

Data Protection Impact Assessment Template

Author: Information Governance Manager

Date: March 2022

Version: V0.1

Title	Data Protection Impact Assessment Template
Author	Information Governance Manager
Owner	Information Governance Manager
Subject	DPIA Template
Created	Marcus Connor and Jacqueline Williams
Approved by	Information Governance Steering Group
Date of Approval	7 March 2022
Review Date	7 March 2024

1. Document Version Control

Document Version Control	
Issue Number	Date
1.0	March 2022 (Bury Council)

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Data Protection Impact Assessment

Introduction

The Data Protection Impact Assessment (DPIA) process is an important means of evidencing our compliance with the requirements of Data Protection. This should be used when introducing new or amending existing systems or processes which involve personal data. To support with identifying when a DPIA needs to be completed the DPIA Screening Questionnaire can help indicate when it is needed.

The DPIA will capture:

- How data protection principles are met
- What risks there may be to non-compliance
- What mitigation is in place to address risks identified
- Processes in place to notify any data breaches

Completed DPIAs ensure services document their activity and provide assurance that they comply with our statutory data protection responsibilities.

Our Data Protection Policy sets out the requirement for changes to be reviewed and this process to be followed where the relevant criteria are met, referring to the Data Protection Privacy Impact Assessment (DPIA) Policy and associated guidance.

How to use this DPIA

Each section of the DPIA should be completed to provide a full overview of the proposal, the information being collected and/or processed and how the data protection principles have been considered and demonstrate that these can be upheld.

The supporting DPIA Policy and guidance document has been created to run alongside the DPIA and provide:

- Further guidance and clarification on the information that is required within the DPIA
- Additional information on what should be in place to meet the data protection principles
- Prompt questions that should be considered when completing the DPIA

2. The Proposal

About this Assessment		
Title of Project		
Cameras on top of Peel Tower		
Brief summary and description of the project		
A member of the public approached the Council as he wanted to put something back into the local area of Ramsbottom. He would like to install a camera on top of the flagpole at Peel Tower to stream the view live to the Tourist Information Centre on a screen for everyone to get an idea of and see the view, including disabled people who cannot traverse the steep path to the tower. There is no intention of filming people just the view and as the tower is a Grade 1 listed building a Heritage Statement has been requested to accompany this Impact assessment, please see the attached. As it is being live streamed and the facility to record removed there will be no personal data collected The company who fitted the cameras deliberately took out the recording of the cctv cams and if you try to record it says you are not authorised		
Stakeholders		
Have stakeholders been consulted/contributed to the assessment of the project		☒ Yes ☐ No
Stakeholder (Organisation/Service, Name, Role)	Contact details	Project responsibility (Data controller, Processor, Technical Solution Provider etc)
Parks & Countryside, Mike Bent	m.bent@bury.gov.uk 0161 253 5917	Data controller
Grounds Maintenance Manager, Kevin Dickinson	k.dickinson@bury.gov.uk 0161 253 5905	

Assistant Director Operations Neil Long	n.s.long@bury.gov.uk 0161 253 7928	

3. Information collected

Personal Data			
Type (please tick)		Type (please tick)	
Name	☐	Telephone/contact numbers	☐
Date of Birth/Age	☐	Email address	☐
Gender	☐	Location data	☐
Personal representative / next of kin	☐	Financial information	☐
Physical description	☐	Cultural /Social identifiers or information about family life	☐
Address	☐	Other Unique identifier (please state)	☐
Postcode	☐	Images/CCTV and/or audio recordings	☐
Explain necessity			
Special (Sensitive) Personal Data			
Type (please tick)		Type (please tick)	
Physical or mental health	☐	Religious beliefs or similar	☐
Health/social care	☐	Political opinions	☐
Genetic data	☐	Sexual life/orientation	☐
Biometric Data	☐	Trade union membership	☐
Racial or ethnic group	☐		
Explain necessity			
Crime data			

