DATA PROTECTION IMPACT ASSESSMENT POLICY

POLICY:	**Data Protection Impact Assessment Policy**
Author:	Greg Dwyer
Division:	ICT
Date:	Sept 2022
Review Date:	March 2023

Contents

DATA PROTECTION IMPACT ASSESSMENT POLICY

1.0 Background

The Information Commissioner's Office has issued guidance and a comprehensive handbook about the use of Data Protection Impact Assessments (DPIA). It recommends use of these techniques so that organisations can identify the risks in the use of personal data in projects and processes, both present and planned. A properly completed DPIA helps to identify any potential problem areas or risks, mapping the procedure for the implementation of any current or new process controls involving information systems, software and/or hardware. The completion of a DPIA may help to reduce any enforcement action against Rushcliffe Borough Council in the event of a personal data breach.

2.0 Purpose

The purpose of this policy is to identify the procedure to be followed by all Rushcliffe Borough Council officers who are responsible for designing processes and the implementation of projects and technology involving personal data.

The benefits to this process are:

- Risk is mitigated and process actions are designed-in as part of the process/project rather than the process requiring redesigning after implementation.
- A change of use or process change is assessed to ensure information security isn't compromised because of the amendment.
- Increased stakeholder and public confidence in the Council's processes.
- Ensure compliance with the UK General Data Protection Regulation and the Data Protection Act (2018), setting out practical steps on
- how this can be achieved.

3.0 Scope

This policy applies to all personal and sensitive data and related information systems managed by Rushcliffe Borough Council**.**

4.0 Policy

4.1 Principles

Rushcliffe Borough Council processes large amounts of personal and official sensitive data and implements processes, systems and technologies to process this data.

Rushcliffe Borough Council should assess the risks attached to the processing of personal data in each project, process and change of usage. This assessment should be undertaken in conjunction with the Data Protection Impact Assessment (DPIA) form (see appendix 1).

Adherence to this policy allows the Council to identify and mitigate the impact of any risks associated with the processing of personal data when implementing new technologies, systems, designing processes and amending existing

technologies, systems and processes. This may negate or reduce any potential fine from the Information Commissioner's Office in the event of a personal data breach.

4.2 Risk

Non-compliance with this policy may result in legal action being taken against the Council which may result in financial loss, an inability to provide services to our customers and adversely impact the Council's reputation**.**

4.3 Assertions

All employees handling personal information must familiarise themselves with this policy.

In the event of processes, systems and technologies being implemented or amended, the Data Protection Impact Assessment Guidance must be adhered to, which is available on the intranet.

4.4 Responsibilities

Departmental heads, managers, system owners, project managers and contract managers are responsible for ensuring their processes and systems comply with this policy and guidance.

The Chief Information Officer is responsible for this policy.

The Data Protection Officer is responsible for guiding and advising officers regarding Data Protection and the use of DPIAs**.**

5.0 Related Policies, Standards and Guidelines

This policy should be read in conjunction with the:

Data Protection Impact Assessment Guidance
Data Protection Policy
Information Classification Policy
Data Sharing Agreements and Data Processing Contracts
Information Technology Service Management Standards
Information Security Management Standards
Information Management Policy
Project Management Policy

6.0 Terms and Definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in Appendix A of the Information Security Policy.

7.0 Enforcement

Any user or administrator found deliberately contravening this policy or caught jeopardising the security of information that is the property of Rushcliffe Borough Council may be subject to disciplinary action and, where appropriate, legal action.

8.0 Review

This document will be reviewed annually as a minimum or wherever there may be a change of influencing circumstances.

9.0 Appendix

DATA PROTECTION IMPACT ASSESSMENT GUIDANCE & PROFORMA

OVERVIEW

This Guidance sets out the process required to complete a Data Protection Impact Assessment (DPIA).

1.0 What is a Data Protection Impact Assessment?

A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

It helps assess the level of risk, considering both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

If you identify a high risk and you cannot mitigate that risk, you must consult the ICO before starting the processing.

