


Data Protection Impact: Screening and Assessment Form

Decision/Project:	Newham Hall	DPO to add PIA #.
Lead Officer:	Claire Bell	Project Officer
Head of Service (IAO):	Steve Fletcher	Head of Development









Any new decision or project involving high risks to the rights and freedoms of natural persons must have a 'Data Protection Impact Assessment' (DPIA) carried out on it BEFORE any personal data is used or 'processed' – this includes buying new ICT solutions. The Council can be fined up to £9million if it does not complete a DPIA when one was required by law.

- Answer **ALL** of the following screening questions in Step 1 to determine if your decision or project requires a data protection impact assessment (DPIA).
- This is not an exclusive list and DPIAs are required where there is likely to result in 'high risks to the rights and freedoms of natural persons'.
- The Information Commissioner's Office (ICO) recommends that a DPIA is completed where a major project requires the processing of personal data, particularly of vulnerable people.
- If you decide you need to complete a DPIA, fill in steps 2 to 7.
- Hover your mouse cursor over the  images for each question to see further information or examples or go here for [more information about the DPIA process](#).

Step 1: Screening Questions

Section A: Review and answer ALL of the following eight questions. Answering 'Yes' for any will automatically require a DPIA to be completed

1. Systematic and extensive evaluation based on automated processing or profiling resulting in decisions with legal or other significant effects		No
2. Large scale use of special category and/or criminal convictions or offences data		No
3. Systematic monitoring of a publicly accessible area on a large scale		No
4. Decisions about access to a product, service, opportunity or benefit that is based on automated decision-making (including profiling) or involves special category data		No
5. Any profiling of individuals on a large scale		No
6. Combining, comparing or matching personal data obtained from multiple sources		No

Step 1: Screening Questions

7. Targeting of children / other vulnerable individuals for marketing, profiling, or other automated decision-making, or the offer of online services directly to children	?	No
8. Use of data that could jeopardise the physical health or safety of individuals if it were disclosed in a personal data breach	?	No

Section B: Review and answer ALL of the following nine questions. Answering 'Yes' for two or more will automatically require a DPIA to be completed

1. Evaluation or scoring, profiling or predicting , especially aspects about performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements	?	No
2. Automated-decision making with legal or similar significant effect e.g. which could lead to exclusion or discrimination	?	No
3. Observation, monitoring or control of individuals , including data collected through networks or a systematic monitoring of a publicly accessible area	?	No
4. Special category or criminal convictions or offence information use or anything that could increase the possible risk to the rights and freedoms of individuals	?	No
5. Large scale use of any personal data either by number of individuals, volume, duration, or geographical extent	?	No
6. Matching or combining datasets from two or more sources where the original purposes were different	?	No
7. Information about vulnerable individuals including children, adults, employees where there is an imbalance of power with the organisation	?	No
8. Innovative use of or applying new technological or organisational solutions	?	No
9. Preventing individuals from exercising a right or using a service or a contract as a result of use of their information	?	No

Section C: Review and answer ALL of the following five questions. Answering 'Yes' for any in Section C AND one or more in Section B above will automatically require a DPIA to be completed

1. Use of innovative technologies , or the novel application of existing technologies (including AI)	?	No
2. Biometric data use (e.g. fingerprint or facial recognition)	?	No
3. Genetic data use , (other than that processed by an individual GP or health professional for the provision of health care direct to the data subject)	?	No
4. Invisible processing where personal data that has not been obtained direct from the individuals and providing a privacy notice would prove impossible or involve disproportionate effort	?	No
5. Tracking an individual's geolocation or behaviour , including but not limited to the online environment	?	No

Section D: Justification for not completing a DPIA

The project will be delivered in line with the Council's wider Housing Growth Programme with the aim of assisting the Council to set a sustainable budget, as the capital receipts from housing sites along with the subsequent Council Tax are the key components of the Medium Term Financial Plan.

It is believed the project would not require the collection of data that would impact upon the rights and freedoms of natural persons.



Send the form with completed screening questions to:

dataprotection@middlesbrough.gov.uk.

It will then be checked and advice provided on your responses.

If you do not need to complete a DPIA, you do not need to follow the rest of this procedure.

Step 2: Identifying the Need

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 3: Describe the Processing

Nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Describe the Processing

Step 4: Consider consultation

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 5: Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 6: Risk Identification and Assessment

Describe source of risk and nature of potential impact on individuals without any controls in place.	Likelihood of harm	Severity of harm	Overall risk
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Step 8: Sign-off and Outcomes

Consultation responses reviewed by and date:

Click here to enter name.

Click here to enter a date.

Reasons for departing from consultees views:

If your decision departs from individuals' views, you must explain your reasons.

DPO advice provided by and date:

Click here to enter name.

Click here to enter a date.

Summary of DPO advice

DPO should advise on compliance, step 7 measures, and whether processing can proceed.

Advice accepted or rejected, by, and date:

Choose an item.

Click here to enter name.

Click here to enter a date.

Reasons for rejection of DPO advice:

If rejected, you must explain your reasons.

Measures approved / not approved by:

Choose an item.

Click here to enter name.

Click here to enter a date.

Residual risks accepted or rejected by:

Choose an item.

Click here to enter name.

Click here to enter a date.

If accepting any residual high risk, you must ask the DPO to consult the ICO before going ahead.

DPIA to be reviewed by and next review date:

Click here to enter name.

Click here to enter a date.

Previously reviewed by and date:

Click here to enter name.

Click here to enter a date.