

Information Assurance Group

**Data Protection Impact Assessment (DPIA) on: Moray Council Learning Estate Engagement**

|  |  |
| --- | --- |
| Link to Product Website | <http://www.moray.gov.uk/moray_standard/page_140530.html> |
| Link to Product Privacy Policy |  |
| Author | Name Jane Martin  Role Community Support Officer  Department Community Support Unit |
|  | Draft Version 0.0 |
| Date | 29 August 2023 |

A DPIA is a tool designed to identify and minimise the data protection risks of a project or process. They are required for any processes that are likely to result in a high risk to individuals and will assist the Council in adopting a ‘privacy by design’ culture. For more information, please see [**Appendix A**](#AppendixA)**.**

To identify whether you need to carry out a DPIA, please complete the question below and the initial screening questions, these will indicate if any further steps in the DPIA are required.

## NOTE for Education/Schools:

Schools and Early Learning Centres should contact [LearnTech@moray.gov.uk](mailto:LearnTech@moray.gov.uk) before starting a DPIA to avoid duplication of work, as another school may have already completed/be in the process of completing a DPIA since more than one school may require access to websites and applications.

# Step 1: Description of the project/resource

Provide a brief description of the project, and, explain the aims and benefits. Where suitable, please link or refer to documents such as a project proposal, host site etc.

If the DPIA relates to a resource, please describe what the resource/system will do, how it will be used and who will require access. Please also describe how the resource will be accessed.

|  |
| --- |
| **A Learning Estate that is flexible and inspirational, that supports excellence and equity for all in Moray, building a better future for our children and young people, providing life-long learning opportunities and providing the foundations for a growing and diverse sustainable economy.”**  **During the course of the project, estimated at 10 to 15 years we will be engaging with key stake holders such as , pupils, staff, parents, and communities** |

## Step 2: Screening Questions

There are two sets of screening questions, they will signpost whether a full, brief or no DPIA is required.

## Set A (directs to Full DPIA)

|  |  |  |
| --- | --- | --- |
| **Does the project involve any of the following?** | **Yes (tick)** | **No (tick)** |
| 1) Evaluation or scoring, profiling and predicting  *- Especially from aspects concerning the data subject’s economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.* |  | √ |
| 2) Automated decision making  *- Any processing of personal data that has zero human involvement. E.g. an online HR recruitment test in which the data subject completes a series of multiple choice questions which automatically determine whether the subject proceeds to the next stage of the recruitment process or not.* |  | √ |
| 3) Systematic monitoring  *- Processing used to observe, monitor or control data subjects. E.g., CCTV in a public area. Includes any monitoring in circumstances where the subject may not be aware that their data is being collected.* |  | √ |
| 4) Data processed on a large scale  *You should consider:*  *A) The number of data subjects involved in the process*  *B) The volume and range of personal data involved*  *C) How long will the processing activity be in place for (e.g. will this affect data subjects on an indefinite basis or over many years?)*  *D) The geographical extent of the processing activity (consider this in combination with other factors – e.g. if Moray-wide is it collecting data from a significant proportion of the people within Moray?)* | √ |  |
| 5) Re-using old dataset(s) for a new, completely different purpose from which it was first intended  *- An example of this would be using a database of unsuccessful applicants for a job as the basis for a mailing list advertising a ‘job club’ or similar employment help scheme. The data subject provided their information in order to apply for the job only: it should only be used and retained for this purpose alone.*  *- However, using information collected as part of the housing benefit assessment to verify eligibility for another entitlement is a reasonable enough expectation and so is not a “completely different purpose”. There is a question in Screening Questions Set B for these types of instances.*  *- Includes combining two data sets previously used for different purposes and/or originating from different controllers* |  | √ |
| 6) Data primarily concerning vulnerable data subjects  *- Note that this is distinct from the earlier question on sensitive data in general. This is concerned with* who *the data subject is about rather than* what *the data is.*  *- This includes any vulnerable groups of people (e.g. the elderly, asylum seekers, patients etc.) and children in general. It also includes areas where the imbalance of power between the Council and the data subject can be seen as greater and thus leave them ‘vulnerable’ by being unable to consent to or oppose the process. For example, it would be difficult for an employee to oppose personal data being processed for HR reasons.* | √ |  |
| 7) Applying novel/innovative technologies  *- E.g. facial recognition software, biometric technology, other novel ways of collecting personal data.*  *- This does not include collecting information through a different medium, such as online rather than by using paper forms.* |  | √ |
| 8) Sharing data outside of the United Kingdom (UK)/European Union(EU)/European Economic Area (EEA)  *- Note that this may include third party services based outside of the UK/EU/EEA. For example, if you are using a system run by a Russian company it is possible that the personal data you enter into the system is held on their Russian-based servers.*  *- This does not include instances where you are sharing a data subject’s own personal data with themselves.* |  | √ |
| 9) When the processing in itself prevents data subjects from exercising a right or using a service or a contract  *- This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is a bank screening its customers against a credit reference database in order to decide whether to offer them a loan or not. Another example would be if the Council banned a service user from a certain building, but also ran a consultation that could only be accessed by visiting that building.* |  | √ |