Type		Type			
	☐		☐		
	☐		☐		
Explain necessity					
Other personal information not included above					
Type		Type			
	☐		☐		
	☐		☐		
Explain necessity					
N/A					
Is any category of data used for law enforcement purposes					
Personal Data			☐ Yes ☒ No		
Special Personal Data			☐ Yes ☒ No		
Crime Data			☐ Yes ☒ No		
Categories of data subject					
Tick the categories of data subject whose personal data will be processed					
Customers	☐	Complainants (and their reps)	☐	Suspected offenders	☐
Suppliers	☐	Advisors/consultants	☐	License/permit holders	☐
Offenders	☐	Benefits recipients	☐	Inspected persons	☐
Claimants	☐	Carers	☐	Captured on CCTV	☐
Students/Pupils	☐	Incident witnesses	☐	Employees of other orgs	☐
Landlords	☐	Employees/contractors	☐	Holders of public office	☐

4. Information flows

This table summarises the type of data, the source of the data, recipient organisations for each distinct data flow, the protective method of exchange and expected frequency. Data flow maps /information architecture diagrams may be added to section 8 to illustrate.

Data flows					
Flow Ref.	Data	From	To Including external parties	Method of transfer	Frequency
01					
02					
03					
04					
05					

5. The Principles

A. Processed lawfully, fairly and in a transparent manner

i. Legal basis for processing

Conditions for Processing			
Tick all relevant conditions which identify a lawful basis for the processing of personal and special category data.			
GDPR Article 6			
All personal data processed for non law enforcement purposes			
6(1)(a)	Consent	☐	Outline any applicable legislation and explain how this supports the processing
6(1)(b)	Contracts	☐	
6(1)(c)	Legal obligation	☐	
6(1)(d)	Vital interests	☐	
6(1)(e)	Public Interest/ Official Authority	☐	
6(1)(f)	Legitimate interests	☐	
GDPR Article 9			
All special category data processed for non law enforcement purposes			
9(2)(a)	Explicit Consent	☐	Outline any applicable legislation and explain how this supports the processing
9(2)(b)	Employment, Social Security, Social Protection law	☐	
9(2)(c)	Vital interests	☐	
9(2)(d)	Not-for-profit body	☐	
9(2)(e)	Made public	☐	
9(2)(f)	Legal claims / Judicial	☐	
9(2)(g)	Public Interest	☐	
9(2)(h)	Medicine, Employee capacity, Medical Diagnosis, Health or Social Care	☐	
9(2)(i)	Public Health	☐	
9(2)(j)	Archiving, Scientific and Historical Research or Statistical Purposes	☐	

DPA 2018 Schedule 1(3)**All special category data as part of criminal offence data processed for non law enforcement purposes**

1(3)(29))	Consent	☐	Outline any applicable legislation and explain how this supports the processing
1(3)(30))	Vital Interests	☐	
1(3)(31))	Processed by not-for-profits	☐	
1(3)(32))	Manifestly made public by data subject	☐	
1(3)(33-34)	Legal Claims or Judicial Acts	☐	
1(3)(35))	Administration of accounts used to commit indecency offences involving children	☐	
1(3)(36))	Substantial Public Interest	☐	

DPA 2018 Part 3(35)**All personal data processed for law enforcement purposes**

3(35)(2) a)	Consent	☐	Outline any applicable legislation and explain how this supports the processing
3(35)(2) b)	Public Interest	☐	

DPA 2018 Part 3(35) and Schedule 8**All special category data processed for law enforcement purposes**

3(35)(4) a)	Consent	☐	Outline any applicable legislation and explain how this supports the processing
8(1)	Statutory purpose (legal obligation or public interest)	☐	
8(2)	Administration of justice	☐	
8(3)	Protecting individuals vital interests	☐	
8(4)	Safeguarding of children and individuals at risk	☐	
8(5)	Personal data already in public domain	☐	
8(6)	Legal claims	☐	

8(7)	Judicial acts	☐	
8(8)	Preventing fraud	☐	
8(9)	Archiving, scientific or historical research, or statistical	☐	

