects.

The type of processing activity will be captured and will include collection, transmission, storage, access and deletion of personal data.

In line with the School's retention policy, the lawful basis for the processing of data will be documented.

The category and format of the data to be processed will be established and documented accordingly.

The DPIA will also be populated with who has access to the data, who is involved with the processing of personal data, recording the geographic location of where the processing takes place and if there will be any transborder processing.

## Risk Analysis

Using the responses obtained from answering the assessment questions, privacy issues and associated risks can be identified, the project team will use best judgement and reasoning in order to assess the likelihood and impact to personal data.

Once the risks have been identified, the below risk matrix is used to give the risk a rating based on the severity of the impact and the likelihood of the risk occurring. This rating provides an easy to see colour code for how severe the risk could be to the privacy of individuals and therefore the necessity of implementing mitigating actions, or reassessing using the processing activity.

The risk rating table below uses the common 'Red, Amber, Green (RAG)' matrix, where each risk is given a RAG score based on the likelihood versus the impact.

| | | IMPACT | | | | |
|---|---|---|---|---|---|---|
| | | Trivial | Minor | Moderate | Major | Severe |
| LIKELIHOOD | Almost Certain | Low Med | Medium | High | Very High | Very High |
| | Likely | Low | Low Med | Med High | High | Very High |
| | Possible | Low | Low Med | Medium | Med High | High |
| | Unlikely | Low | Low Med | Low Med | Medium | Med High |
| | Rare | Low | Low | Low Med | Medium | Medium |
| Impact x Likelihood = Risk | | | | | | |

- **GREEN** - Where an assessment outcome is Green, work should still be undertaken to see if the School can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Where a green RAG rating has been assessed, the risk is still added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.
- **AMBER** - Where an assessment outcome is Amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (acceptable) level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.
- **RED** - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered to high risk to proceed.

The outcomes will be recorded on the Privacy Issues and Associated Risk form (see Appendix 3).

## Evaluate DPIA

Where risks are identified, wherever possible consider action to mitigate the risk.  It may not be possible to eliminate all risks.  Where the School is unable to reduce risks to an acceptable level, a decision may be made to cancel the project.  The aim is always to assess whether the impact on privacy is proportionate to the objectives of the project and to ensure that individuals and their privacy remain the priority.

Any proposed solutions will be documented on the Risk Solutions form (see Appendix 4).

The risk rating obtained in the Risk Identification process is used to ensure that the School is aware of the current risk and what an acceptable level would be.  The new risk rating is then added to the template.

Some of the steps that may be used to mitigate risks include…

- Changing the personal information collected to reduce the privacy level when processing
- Carry out all processing in-house to avoid transfers or data sharing
- Utilise systems/technology to make the processing more accessible
- Creating new procedures for areas such as retention, destruction methods, exercising rights
- Developing new security measures for a specific project that align with its aims
- Ensuring that adequate and effective training is provided to staff of the data protection regulations and the project processing
- Publishing guidance manuals and supporting documents for use by those involved in the project
- Creating new materials and website content to enable better communication with individuals
- Carrying out higher level of due diligence on any processors used for the project
- Producing data sharing agreements and transfer contracts

Costs and benefits associated with all solutions will be reviewed to ensure that they are viable, feasible and proportionate to the DPIA impact.  All solutions also involve a review and input from the DPO, who reviews them against the GDPR and any codes of conduct that are followed in accordance with data protection laws.

## DPIA Outcomes

If a high risk is identified and the School wishes to proceed with the proposed change, the ICO must be consulted and advice should be received prior to the commencement of processing.

## Compliance

All staff are expected to comply with the School's policies to the highest standards.  If any School employee is found to have breached this policy, they may be subject to the School disciplinary procedure.  If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

## Appendix 1 – DPIA Screening Questions

| Screening questions | Y/N | Comments |
|---|---|---|
| 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 it is not currently used for, or in a way it is not currently used? | | |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? | | |
| 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? | | |
| Will the project require you to contact individuals in ways which they may find intrusive? | | |

**Notes**

- If the answers to all of the above screening questions are NO, it is unlikely that a DPIA will be required.
- If the answers to at least one of the questions above is YES, a DPIA should be conducted.
- A copy of this screening questionnaire should be retained.

