

---

# THE CAREY FEDERATION

---



*Aim High; Be Resilient; Take Care of Each Other*

## Data Protection

DATA PROTECTION IMPACT ASSESSMENT POLICY  
APPENDIX 5 OF DATA PROTECTION POLICY

|                        |  |                       |          |
|------------------------|--|-----------------------|----------|
| <b>Author</b>          | <b>Name</b>                            | Ruhaina Alford        |          |
|                        | <b>Job Title</b>                       | Executive Headteacher |          |
|                        | <b>Date policy created</b>             | 12.01.22              |          |
| <b>Approved by:</b>    | The Carey Federation<br>Governing Body | <b>Approved date:</b> | 20.1.22  |
| <b>Version number:</b> | 1                                      | <b>Review date:</b>   | Jan 2024 |

## Contents

|    |  |   |
|----|--|---|
| 1  | Purpose .....  | 2 |
| 2  | Introduction.....  | 2 |
| 3  | Responsibilities.....  | 2 |
| 4  | Implementation of policy.....  | 3 |
| 5  | Review.....  | 3 |
|    | Annex 1: Procedure for managing data protection impact assessments ..... | 1 |
| 1. | Data protection impact assessment resources.....                         | 1 |
| 2. | Procedure overview.....  | 1 |
| 3. | Notification of a potential candidate for a DPIA. ....                   | 1 |
| 4. | Determining if a DPIA is necessary. ....                                 | 2 |
| 5. | Documenting the Proposal. ....   | 2 |
| 6. | Assess the risks.....  | 3 |
| 7. | Proposing mitigations .....  | 3 |
| 8. | Approval and consulting the ICO .....                                    | 4 |

## 1 Purpose

The Carey Federation (the Federation) is required to follow the Data Protection Act (2018) (the Act) in the way that it collects and uses personal data. The Act references and implements the UK General Data Protection Regulation (UK GDPR) with some specific amendments.

Section 3 of Chapter 4 of the UK GDPR sets out the requirement upon data controllers and data processors to ensure that the risks to the rights and freedoms of individuals from projects that create substantial changes in data processing are reviewed. This review should take place before the proposed processing is undertaken. Such a review is called a Data Protection Impact Assessment (DPIA)

This policy sets out the approach that the Federation will take to deal with data protection impact assessments. This policy applies to all employees of the Federation.

The Data Protection Officer is GDPR Sentry.

## 2 Introduction

Complying fully with the Data Protection Act, including the GDPR, demands that organisations adopt a risk managed approach to data protection. This means that measures taken to ensure the confidentiality, availability and integrity should be proportionate the risks posed by the processing to the rights and freedoms of data subjects.

Where the Federation is proposing changes to processing, whether by introducing novel means, or changing the method of existing processing, the relative risk assessment changes.

For initiatives that meet specific criteria a more detailed assessment must be undertaken. The assessment sets out the necessity of the processing, the reasons why the approach chosen is preferred and enumerates the risks associated with the proposal.

For identified risks, mitigations should be considered from the points of view of both the effect on the risk and whether the cost of mitigation is acceptable. A list of mitigations that the Federation is willing to undertake should be compiled. This enables an assessment of residual risk. The level of residual risk may require additional consideration of mitigation, but if all acceptable mitigation has been considered and the residual risk remains high then the position will need to be discussed with the Information Commissioner's Office.

Related policies

This policy is closely linked with other policies which should be referenced when appropriate, including:

- Data Protection Policy
- Any other relevant guidance

## 3 Responsibilities

3.1 The Federation will:

- 3.1.1 1.1.1 Put in place a clear procedure for dealing with data protection impact assessment. This procedure should take account of the requirements laid down in Annex 1.

- 3.1.2 Follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy.
- 3.1.3 Inform the Data Protection Officer of any initiatives that might require a data protection impact assessment to be undertaken.
- 3.1.4 Provide access to suitable expert resources to allow the risks and mitigations for the proposed project to be considered.
- 3.1.5 Provide written feedback confirming which mitigations are accepted and which rejected including the rationale for any measures rejected.
- 3.1.6 Take advice from the Data Protection Officer with regards to the management of data protection impact assessments
- 3.1.7 Commit to implementing agreed mitigations
- 3.2 The Data Protection Officer will:
  - 3.2.1 Provide guidance and support to the Federation in dealing with data protection impact assessments.
  - 3.2.2 Provide a route of communication to the Information Commissioner's Office in the event of high residual risk projects.

#### 4 Implementation of policy

This Policy shall be deemed effective on 20/01/22. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

#### 5 Review

This policy on data protection impact assessments will be reviewed bi-annually, or when the Information Commissioner's Office (ICO) issues revised guidance on this topic.

## Annex 1: Procedure for managing data protection impact assessments

### 1. Data protection impact assessment resources

Unlike most other data protection tasks, the conduct of a data protection impact assessment is mostly done by team members without specialist data protection training.

Where an initiative is to include Federations or other premises owned by the Federation, representatives of those parts of the organisation should be involved.

Other staff involved should include:

- A senior leadership sponsor
- An IT Lead for the project where appropriate
- The business owner of the project
- Representatives of any data processors where they exist

The team should be led by a representative of the owner of the initiative.