Consent

If consent is being relied upon, confirm that the relevant conditions are in place

Evidence that an individual data subject has consented to the processing	☐ Yes ☐ No
Processes in place to manage the withdrawal of consent	☐ Yes ☐ No
Capability to manage data processed pre- and post- withdrawal of consent	☐ Yes ☐ No
Consent is freely given	☐ Yes ☐ No
For data subjects under 13 years old, parental consent/ authorisation is in place	☐ Yes ☐ No

ii. Rights

Does the processing support an individual's rights

Right to be informed (what privacy notices are in place?)	☒ Yes ☐ No
Right to access	☒ Yes ☐ No
Right to rectification	☒ Yes ☐ No
Right to erasure	☒ Yes ☐ No
Right to restrict processing	☒ Yes ☐ No
Right to data portability	☒ Yes ☐ No
Right to object	☒ Yes ☐ No
Rights relating to automated decision making and profiling	☒ Yes ☐ No

Comments/supplementary evidence

Notices will be installed around the Tower to inform people that there are cameras on top of the flag pole.

iii. Data Subject consultation

Consultation with data subjects	
Has any consultation been undertaken with data subjects over appropriate processing of personal data?	☐ Yes ☒ No
Comments/supplementary evidence	

B. Collected for specified, explicit and legitimate purposes

Legitimate purposes	
Does your project plan cover all of the purposes for processing personal data?	☐ Yes ☐ No
Have potential new/secondary purposes been identified as the scope of the project expands?	☐ Yes ☐ No
Do the purposes include scientific, historical or statistical purposes, or archiving in the public interest?	☐ Yes ☐ No
Purpose	
1	
2	
3	
	(Add additional lines as required)
Comments	

C. Adequate, Relevant and Limited

Minimising personal data	
Is there any personal data that could not be used, without compromising the needs of the project?	☐ Yes ☒ No
Are there any data minimisation techniques being used? (eg, anonymisation, pseudonymisation, redaction)	☐ Yes ☒ No
Comments	

D. Accurate and, where necessary, kept up to date

Accuracy

If you are procuring new software does it allow you to amend data when necessary?	☐ Yes ☐ No
Are there processes in place for ensuring that personal data is accurate and is reviewed where necessary?	☐ Yes ☐ No
Comments	

E. Kept no longer than is necessary

Retention and destruction	
If you are procuring new software does it allow you to delete data when necessary?	☐ Yes ☐ No
Are retention periods suitable for the personal data you will be processing? (Please outline the retention periods below)	☐ Yes ☐ No
Are processes in place to ensure information can be securely deleted/destroyed in relation to both paper and electronic files	☐ Yes ☐ No
Comments	

F. Appropriate Security

i. Organisational Controls

Contractual controls			
Is there a contract in place with any third party for the purpose outlined in section 5B			☐ Yes ☐ No
If yes, does the contract contains the organisation's standard contract schedule relating to Information Governance requirements			☐ Yes ☐ No
Contact term			
Start Date		End Date	
Optional extension period (years):			
Additional processing assurances			
Is a Data Processing Agreement and/or Data Sharing Agreement required to specify the processing involved and appropriate information governance requirements			☐ Yes ☐ No
Comments			

Third party accreditations	
Has evidence of appropriate industry accreditations from third parties been collated	☐ Yes ☐ No
Details	
Training in how to securely process the data	
Confirm that employees (and users where relevant) of the system will receive appropriate training	☐ Yes ☐ No
Confirm that comprehensive written guidance will be available to employees and users	☐ Yes ☐ No
Comments	
Capture issues impacting on Organisational Policy	
Does the proposal impact on any current organisational policy in a way that requires an update to ensure the adequacy of the policy?	☐ Yes ☐ No
Comments	

ii. Technical Controls

Access controls	
Are access controls in place that ensures only those with a valid need to access the data can do so	☐ Yes ☐ No
Is a process in place which assigns and reviews appropriate permissions to view, create, amend and delete data	☐ Yes ☐ No
Process in place to ensure notification of any data breaches by any party involved	☐ Yes ☐ No
Outline the secure method used for controlling access to the information	
Security in transit – when data transferred from one system to another	