If the answer to **any** of these questions is “Yes”, a **full DPIA** should be carried out.

If the answer to **none** of these questions is “Yes”, complete Set B

## Set B (directs to Brief DPIA)

|  |  |  |
| --- | --- | --- |
| **Does the project involve any of the following?** | **Yes (tick)** | **No (tick)** |
| 1) Sensitive data  *- This includes data regarding:*  *(a.) Racial or ethnic origin*  *(b.) Political opinions*  *(c.) Religious or philosophical beliefs*  *(d.) Trade union membership*  *(e.) Genetic and/or biometric data for the purpose of uniquely identifying a person*  *(f.) Data concerning a person's health*  *(g.) Data concerning a person's sex life or sexual orientation*  *(h.) Data relating to criminal convictions and offences or related security measures* |  |  |
| 2) A new collection of personal information  *- For example, collecting information about individuals’ locations or for a new ‘opt-in’ process, mailing list or similar.* |  |  |
| 3) Re-using old dataset(s) for a new purpose, but one which is related to the purpose for which the data was first gathered  *- For example, using information collected as part of the housing benefit assessment to verify eligibility for another entitlement* |  |  |
| 4) Using a third-party contractor when processing personal information  *- For example outsourcing HR functions or storing information in the cloud.* |  |  |
| **Note**: Question 5 will not apply if this is a brand new process and no data has as yet been collected  5) A change in the way personal information is stored or secured  *- For example, transferring the storage of personal information into the cloud, or the implementation of a policy that effects a change to the way personal information is stored or secured.* |  |  |
| **Note**: Question 6 will not apply if this is a brand new process and no data has as yet been collected  6) A change to the way that personal data is currently collected.  *- For example, collecting information online rather than on paper forms.* |  |  |

If the answer to any of these questions is “Yes”, a **brief** DPIA should be carried out.

If the answer to none of these questions is “Yes” then send the DPIA form to [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk).

**NOTE:** Schools and Early Learning Centres can check the scenarios table for more information on what is required for different types of products, then email the completed form to both [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk) and [LearnTech@moray.gov.uk](mailto:LearnTech@moray.gov.uk).