**Appendix 2 – DPIA Form**

# Data Protection Impact Assessment Form

| | | |
|---|---|---|
| **Project Name** | | **Directions**<br>• Complete each section and answer all questions<br>• Provide as much detail as possible to ensure a complete assessment is made |
| **Author** | | |
| **School** | | |
| **Date** | | |

## 1 Project Background

| | | |
|---|---|---|
| 1.1 | **PROJECT SUMMARY:** Give an outline of the project, the processing and describe what is being planned | |
| 1.2 | **CONSULTATIONS:** - Detail any findings from discussions with stakeholders that may impact upon the security of personal data | |
| 1.3 | **OTHER:** - Detail any other information or suggestions that can add to the impact assessment? | |

## 2 Information Audit

| Personal Data | | Justification | Processing Activity |
|---|---|---|---|
| What data will be collected? | | Why does this data need to be collected? Is there anything you can omit if not necessary? | What processing operation(s) will the data be used for? |
| First Name + Surname | | | |
| Address | | | |
| Postcode | | | |
| DOB | | | |
| Age | | | |
| Gender | | | |
| Email Address | | | |
| Tel No. | | | |
| NI Number | | | |
| Income/Expenses | | | |
| Employment Data | | | |
| Ethnicity | | | |
| Religion | | | |
| Health Details | | | |
| Convictions | | | |
| SEN | | | |
| FSM | | | |
| Profile Picture | | | |
| Other (complete below) | | | |

| 3 Assessment Questions | | |
|---|---|---|
| 3.1 | What is the legal basis for processing the data? | |
| 3.2 | If consent is used as the legal basis, how will this be obtained and the right to withdraw consent be made available? | |
| 3.3 | Who will have access to the data? (School staff/3rd parties etc.) | |
| 3.4 | Will there be restrictions applied to access? (strong passwords, 2 factor authentication etc.) | |
| 3.5 | Does the data need to be transferred to a third-party? | |
| 3.6 | Are safeguards in place for transferring the data? (encryption etc.) | |
| 3.7 | Will personal data be transferred to a third country or international organisation outside the EEA?<br>If yes, what safeguards and Chapter 5 GDPR measures are in place? | |
| 3.8 | How will the data be kept secure? (ISO 27001, encrypted at rest etc.) | |
| 3.9 | How will consent be obtained and the right to withdraw consent be made available? | |
| 3.10 | Will the school retain control over data and be able to update where necessary? | |
| 3.11 | Are all data items necessary? (data minimisation) | |

| | | |
|---|---|---|
| 3.12 | How will the data be stored? (cloud, local PC etc.) | |
| 3.13 | How will the data be destroyed after it is no longer necessary? (deleted, deleted from all backups, shredded etc.) | |
| 3.14 | How long will data be retained for? | |
| 3.15 | Will the ability to act on all rights of data subjects be retained? (i.e. objection, rectification, erasure, access etc.) | |
| 3.16 | Will the system be used in a way other than expected which may increase the risk to data? | |
| 3.17 | Have all employee, agents and third parties involved in the project been trained on data protection regulations? | |
| 3.18 | Is a GDPR compliant contract in place? | |
| 3.19 | Will any processors transfer data to any sub processors? | |

**Appendix 3 – Privacy Issues and Associated Risks Form**

| Privacy Issues and Associated Risks | | | | | |
|---|---|---|---|---|---|
| | **Privacy Issue** | **RAG** | **Risks to Individual(s)** | **Compliance Risk** | **Risk to School** |
| # | Use assessment response to detail the privacy factor resulting in risk | Risk Rating | Complete if risk impacts data subject(s) or put N/A if not applicable | Complete if risk causes non-compliance or put N/A if not applicable | Complete if risk impacts business or put N/A if not applicable |
| PR1 | E.g. Processing makes it difficult to withdraw consent once given | Medium | Affects right to withdraw consent<br>Unlawful processing | Breaches Article 7(3)<br>Unlawful processing | Breach fines<br>Reputational damage |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Appendix 4 – Risk Solutions Form**

## Risk Solutions

| | Risk | RAG | Solution | Result | Outcome | RAG |
|---|---|---|---|---|---|---|
| # | Risk to be mitigated | Current rating | Detail corrective actions, solutions and mitigating controls that address the risk | Reduced, Eliminated or Accepted | Has the solution(s) reduced the risk enough to proceed with processing? | New risk rating |
| PR1 | E.g. Difficult to withdraw consent once given | Medium | Create communication to be sent to individual(s) with guidance for withdrawing consent in writing | Withdrawal possible, but only in 1 format - Reduced | Due to type/location of processing, withdrawal of consent can only be done in writing. Can't offer opt-out or automated withdrawal options at this time | Medium |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | | |
|---|---|---|
| Status: Approved | Approved by Governing Body date: Sept 2018 | |
| Last Updated: | Next Review: Sept 2019 | Version: 1.0 |