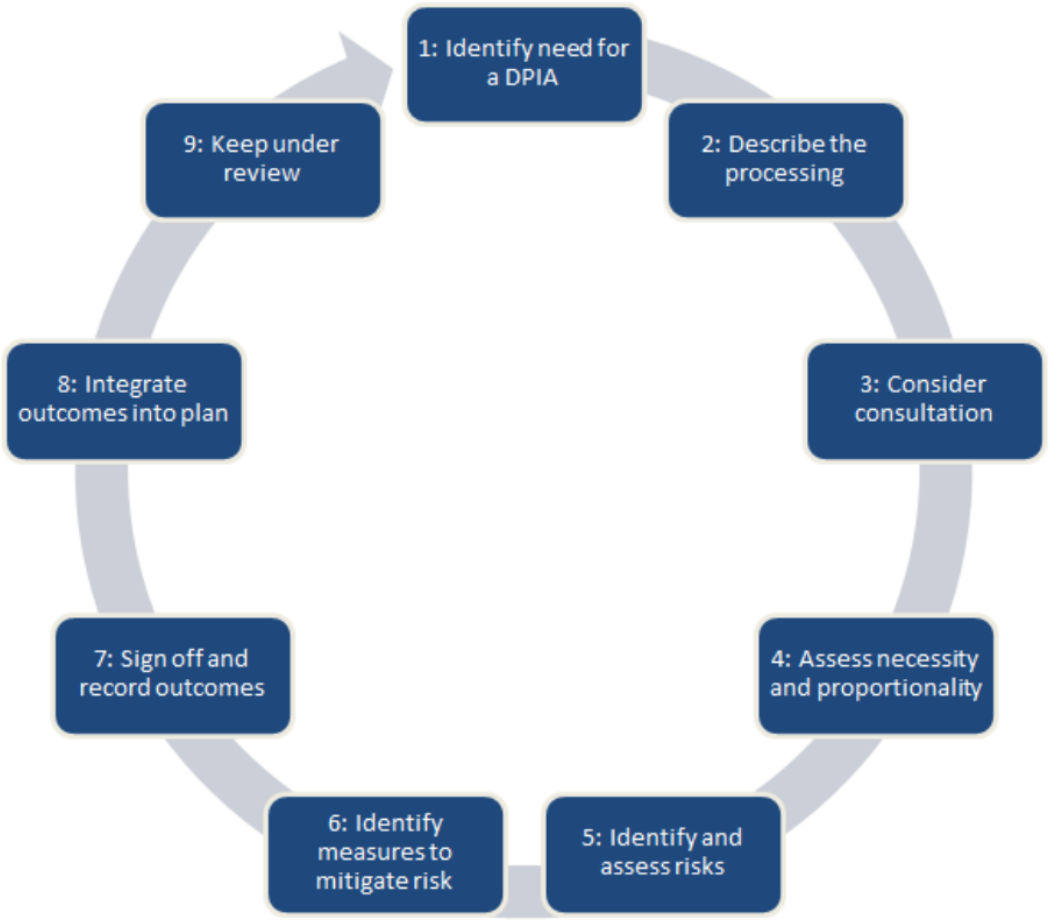
2.0 When Should a Data Protection Impact Assessment be completed?

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”.

This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.

3.0 Privacy Impact Assessment Process

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



Appendix A – Initial Screening Questions

A1	User Name (completed by)	
A2	Project / Process Title	
A3	Description of Process / Project	
A4	Is it a new project / process or an amendment to an existing process / project?	
A5	What 'types' of information 'is / will' be processed? (i.e. Name, DOB, Company Information) and does any of the information come under the **OFFICIAL SENSITIVE** classification?	
A6	Which of these 'types' of information identified in A5 'is / will' be specifically Personal Data? (and classified as **OFFICIAL SENSITIVE**) (If none put 'none')	

If in response to question 5 personal data is being processed please complete the questions in Appendix B.

If in response to question 5 no personal data is being processed no further action is required.

PRIVACY IMPACT ASSESSMENT FORM

Definitions

Personal Data is:

"Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.".

Processing is:

"Any operation which is performed on personal data; collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure and dissemination".
–

Appendix B – Privacy Impact Assessment Questions

Data Subjects and Personal Data	
B1	Who are the Data Subjects? (Residents, employees, a particular group of employees etc.)
B2	How many Data Subject records will be processed? (How many individuals' data is involved)
B3	What types of personal information will be processed? (i.e name, address, date of birth etc.)
B4	Are **all** types of personal information in **B3** required?
B5	What is the justification for processing these types of data? (Why do we need this personal information?)
B6	Is there a statutory requirement to process this data? (Please quote regulations if 'yes')
Fair Processing	
B7	Does the Data Subject know about the use of their personal information?
B8	If 'yes' to **B7** how were they informed and have they specifically given their consent?