# Step 3: Full and Brief DPIA

#### Summarise why you have identified the need for a DPIA; is it for part of a process, a new project, or for a proposed alteration to an existing process?

|  |
| --- |
| The project requires the full Moray wide geographical area, we will be engaging in school associated areas.  We will be engaging with pupils, staff, parent and community. We will be collecting contact information. We will also collect what school they/their children attend. |

#### Describe the flow of information – include where it comes from, who collects it and how, where it’s stored, how it’s used, who manages it at each stage of the process, when and how it’s deleted or archived. A diagram, flow chart or link to relevant websites or documents might be useful here. For a full DPIA this needs to be as thorough as possible.

|  |
| --- |
| The information will come from surveys and comments from the above mentioned stakeholders.  The learning estate team will hold onto the information gathered and share the views but not their personal data with elected members and the community.  Personal data will only be used to contact them directly if they have opted to be kept up to date.  The Learning Estate team will only have access to the personal data. And will be stored securely on sharepoint.  Surveys will be linked on the Council’s corporate Facebook page and added to the Learning Estate engagement [webpage](http://www.moray.gov.uk/moray_standard/page_140530.html) for completion. The Consul platform will be used for the electronic surveys. Consul will link back to the surveys that will be available for completion on the Moray Council website here: <http://www.moray.gov.uk/moray_standard/page_140530.html>  Paper copies of surveys/comments sheets will be provided at in person Community drop in sessions.  All data subjects who complete the surveys/comments sheets in person or online (apart from pupils) will be asked if they would like to provide their name and email address so that they can be contacted by the Learning Estate team and kept up to date about the project. Those who opt to provide their name and email address may be offered to join future strategic working groups/panels that are set up in future. |

#### How are data protection and privacy currently managed in relation to this process or activity? Show where the change that the project involves will fit with the current systems.

|  |
| --- |
| Project originally commenced June 2022, however the first survey for this project is set to launch on 19th September 2023. |

#### Is the project a one-off initiative or part of an ongoing system?

|  |
| --- |
| No it will be ongoing for the next 10 to 15 years |

#### Is the information being processed already collected/held? (Yes/No)

|  |
| --- |
| No |

#### Who are the main stakeholders (Council department(s), Schools, third parties/other organisations involved) and what are their roles in the project?

|  |
| --- |
| Schools including pupils, staff and parents, elected members, community planning partners, community councils and the general public who as an interest in the school estate |

#### Who will be the Asset Owner/person responsible for the data? (e.g. head teacher, head of dept)

|  |
| --- |
| Andrew Hall is the head of service  Robin Paterson – Project Lead  Jane Martin – Community Support Officer  Kirsty McBeath – Comms officer |

#### How many data subjects (individuals) are likely to be affected by the project?

|  |
| --- |
| Lots |

#### Do the data subjects include children (under 12 years old) or any other vulnerable group(s)?

|  |
| --- |
| Yes  No personal data will be collected from pupils, only their views and possibly which school they attend. Their views will be collected via paper surveys/comment forms provided at workshops to be attended by pupils (to be arranged with the Education Service). The paper forms/surveys provided to pupils will not have the option to provide name and email addresses, nor will they contain free text boxes into which personal data could be input. |

#### What timescales are involved; is there a target implementation date?

|  |
| --- |
| Project commenced June 2022 and will be ongoing for 10 to 15 years. |

# STEP 4: Personal Data (Brief and Full DPIA)

#### What personal data will be collected? E.g. names, email addresses, NI numbers, gender, health information, criminal offences etc. Note what is required and what is optional.

|  |
| --- |
| Names , contact information  Names and email addresses will be collected if respondents opt to provide these. Surveys/comment forms can be completed anonymously.  School attended by respondent’s child/children will also be collected. |

#### How will the information be collected/where does the data come from?

|  |
| --- |
| Surveys and in person  Survey Monkey is being used for the surveys, however no personal data will be collected on the Survey Monkey surveys. The [LearningEstate@moray.gov.uk](mailto:LearningEstate@moray.gov.uk) email address will be provided at the end of the survey for those who wish to provide their name and email address.  In person surveys/comments forms will provide the option for name and email address to be added at the end of the paper form. There will not be free text boxes in which additional personal data could be input. |

#### If reused, is the use or collecting method different?

|  |
| --- |
| No |

#### Where will the data be stored and in what format? E.g. Shared drive spreadsheet, national database, paper files in locked cabinet in dept’s office, online website hosted within EU.