Confirm that appropriate security processes is in place to protect the data in transit from threats	☐ Yes ☐ No
Outline how information is transferred securely	
Security at rest - data within a system	
Are appropriate technical security processes is in place to protect the data at rest from threats	☐ Yes ☐ No
Outline how external parties will hold information securely	
Cloud security	
Does the project involve cloud computing	☐ Yes ☐ No
Is the processing compliant with the National Cyber Security (NCSC) Cloud Security Principles	☐ Yes ☐ No
Comments / assessment outcome	

G. Demonstrate Compliance

Records of Processing Activity (ROPA)	
Does the council's ROPA need to be updated to reflect any change resulting from this processing?	☐ Yes ☐ No
Comments	

6. International transfers

Transfer of personal data to third countries	
Personal data will stay within the UK only	☐ Yes ☐ No
Personal data may be transferred within the EEA	☐ Yes ☐ No
Personal data may be transferred outside of the EEA (please detail how secured)	☐ Yes ☐ No
Comments	

--

7. Risk Management

Risk Register							
Risk Ref.	Description of Risk	Probability (1 – 5)	Impact (1 – 5)	Level (High, Med, Low)*	Solution (s)	Impact (eliminated, reduced, or accepted)	Approved by
01							
02							
03							
04							
05							

* The level is calculated by multiplying the probability and impact scores and plotting on the risk matrix, see section 6B of the guidance.

High risk assessment			
Are there any High Level risks that have been accepted			☐ Yes ☐ No
Are there any High Level risks that cannot be significantly reduced following mitigation			☐ Yes ☐ No
In any cases where there are high level risks that cannot be adequately addressed through mitigation then the processing cannot begin until the ICO have been consulted.			
Any DPIA that needs to be referred to the ICO must be reviewed by the DPO prior to being sent to the ICO.			
ICO review			
Date submitted to ICO		Date ICO feedback received	
ICO feedback			

8.Supporting documentation

Please embed relevant documents below.

This section and the documents within will not be routinely published with the DPIA.

Document	Title/Summary
Information Governance (Privacy Notice/ Consent Form)	
[Embed Doc]	
[Embed Doc]	
Project (including Business Case, PIDs, EMT reports etc)	
[Embed Doc]	
[Embed Doc]	
Design (including Specification, High level, Low level, network diagrams, Data flow maps etc)	
[Embed Doc]	
[Embed Doc]	
Procurement (Specification, Contract/ Agreement)	
[Embed Doc]	
[Embed Doc]	

9. Actions

Action plan		
Please outline any residual actions identified as part of the DPIA that are required to be completed as part of the project or business as usual processes.		
Action	Date	Responsible person

10. Approvals

Approved by Senior Responsible Officer / project board		
Name	Role	Date
Reviewed by Data Protection Officer		
Name	Date	
Advice / comments		
Have all recommendations from the Data Protection Officer been implemented	Yes ☐	No ☐
Approved by SIRO (if required)		
Name	Date	

11. Reviews

Regularity of Reviews		
A timetable for reviewing the processing has been identified, taking into account the intended length of the activity and the risk rating		☐ Yes ☐ No
Comments		
Review 1		
Date Review Undertaken		
Processing as initially defined in this assessment remains unchanged	☐ Yes ☐ No	
All mitigations remain in place and are effective and appropriate to the level of risk	☐ Yes ☐ No	
Residual actions have been completed	☐ Yes ☐ No	
No further action is required as a result of the review	☐ Yes ☐ No	
Comments		
Review 2		
Date Review Undertaken		
Processing as initially defined in this assessment remains unchanged	☐ Yes ☐ No	
All mitigations remain in place and are effective and appropriate to the level of risk	☐ Yes ☐ No	
Residual actions have been completed	☐ Yes ☐ No	
No further action is required as a result of the review	☐ Yes ☐ No	
Comments		

(Add additional sections for further reviews)