PRIVACY IMPACT ASSESSMENT FORM

Security	
B9	Where will the personal information be stored and how?
B10	Who will have access to the personal information?
B11	What security is in place to stop unauthorised access or loss of this personal information?
Data Sharing	
B12	Will the personal information be shared / visable?
B13	If 'yes' to B12 please detail who it will be shared? Please list external and internal departments and organisations.
B14	If 'yes' to B12 please detail why it will be shared with the organisations listed in B13?
B15	How will the personal information be shared? What security arrangements are in place for external data sharing? (The transferring / movement of data).
B16	Will the personal information leave the location identified in B9?
B17	If 'yes' to B16, please explain why.
B18	Is there a data processing or sharing agreement in place?

PRIVACY IMPACT ASSESSMENT FORM

Disposal	
B19	What is the retention period for the personal information?
B20	How will the personal information be securely disposed of when no longer required?
Compliance and Proportionality	
B21	What is the lawful basis for processing? (Consent, Contract, Legal Obligation)
B22	Does the processing actually achieve your purpose and is there an alternative way to achieve the same outcome?
B23	How will you ensure data quality (accuracy) and data minimisation (the least amount needed to process)?
B24	What information will you give individuals and how will you help to support their rights? (The right to amendment, deletion, cessation of processing, portability, deletion of entire records)
B25	What measures do you take to ensure processors comply? (3rd party processing contract in place, etc.)

Appendix C – Identified Risks (C1) and Mitigating Actions (C2)

What risks can be identified with regards to the processing of personal information and adherence to the General Data Protection Regulation? (In particular ensuring the data is accurate, secure, lawfully processed, for the intended purpose and ultimately retained).

THE INFORMATION IN THE TABLE IS AN EXAMPLE. YOU WILL NEED TO TAILOR THIS TO YOU OWN PROJECT AND REPEAT THE TABLE FOR EACH IDENTIFIED RISK.

REFERENCE:				
Describe the source of risk and nature of potential impact on individuals (C1). (Include associated compliance and corporate risks as necessary)	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Responsibility**
Mitigating Actions (C2)	**Effect on risk** (Eliminated reduced accepted)	**Residual risk** (Low/medium/high)	**Measure approved** (Yes/No)	**Date action implemented**

REFERENCE:				
Describe the source of risk and nature of potential impact on individuals (C1). (Include associated compliance and corporate risks as necessary)	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Responsibility**
Mitigating Actions (C2)	**Effect on risk** (Eliminated reduced accepted)	**Residual risk** (Low/medium/high)	**Measure approved** (Yes/No)	**Date action implemented**

REFERENCE:				
Describe the source of risk and nature of potential impact on individuals (C1). (Include associated compliance and corporate risks as necessary)	**Likelihood of harm** (Remote, possible or probable)	**Severity of harm** (Minimal, significant or severe)	**Overall risk** (Low, medium or high)	**Responsibility**
Mitigating Actions (C2)	**Effect on risk** (Eliminated reduced accepted)	**Residual risk** (Low/medium/high)	**Measure approved** (Yes/No)	**Date action implemented**

OFFICE USE ONLY

Item	Name / Date	Notes
Measures Approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO Advice Provided: (Maybe n/a)		DPO should advise on compliance, step 7 measures and whether processing can proceed
Summary of DPO advice: (If referred to)		
Comments:		
DPIA Review Date:	/ /	

OFFICE USE ONLY

Item	Name / Date	Notes
Measures Approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO Advice Provided: (Maybe n/a)		DPO should advise on compliance, step 7 measures and whether processing can proceed
Summary of DPO advice: (If referred to)		

Comments:	
DPIA Review Date:	/ /

10.0 Document Attributes

Document Information

Title	Data Privacy Impact Assessment Policy
Identifier	Data Privacy Impact Assessment Policy
File Location	
Description	Data Privacy Impact Assessment Policy
Keywords	Data Privacy Impact Assessment Policy
Format	MS Word
Author	Greg Dwyer
Owner	CIO
Classification	OFFICIAL
Date Created	02 March 2018
Last Review Date	Sept 2022
Next Review Date	March 2023
Date to Dispose	12 months after latest revision

Document History

Date	Summary of Changes	Version
02 March 2018	Initial creation of document	1.0
20 April 2018	Reviewed and Updated by CIO	1.1
26 November 2018	Further review and update by CIO	1.2
27 November 2018	Final Review by CIO	1.3
25 March 2019	Revised for RBC use	1.4
07 April 2020	Reviewed, no changes	1.5
17/03/2021	Reviewed, no changes	1.6
27/03/2022	Changed reference to GDPR to UK GDPR (CF)	1.7

Document Approval

Date	Name & Job Title of Approver(s)	Version

Distribution

Name / Group	Title
Heads of Service	

Coverage

Group
All employees

End of Document