|  |
| --- |
| Spreadsheet on SharePoint  Names and email addresses will be stored on a spreadsheet on SharePoint accessible by 5 Learning Estate team members.  Paper surveys/comments sheets will be securely stored in a locked bag at in person workshops/drop-in sessions. The information on these will be added to the Learning Estate shared drive and names and email addresses provided will be added to the spreadsheet on SharePoint as soon as possible after the workshops/drop-in sessions. Paper copies will then be placed into confidential waste receptacles for secure destruction. |

#### What measures are in place to ensure the information is accurate and up to date? Can incorrect information be amended?

|  |
| --- |
| If we contact them we will ask if the information has changed and update accordingly |

#### Who will have access to the information (whether inside or outside the Council)? E.g. NHS, data subjects (inc parents for school pupils)

|  |
| --- |
| Learning Estate team inside the council |

#### Are any other third party processors or sub-processors used to process data at any point? If so, please identify all of these, where they are located and the role they perform in processing personal data.

|  |
| --- |
| No |

#### Does any part of the data leave the Council’s ICT infrastructure?

|  |
| --- |
| No |

#### Does any part of the data leave the UK, European Union (EU) or European Economic Area (EEA)? This includes via a sub-processor or third party.

|  |
| --- |
| No |

#### If a new process how will the data subjects be informed of any changes?

|  |
| --- |
| email |

#### How is the information managed and protected? Any security features? For example encryption of the personal data or pseudonymisation (removing personally identifiable information fields and replacing with pseudonyms)? How is the personal data backed up and can it be restored timeously?

|  |
| --- |
| Don’t know  Paper copy forms/surveys will be stored in a locked bag at in person drop-in sessions/workshops. The information on these will be added to the Learning Estate shared drive and names and email addresses provided will be added to the spreadsheet on SharePoint as soon as possible after the workshops/drop-in sessions. Paper copies will then be placed into confidential waste receptacles for secure destruction.  SharePoint spreadsheet accessible by 5 Learning Estate team members only. |

#### How long will the information be retained and how will it be disposed of or archived? Does it align with the Council’s Retention Schedules (Available [here](http://www.moray.gov.uk/moray_standard/page_92820.html))?

|  |
| --- |
| As long as required |

# STEP 5: Legal Basis (Brief and Full DPIA)

Check how your proposal measures up against the data protection requirements. The questions follow the guidance information:

## Legal Basis

It is unlawful to process personal data without having a valid legal basis.

For personal data that does not relate to any of the special categories the legal basis for the proposed processing must be one or more from the following list.

Please note that ‘data subject’ means the person to whom the personal data relates.

* **6(1)(a)** – Consent of the data subject
* **6(1)(b)** – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
* **6(1)(c)** – Processing is necessary for compliance with a legal obligation
* **6(1)(d)** – Processing is necessary to protect the vital interests of a data subject or another person
* **6(1)(e)** – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
* **6(1)(f )** – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject**.**

In many cases condition 6(1)(e) will be the most relevant.

For personal data that relates to any of the **special categories** the legal basis for the proposed processing must be one or more from the following list:

* **9(2)(a)** – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
* **9(2)(b)** – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
* **9(2)(c)** – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
* **9(2)(d)** – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
* **9(2)(e)** – Processing relates to personal data manifestly made public by the data subject
* **9(2)(f)** – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
* **9(2)(g)** – Processing is necessary for reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards
* **9(2)(h)** – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional
* **9(2)(i)** – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
* **9(2)(j)** – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

The ICO advises that public authorities will find using consent as a legal basis difficult. So if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of the DPO.

‘**Sensitive data**’ includes:

* **special categories** of data as defined in Article 9 i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation.
* personal data relating to criminal convictions or offences;
* data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud).

