**Process**

1. Complete Part 1 DPIA Screening Questionnaire.
2. If the Screening Questionnaire identifies the necessity for a full DPIA, complete Part 2 ‘Full DPIA Template’ (see instructions below):
	1. Complete steps 1-5
	2. Send your draft DPIA to i-west@bathnes.gov.uk
	3. Complete step 6 and retain the final DPIA for reference, along with Part 1 Screening Questionnaire.
	4. Review your DPIA annually (or when risk identified).

**Instructions for completing Part 2 ‘Full DPIA Template’**

The following DPIA template includes a series of steps to follow. At each step there are several questions relating to the processing that you will need to answer.

In some cases, we have provided either a drop-down list or a series of likely answers plus the facility to write your own answers should none in the list fit with your circumstances. In some cases, we have provided a simple text field for you to write your answer.

**Step 5** **‘Identify, Assess and Reduce Risks’** is key to your organisation’s understanding and mitigating risks. ***We have included examples to get you started (Appendix 1) – please do not just copy and paste these risks into the table (unless they apply) They are intended to help you think about the specific risks relating to your own proposed use of personal data.***

Please note that the risk assessment and solution assessment fields are in drop-down lists for you to pick from.

If you have any questions about filling out this form, please consult your DPO:

i-west@bathnes.gov.uk

|  |
| --- |
| **Step 1: Identify the need for a DPIA**  |

|  |
| --- |
| **1.1 Project Details** |
| **Organisation**  | Enter your organisation name |
| **Project name** | Enter project name |
| **Project manager / lead** | Enter details of Project Manager or Lead |
| **Version no.** | **Version date** | **Summary of key changes** |
| 1 |  | First draft |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| * 1. **The need for a DPIA**
 |
| ***You do not need to complete this section as this will be detailed in Part 1 of the Screening Questionnaire.*** |

|  |
| --- |
| **Step 2: Describe the processing**  |

|  |
| --- |
| * 1. **Nature of the processing**
 |
| **2.1.a How will/do you collect, use, store and delete the personal data?** |
|

|  |  |
| --- | --- |
| **How we collect the data** |  |
| **How we use the data** |  |
| **How we store the data** |  |
| **How we delete the data** |  |

 |
| **2.1.b What is the source of the data?**  |
|  |
| **2.1.c Who will you be sharing the data with? (E.g. Local Authority, other public bodies etc.)** |
|  |
| **2.1.d What type of processing have you identified as high risk?** |
| See Part 1 Screening Questionnaire |

|  |
| --- |
| * 1. **Scope of the processing**
 |
| **2.2.a What categories of personal data will be processed? Does it include special category or criminal offence data?** |
|

|  |
| --- |
| Identifiers e.g. *names, username, photo, video footage, recordings, vehicle registration.* |[ ]
| Contact details e.g. *email address, home address, telephone number.*  |[ ]
| Physical characteristics e.g. *height, age, DoB, hair colour, skin tone, tattoos, piercings.*  |[ ]
| Family e.g. *family structure, siblings, offspring, marriages, divorces, relationships.* |[ ]
| Behavioural e.g. *browsing behaviour, call logs, links clicked, demeanour, attitude.* |[ ]
| Professional e.g. *job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary*  |[ ]
| Financial e.g. *credit card number, bank account.* |[ ]
| Device e.g. *IP/Mac address, browser fingerprint, serial number, device license plate* |[ ]
| Racial or ethnic origin |[ ]
| Political opinions |[ ]
| Religious or philosophical beliefs |[ ]
| Trade Union membership |[ ]
| Genetic & biometric Data |[ ]
| Health information (mental or physical health) |[ ]
| Sex life or sexual orientation |[ ]
| Details of criminal offences / convictions |[ ]
| Other: …click to add details. |

 |
| **2.2.b How much personal data will you be collecting and using? How often? How many individuals are affected by the processing?** |
| *For example (i) How many officers/staff/pupils/residents? (ii) What specific data fields will you be processing – e.g. name, address, mobile no, DoB, ethnicity (iii) How frequently will you be collecting it?* |
| **2.2.c How long will you keep the data? How will you ensure it is deleted in line with your retention policy?**  |
|  |