### 2. Procedure overview

The procedure for managing data protection impact assessments needs to be implemented in detail across the Federation. These procedures need to take account of the following stages and requirements. The actions described in this section are by no mean exhaustive. The Federation may establish further detailed procedures and work instructions. Where this happens, they will be referred to in the main body of this policy.

- Notification of a potential candidate for a DPIA
- Determining if a DPIA is necessary
- Documenting the proposal
- Assessing the risks
- Proposing mitigation
- Approval and consulting the ICO

### 3. Notification of a potential candidate for a DPIA.

This element of the process is the responsibility of staff outside the normal sphere of data protection (unless the new processing relates to managing data protection information). It is therefore essential that all staff are briefed on the recognition of a potential candidate initiative.

It is likely that this will, initially, result in a large number of potential candidates being notified.

Initial notification should include:

- The purpose of the proposed processing
- The number of data subjects it is likely to affect

- The amount of personal data that will be processed
- Whether special category personal data or criminal records data will be processed
- Whether there is any automated decision making
- Whether the initiative has been mandated by government

#### 4. Determining if a DPIA is necessary.

This task is best carried out by the data protection lead in concert with the data protection officer. The details of the initiative will be compared to the criteria set out in Article 35 of the GDPR. This will determine if an automatic DPIA is required.

If an automatic DPIA is not required then the initiative will be compared against the guidance in the Article 29 Working Party (now the EU Data Protection Board) document WP 248 rev.01. This document establishes additional criteria for undertaking a DPIA. In addition the Information Commissioner's Office has published a set of criteria.

The DPO has access to a tool that reviews these various criteria. If the review shows that a DPIA is not required, the initiative will be handed back to its operational owner to progress. If a DPIA is indicated, then this process will continue.

#### 5. Documenting the Proposal.

This part of the process is dependent on the team dealing with the proposed processing. Paragraph 7 of Article 35 of the GDPR sets out the minimum requirements and this is explained in further detail in the guidance in WP 248 rev.01. Paragraph 7 of Article 35 is reproduced below:

*7. The assessment shall contain at least:*

*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.*

*(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes.*

*(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

*(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

In this step we are focused on (a) and (b). Given the overall requirement to demonstrate that the processing of personal data is proportionate and necessary, in addition to a full description of the method by which data will be processed, attention must be given to when the proposed method of processing has been chosen.

It is also required to show that the outcome of the processing is necessary, has a lawful basis and that there is no other means of processing to achieve the same objectives that would require less intensive use of personal data.

For major projects, usually with a substantial IT component, it is normal to involve suppliers in this phase.

Normal outputs from this phase are:

- A diagram showing the flow of personal data and the operations performed
- The data protection features of the proposed system
- A functional specification of the proposed system
- A document outlining necessity, lawfulness and alternatives considered

This phase should be completed before any purchasing decision has been made. In a project involving a tendering exercise the outputs, especially the review of data protection features, should form part of the selection of supplier.

## 6. Assess the risks.

This phase is where expert data protection input is essential. Working from the functional specification and data flow diagram, the team identify where the processing might create risks to the confidentiality, availability and integrity of the personal data being processed.

They should also look at whether there are risks against any of the other principles of data protection.

Where risks are identified they should be documented and then scored in terms of the likelihood of occurring and the impact on data subjects if they should occur. Similar to considering a breach, the assessment should look at the worst-case scenario in terms of impact.

For example, if a proposal has special category data on health conditions being transferred by email then there is reasonable level of risk that it will at some point be misdirected and the potential consequences include acute embarrassment, distress and exclusion from relationships and activities depending on the exact nature of the content.

A severity / probably matrix is useful for this purpose and should ideally have an even number of categories to prevent centre bias.

Although it is preferable for all members of the team to agree the scoring the data protection lead, or data protection officer should have final say if consensus can't be reached.

## 7. Proposing mitigations

This step can often overlap with the risk assessment but should be completed afterwards.

With a list of identified and scored risks, the full project team can put forward ways to mitigate the risk. These methods may be both technical or organisational.

A view can then be taken about the degree to which any proposed mitigation will reduce the likelihood of an incident, limit its' impact or both. At the same time a mitigating action may impact the functionality of the proposed processing and may also incur an additional cost. These aspects of the mitigations must also be evaluated.

Once prepared it is for the project sponsor to determine which of the proposed mitigations is acceptable.

This enables a view to be taken about the level of risk that remains in the projects, call the residual risk.

Proposed mitigations should be documented along with the decision of the project sponsor.

This stage can be cyclical. An initial set of proposed mitigations are produced and evaluated then agreed. If there is still a significant residual risk, additional measure may be considered and evaluated. This may repeat several times.

At the end of the stage there will be a final set of proposed mitigations along with costs and a statement of final residual risk.

## 8. Approval and consulting the ICO

The data protection officer is required to provide written advice to the project sponsor based on the outcome of the analysis. This will include an assessment of the final risk level.

The data protection officer is required to say whether, from a data protection perspective only, the proposed processing should move forward.

The project sponsor then makes a final decision about moving forward. The advice and the decision should be documented.

It is legitimate, in some cases to move forward when the residual risk is high. This is most likely to happen where the processing is in an area that is new or the replacement of a manual method of processing with some type of system.

In some cases, the benefits delivered to data subjects outweigh the residual risks.

In this situation a report of the DPIA must be submitted to the Information Commissioner's Office. A dialogue will follow with the ICO to establish that the high residual risk processing is necessary and that no further mitigation can be economically pursued.