#### What is the legal basis (see above) for processing the personal data?

|  |
| --- |
| ~~Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller~~  **Article 6(1)(a)** – Consent of the data subject – providing contact details is voluntary. Surveys/comments forms can be completed anonymously. |

#### What is the legal basis for processing any special category data?

|  |
| --- |
| ~~Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,~~  n/a |

#### If you are relying on consent to process personal information, how will this be collected and what provision will be made for people to withdraw their consent? What if consent is withheld or withdrawn?

|  |
| --- |
| Optional to provide information, when contacting we will give the option to withdraw  Privacy Notice to be provided at the point personal data is gathered to explain how their personal data will be used for this process. [LearningEstate@moray.gov.uk](mailto:LearningEstate@moray.gov.uk) email address will be provided for withdrawing consent. Spreadsheet of those who have provided consent to be maintained and updated if/when consent is provided/withdrawn. Consent will be reviewed annually. |

#### How will you tell individuals about the use of their personal information? E.g. privacy notices

|  |
| --- |
| Privacy notice |

#### If you already hold or process this information, is there any significant change being made that data subjects would need to be informed about? How will you inform those affected about the change?

|  |
| --- |
| No |

# STEP 6: Consultation (Full DPIA)

The DPIA should consider and be representative of every aspect of the process. For this reason it is strongly recommended that you consult with any other departments or partners involved in the process when completing the DPIA. This section should be used for reporting who you have consulted with and the discussions, recommendations and other salient points that have arisen. You should first familiarise yourself with all of the steps of the Full DPIA process so you will know which issues require consultation. It is more helpful to think of this not as a single distinct step, but as an ongoing part of the Full DPIA.

#### Who has been consulted and what issues were discussed? Have any assurances, demands or concerns been raised, and if so how have they been resolved?

|  |
| --- |
| No other department |

#### Is there any other pertinent information about what exactly happens to the information during the process? E.g. is the personal information used by a third party with whom we have no direct control or agreement in place?

|  |
| --- |
| No |

# STEP 7: GDPR requirements (FULL DPIA)

### Third Parties:

The Council needs to be able to demonstrate robust arrangements with any third parties who process data on our behalf. This could include software developers, public sector partners (e.g. Scottish Government, NHS), private service providers etc.

#### Will any third parties be processing personal data?

|  |
| --- |
| No |

#### If so is the arrangement set out as part of a contract, data sharing agreement or similar, and, are there pertinent clauses or details regarding data protection?

|  |
| --- |
|  |

#### If the arrangement is not part of a contract, data sharing agreement or similar please specify nature of the current arrangement and state if a new agreement is required.

|  |
| --- |
|  |

### New Technology

#### Does the project involve using new technology that might be perceived as being privacy intrusive? For example, the use of CCTV, Automatic number plate Recognition (ANPR), body worn cameras, biometrics or facial recognition?

|  |
| --- |
| No |

### Public Impact

#### As a local authority we need to be aware of the extent and severity of the impact this project will have on the affected individuals. Will this project have minimal impact on individuals? Will it have some impact on individuals and potentially raise public concerns? Or will it have a high impact on individuals and potentially raise negative media publicity? Are there any current issues of public concern that should be taken into consideration?

|  |
| --- |
| It possibly could have a high impact on individuals and potentially raise negative media publicity |

### Data Subject’s Rights

The data subjects have certain rights relating to the information held on them. These rights can vary, chiefly depending on the legal basis for processing but also on other factors. Not all of these rights will apply all of the time, but you should be prepared to be able to fulfil the main ones.

* Right of access: requires you to respond to Subject Access Requests (i.e. provide a copy of all of the information held on a particular individual). Almost always applies.
* Right to rectification: requires you to update their information upon request. Almost always applies.
* Right to erasure (the ‘right to be forgotten’): requires deletion of personal data held on the subject. Applies when the legal basis is Consent and, in certain cases, Legitimate Interests.
* Right to object: in certain circumstances, requires a halt all processing of their personal data.
* Right to restrict processing: in certain cases, requires that an individual’s data is marked as ‘not to be processed’ and that no action is performed on the marked data.
* Right to data portability: in certain cases, requires that we provide the personal data we hold on an individual in a structured, commonly used and machine readable format. Only applies to entirely automated processes.