|  |
| --- |
| * 1. **Context of the processing**
 |
| **2.3.a What is the nature of your relationship with the individuals?** |
|  |
| **2.3.b How much control will individuals have over the processing of their data?** |
|  |
| **2.3.c Would individuals expect you to use their data in this way? Are they aware of it?** |
|  |
| **2.3.d Does the processing include children or other vulnerable individuals?** |
|  |
| **2.3.e Are there prior concerns over this type of processing or security flaws?** |
|  |
| **2.3.f Is the processing novel in any way? What is the current state of technology in this area?** |
|  |
| **2.3.g Are there any current issues of public concern that you should factor in?** |
|  |
| **2.3.h Do you have any accreditations relevant to privacy / security? E.g. ISO 27001, Cyber Essentials** |
| *NB: If the provider has security/privacy accreditations then please detail these in 4.2.g (p10)* |

|  |
| --- |
| **2.4 Purposes of the processing** |
| **2.4.a What do you want to achieve?** |
|  |
| **2.4.b What is the intended effect on individuals?** |
|  |
| **2.4.c What are the benefits of the processing – for your organisation and more broadly?** |
|  |

|  |
| --- |
| **Step 3: Consultation** |

|  |
| --- |
| **3.1 Consultation with stakeholders** |
| **3.1.a When and how will you seek individuals’ views? (or justify why it’s not appropriate to do so).** |
|  |
| **3.1.b Who else do you need to involve (or have involved) within your organisation and how will you engage with them?** |
|  |
| **3.1.c Do you need to ask any third party / data processors to assist?** |
|  |
| **3.1.d Do you plan to consult information security experts, or any other experts?** |
|  |

|  |
| --- |
| **Step 4: Compliance, Necessity and Proportionality** |

|  |
| --- |
| * 1. **Lawfulness**

 ***Use drop down lists. The DPO can complete this section if you are unsure*** |
| **4.1.a What is your lawful basis (or bases) for processing?**  |
| The legal basis for processing of personal data (Article 6) is: …choose from drop-down list. *If applicable:* The specific legislation relating to this processing is …provide details of legislation or regulation relating to your organisation’s legal obligation or public interest duties. |
| **4.1.b What is your condition for processing special category data? (select N/A if you are not processing special category data)** |
| The special category data condition for processing (Article 9) is: …choose from drop-down list. *If applicable* The associated condition under the Data Protection Act 2018 Schedule 1 is: Enter DPA 2018 Schedule 1 condition. |
| **4.1.c What is your Article 10 basis for processing criminal offences/convictions? (select N/A if you are not processing criminal offence data)** |
| The Article 10 condition for processing criminal offence data is: …choose from drop-down list. *If applicable* The associated condition under the Data Protection Act 2018 Schedule 1 is: Enter DPA 2018 Schedule 1 condition. |

|  |
| --- |
| * 1. **Fairness, necessity and proportionality**

 |
| **4.2.a Is there another way to achieve the same outcome?** |
|  |
| **4.2.b What information will you give to individuals about the processing of their data?**  |
|  |
| **4.2.c How will you prevent function-creep? i.e. make sure that the personal data being used for this project/process isn’t used for something else.** |
|  |
| **4.2.d How will you ensure that your use of the personal data is adequate, relevant and no more than necessary to achieve your purpose? How will you ensure data minimisation?** |
|  |
| **4.2.e How will you ensure data quality and accuracy? How will it be kept up to date?** |
|  |
| **4.2.f How will you ensure that the data isn’t stored in an identifiable format for longer than necessary?**  |
|  |

|  |
| --- |
| **4.2.g How will you ensure that personal data is protected against unauthorised / unlawful use, accidental loss, damage or destruction?** |
| *What technical and organisational security measures will be put in place to protect the data?* |
| *How will you make staff aware of any security measures or procedures they need to follow?* |
| **4.2.h How will you ensure that individuals can exercise their data protection rights?** |
|  |
| **4.2.i How will you ensure that data processors comply with the requirements of any contracts / data processing agreements?** |
|  |
| **4.2.j How will you safeguard any international transfers? (contact DPO if unsure)** |
| *Where will personal data be hosted? Include routes of transfer if data leaves the UK (for example, while most Microsoft cloud services are based in Europe, the data sometimes goes via America*) |
| *If the personal data leaves the UK, explain which of the formal / recognised adequacy measures are in place (DPO can advise)*: |

|  |
| --- |
| **Step 5: Identify, Assess and Reduce Risks** |

**Please complete the Risk Assessment below with specific risks relating to the processing and how you will mitigate the risks.**

*Consider the practical / day to day risks that apply to your project/processing. E.g. Could personal data be downloaded to a non-secure device? Could sensitive data be inadvertently displayed on a classroom whiteboard? Could data be saved to a memory stick which could be lost?*

*You will find examples of potential risks and solutions in the table shown in* ***Appendix 1****.*

You can add additional rows (‘right click, insert, insert row’) or delete rows (‘right click, delete row’) as needed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Select from dropdown list** | **Solutions** | **Select from dropdown list** |
| **Likelihood of harm**Remote/ Possible/ Probable | **Severity of harm**Minimal/ Significant/ Severe | **Overall risk level**Low, medium or high | **Effect on risk**Eliminated/ Reduced/ Accepted | **Residual risk**Low/ Medium/ High | **Solution approved**Yes/no |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Select from dropdown list** | **Solutions** | **Select from dropdown list** |
| **Likelihood of harm**Remote/ Possible/ Probable | **Severity of harm**Minimal/ Significant/ Severe | **Overall risk level**Low, medium or high | **Effect on risk**Eliminated/ Reduced/ Accepted | **Residual risk**Low/ Medium/ High | **Solution approved**Yes/no |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |
| What is the risk?  | Choose an item. | Choose an item. | Choose an item. | What is the solution? | Choose an item. | Choose an item. | Choose an item. |

|  |
| --- |
| **Step 6: Authorisation / Sign-off** |

|  |
| --- |
| **DPIA authorisation** |
| **Measures approved by:** | Enter name | Enter a date. |
| **Residual risk approved by***If accepting any residual high risk, consult the ICO before going ahead* | Enter name | Enter a date. |
| **Date of consultation with DPO** | Enter a date. |
| **Summary of DPO advice** |  |
| **DPO advice accepted or over-ruled by Project Manager / Sponsor** | DPO advice is: …choose from drop-down list.  |
| **Rationale for over-ruling the DPO’s advice (if applicable)** |  |
| **Date and name of person referring DPIA to ICO (if applicable)** | Enter name | Enter a date. |
| **Summary of ICO advice (if applicable)** |  |
| **Date of updating Record of Processing Activity** | Enter a date. |
| **Date of next review** | Enter a date. |

**Appendix 1 - Example Risks and Solutions**

The table below includes examples of potential risks that might arise and some suggested solutions. This list is not exhaustive, and you should work with key stakeholders to identify specific risks.

|  |  |
| --- | --- |
| ***Example risks*** | ***Example solutions*** |
| *Loss or theft of personal data due to external attack by third party e.g. cyber attack* | *IT Lead/provider will advise on appropriate security including firewalls and password controls.* |
| *Unauthorised access of personal data due to loss of device (laptop, mobile phone etc).* | *Multi factor authentication is in place. All devices are encrypted. Password requirements are in line with NCSC advice. Device can be remotely wiped.*  |
| *Unauthorised use or sharing of personal data by staff (e.g. downloading data onto unsecure memory stick, copying data out of the system and saving it elsewhere).* | *Access rights will be tightly controlled and reviewed regularly by IT. Staff receive annual data protection training and are subject to the Acceptable Use Policy. Memory sticks are not permitted.*  |
| *Data is not backed up and cannot be accurately restored leading to loss of data (data breach).* | *Data is regularly backed up to a separate server.* |
| *Data is inaccurate or out of date leading to unsafe decisions being made (e.g. personal data sent to wrong address).* | *Data is drawn from the main MIS system which is maintained by the Business Support Manager and updated regularly.* |
| *Data which is required to be deleted cannot be securely deleted in line with the organisation’s retention policies.* | *Essential criteria for selecting the new system provider will include technical solution for permanent deletion.* |
| *Processing of personal data is not fair or lawful. Data subjects are not expecting their data to be processed in this way leading to complaints to the ICO.* | *DPO has advised on lawful basis. Communications will be sent to data subjects and Privacy Notice has been updated.*  |
| *Data subjects not able to exercise their rights (e.g. data cannot be extracted for a Subject Access Request or transferred in a machine-readable format).* | *Essential criteria for selecting the new system provider will include technical solution for data extraction in accordance with requirements of UK GDPR.* |
| *Data contained within the system is not limited to that which is necessary and is excessive.* | *Data is drawn from the main MIS system which is maintained by the Business Support Manager and updated regularly. System users are trained on data entry requirements.* |