#### In the cases where the data subject’s rights apply, will fulfilling any be problematic?

|  |
| --- |
| No problems |

### Data Breaches

All known or suspected data breaches must be investigated and those that are likely to cause any harm or distress must be reported by the DPO to the Information Commissioner’s Office within 72hrs. Guidance on this is available on the intranet [here](http://intranet.moray.gov.uk/Information_management/information_security.htm), nonetheless:

#### If a data breach were to occur how would this be flagged up? Who within the Council would be initially made aware of a known or suspected breach? If external company is being used are there any reassurances, and, what contact details are there?

|  |
| --- |
| DP Officer  Council’s data breach reporting process would need to be followed. Further information on data breaches is available here: <http://interchange.moray.gov.uk/int_standard/Page_132347.html> |

# STEP 8: Risk Assessment (Full DPIA)

This section is for reporting the exact privacy risks and issues that have arisen so far, as well as any others that are pertinent to the project. For each risk there should be a matching recommendation or action for how to mitigate it. Mitigation solutions should be practical and sustainable. Reviewing the project once it is operating will help to identify whether the mitigations are working as planned.

A privacy risk is the risk that a proposal will fail to meet a data subject’s reasonable expectations of privacy - for example, the Council failing to comply with Data Protection legislation, or unreasonably intruding into a data subject’s personal affairs. Consider the direct risks from the proposal as well as any consequential effects.

The following list is of some potential solutions to risks that you may identify. Note that this list is not exhaustive:

* minimise the amount of personal information collected
* better and clearer communication with data subjects
* design the system to provide better security
* provide training and support for staff to help them get it right

The best opportunity to identify risks is during consultation. Workshops with the key people involved in the project, interviews with individuals likely to be affected by the proposal and conducting a joint review of the documents and procedures relating to the project are some of the ways that can identify the risks.

The data protection requirements provide a good framework for asking the right questions, both legal and non-legal, about the impact on the people involved.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Description** | **Likelihood** | **Impact** | **Risk rating (L x I )** | **Mitigation/ Actions** | **Residual Risk** | **Risk Owner** | **Date** |
| ***Example only****:*  *Staff not aware of their obligations when recording personal data.* | *Medium* | *High* | ***High*** | *All staff to undertake GDPR e-learning.*  *Training guides will be provided to all staff involved in the process.* | *Medium* | *Educ.* | *25/5/18* |
| Consent is not actively managed | L | M | **M** | The Learning Estate mailbox is checked daily. A procedure document will be drafted to manage updating the consents spreadsheet with additions/withdrawalsand annual consent reviews. | L | Learning Estates Team | 07/09/23 |
| Paper copies of forms/surveys not securely managed | L | M | **M** | A note to be added to procedure document to cover the process of securing these in a locked bag at in- person events. Timescales for adding the data on these to shared drive and spreadsheet, so hard copies can be securely destroyed to be added to procedure document. | L | Learning Estates Team | 07/09/23 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# STEP 9: DPO Advice and Sign off (Brief and Full DPIA)

Once you have completed this DPIA, please return it to the DPO.

Residual risks accepted by:

|  |  |
| --- | --- |
| Contact/Approver/Manager | Name  Role  Department |
| DPIA Status | Draft/Final Version 0.0 |
| Date | February 2022 |

**If there are any residual high risks, the DPO must consult the ICO before proceeding any further.**

### DPO Advice:

|  |  |  |
| --- | --- | --- |
| Name: | Alison Morris, Information Governance Manager and Data Protection Officer | |
| Date: | 13th September 2023 | |
| Summary of Advice: | Fine to continue with caveats:   * Retention to be discussed and added to the Retention Schedules * Privacy Notice needed covering consent   If anything significant changes then this DPIA should be updated, otherwise this DPIA should be reviewed in 5years’ time. (Note this process is likely to be 10-15yrs) | |
| Advice | **Accepted / Overruled** | If overruled, you must explain your reasons |
| By: | Name of person accepting or overruling | |
| Reason for overruling: |  | |
| Date of next DPIA review: |  | |
| *(Education only)* Link to RAG List Guidance: |  | |

**When completed please save, rename to *DPIA <insert the name of the project/software/process>*  
and email** [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk) **Thank you.**

**Appendix A: DPIA Introduction**

A Data Protection Impact Assessment (DPIA) is designed to consider potential data protection and the privacy impacts of processes and projects; they are a method of recording identified risks, issues and the safeguarding factors introduced to alleviate such concerns or potential impacts. They will assist the Council in adopting “privacy by design” for any new initiatives that involve personal data as well as consider the potential data protection and privacy impacts of our decisions, and, demonstrate that we have done so, as well as comply with data protection legislation.

All new processes or changes to existing processes involving personal data must undergo the initial screening questions, which will indicate whether any further steps in the DPIA are required. Completing a DPIA offers several practical benefits. It can identify problems and opportunities early, which should make it easier and cheaper to address them. It is more efficient to build in good privacy management throughout a project, rather than trying to bolt it on at the end. It will not be possible to identify and eliminate every risk, or identify every opportunity, and a DPIA does not aim to do so. However, it gives a good chance of identifying the most serious and the most likely problems.

This template covers the initial screening questions and two levels of DPIA; a brief and a full DPIA. Data protection legislation requires a full DPIA to be completed to assess proposed measures that pose particular risks relating to how personal data is used. For brief DPIAs only some of the sections are required (Steps 1-5 and 9), whilst all sections are required for a full DPIA.

It is essential that the Data Protection Officer (DPO) has oversight of the scope of the process or project and is able to input as necessary, although the responsibility for completing the DPIA in a timely manner ultimately falls with the department with chief responsibility for the process or project. The DPO signs off DPIAs, however, it is up to departments to implement recommended caveats and mitigations, if departments do not plan to do so they should document this at Step 9 of the DPIA.

A DPIA does not set out to identify and eliminate every possible privacy risk: its role is to identify genuine risks that are not unreasonably small or remote. They should be kept up to date throughout the lifespan of the process or project and reflect any relevant changes; contact the DPO to make these updates. It is recommended to revisit DPIAs on a regular basis.

At any stage advice and guidance is available by emailing [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk). The Council’s DPO is Alison Morris, Records and Heritage Manager.

## NOTE for Education/Schools:

Schools and Early Learning Centres should contact [LearnTech@moray.gov.uk](mailto:LearnTech@moray.gov.uk) before starting a DPIA to avoid duplication of work, as another school may have already completed a DPIA since more than one school may require access to websites and applications.

**When completed please save, rename to *DPIA <insert the name of the project/software/process>*  
and email** [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk). **Thank you.**

# Definitions

**Data subject** – A living individual to whom personal data relates.

**Data controller** – A body that determines the purposes for and manner in which personal data is used. This includes employees of the data controller. The Council is considered to be the data controller for most of its activities that involve personal data.

**Data processor** – A third-party body who processes information on behalf of the data controller. This only applies to third-parties with who a formal contract is in place. In most cases you will be a controller who processes their own data rather than purely a processor, unless a third party has provided you with personal data and there is a legal contract with them that specifies what you are required to do with this data.

**Personal data** - Any information relating to a data subject, particularly information that can be used to identify them. This ranges from name, age, address and other contact details to health records, HR records, IP addresses and opinions about the individual.

**Process/data process/processing** – Relates to any activity you perform on or uses personal data. This includes storing and gathering the data.

**Data Protection Officer (DPO) –** Moray Council’s designated individual, who is responsible for signing off the outcomes of the DPIA process, is the Records and Heritage Manager, [dataprotection@moray.gov.uk](mailto:dataprotection@moray.gov.uk).

**Data Protection Legislation** primarily includes: Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR).