**Researchers’ rapid assessment Privacy Impact Assessment screening and Data Protection Compliance checklist**

**Please note that this must be a self-explanatory ‘stand-alone’ document and include all the information/explanations necessary in the event that it needs to be provided to the UK Information Commissioner (ICO) if there is a Data Breach or Incident (or other Audit). Please include information as necessary from other documents e.g. project proposals, data management plans, etc. (you can cut and paste into this document as/if necessary)  
Whilst Governance colleagues provide advice to assist you with Data Protection legislation compliance, the responsibility for the processing actually complying with Data Protection legislation lies with the responsible manager e.g. Principle Investigator, Lead Researcher, Budget Holder, etc. (as appropriate).   
If, after completing this PIA, there are residual high risks which cannot be adequately mitigated then we are required to consult the ICO.**

**This assessment should be sent to** [**dataprotection@napier.ac.uk**](mailto:dataprotection@napier.ac.uk) **for review.**

**Information**

A Privacy Impact Assessment (PIA) is a systematic assessment of a project, processing activity or change initiative that identifies the risks that the project/processing might have on the privacy of the individuals whose data is being processed, and enables colleagues to put measures in place for managing, minimising or eliminating that impact.

A proactive approach should be taken and ideally the PIA should be started early in the project life-cycle to enable privacy risks to be mitigated early and reduce costly mistakes and changes later on - this principle is called "Privacy by Design" (Article 25), however a PIA can be conducted at any time.

The legislation requires organisations to keep records to "demonstrate compliance" (accountability principle) and a PIA is one way of doing this e.g. in the event of an audit or breach, the PIA can provide evidence that the risks have been considered and measures taken to mitigate any risks identified."

"The legislation (Article 35 paraphrased) says:

The assessment shall contain:

(a) A systematic description of the processing operations and the purposes of the processing, including the legal basis/es

(b) An assessment of the necessity and proportionality of the processing operations in relation to the purposes

(c) An assessment of the risks to the rights and freedoms of data subjects whose data is being processed (e.g. likelihood and impact of a data breach – all scenarios to be considered)

(d) The measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data"

Please do your best to complete this as fully as possible - this reduces delays and multiple checks/unnecessary work for both yourself and other teams involved in checking the process/project complies with legislation.

Definition of personal data: “any information relating to an identified or identifiable living individual, who can be identified directly or indirectly” e.g. can be identified from that data and other available information, and includes any expression of opinion about the individual.

The processing of personal data for research includes participant recruitment (collection and use of names and contact details in order to contact participants to disseminate surveys, arrange interviews, use other research data collection instruments), the collection of data, the anonymisation of personal data, the storage of personal data after anonymisation (anonymised data may be used for analysis, but the underlying personal data is still being securely stored) and secure/thorough deletion.

If personal data is being retained for potential re-use in future this must be highlighted in this document.

The ICO Anonymisation Code of Practice can be found here: <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>

**Name of Research Project:**

**Name of Principal Investigator:**

**Lead Institution:**

**Name of colleague completing this form:**

**Date of completion of PIA:**

1. What is the purpose of the processing and aims of the project (if there are multiple purposes please include them all)?

Answer:

1. Please provide a full description of what the processing entails or will entail. This needs to be self-explanatory and give a full description of why the processing is necessary and exactly what happens during the procedure from collection to disposal, as this may be required as evidence for the ICO (regulator). If you have a process flow diagram please provide that too?

Answer:

1. Please detail any benefits that the project aims to achieve (to parties/ individuals)?

Answer:

1. Stakeholders. Please provide a list of stakeholders who are involved in or will be affected by the processing/project - internal, external, groups, etc.

Answer

1. How are you recruiting participants?

Answer

1. Please list the categories of data subjects from whom you will be collecting personal data e.g. students, staff, individuals who fit within a specific set of parameters (please detail what these are), etc.:

Answer:

1. Please list all personal data being collected (categories or fields). Note: personal data is data about a living individual from which they may be identified, including when used in combination with other information. This includes comments and opinions.

Answer:

1. How many participants’ are you intending to collect personal data from?

Answer:

|  |  |
| --- | --- |
| **Governance can assist with completing this risk** | |
| **Description the source of the risk and nature of the potential impact to the individual(s).** | **Mitigating measures to ensure privacy and confidentiality rights are maintained?** |
| **Likelihood of harm to individuals (delete as appropriate):** | Remote / Possible but unlikely / Probably (reasonable change that will happen) |
| **Severity of harm (delete as appropriate):** | Minimal, significant or severe |
| **Residual risk (delete as appropriate):** | GREEN – AMBER – RED |

1. **Proportionality test**
   1. Describe how this proposal/processing is necessary and proportionate to achieve the purposes, considering the benefits and risks:
   2. Is there any other reasonable way to achieve the same result which is less intrusive?
   3. How will you prevent “function creep” or the personal data being used for additional purposes?
2. **Consultation**
   1. Have you consulted any data subject, representative groups or other stakeholders about this processing as part of assessing the proportionality of the processing?
   2. Describe any relevant consultation that has taken place for this proposal.

|  |  |
| --- | --- |
| **Governance can assist with completing this risk** | |
| **Description the source of the risk and nature of the potential impact to the individual(s).** | **Mitigating measures to ensure privacy and confidentiality rights are maintained?** |
| **Likelihood of harm to individuals (delete as appropriate):** | Remote / Possible but unlikely / Probably (reasonable change that will happen) |
| **Severity of harm (delete as appropriate):** | Minimal, significant or severe |
| **Residual risk (delete as appropriate):** | GREEN – AMBER – RED |

1. **Compliance checklist**

*Guidance for completing the compliance checklist below:*

*All statements in the second column must have a corresponding Y, N or N/A in the third column. Y = Yes, I agree that the statement (in the 2nd column) is correct in relation to my research project, and N = No, the statement is not correct in relation to my research project. N/A = Statement is not applicable to the project/study.*

*Please provide comments/further details on the 4th column for all questions.*

|  |  |  |  |
| --- | --- | --- | --- |
| # | Requirements of the legislation | Y, N or N/A | Comment |
| **A** | **Consider if the project is covered by the provisions of the legislation with regard to processing for archiving purposes in the public interest, scientific or historical research purposes.** | | |
| i | This information is being used *exclusively* for research purposes. |  | Details: |
| ii | The information is not to support measures or decisions relating to any identifiable living individual. |  | Details: |
| iii | The data is not being used in a way that will cause, or is likely to cause, damage or distress to any data subject or result in a risk to their rights and freedoms, including in the event of a data or security breach. |  | Details: |
| iv | The result/s of the research, or any resulting statistics, will not be available / published in any form that identifies the research participants. |  | Details: |
| v | The project is not undertaking the large scale processing of special category data or criminal convictions/offences. |  | Details: |
| vi | The project is not undertaking systematic monitoring of publicly available personal data. |  | Details: |
| vii | The project is not undertaking the use of innovative new technologies (e.g. Artificial Intelligence) for processing personal data. |  | Details: |
| viii | The project is not undertaking “Data Matching” e.g. combining, comparing or matching personal data obtained from multiple sources. |  | Details: |
| ix | The project is not undertaking “Tracking” e.g. processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment. |  | Details: |
| x | The project is not undertaking processing which is of such a nature that a personal data breach could jeopardise the health or safety of individuals e.g. risk of physical harm. |  | Details: |
| **Governance** comments on unmitigated risks in this section (table below to be replicated in each section below as necessary). | | | |
|  | |  |  | | --- | --- | | **Description the source of the risk and nature of the potential impact to the individual(s).** | **Mitigating measures to ensure privacy and confidentiality rights are maintained?** | | **Likelihood of harm to individuals (delete as appropriate):** | Remote / Possible but unlikely / Probably (reasonable change that will happen) | | **Severity of harm (delete as appropriate):** | Minimal, significant or severe | | **Residual risk (delete as appropriate):** | GREEN – AMBER – RED | | | |
| **B** | **Principle 1 – Lawfulness, fairness and transparency**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | (Lawfulness) The legal basis for processing is Art 6(1)(e), performance of a task in the public interest/exercise of official duty vested in the Controller by Statutory Instrument No. 557 (S76) of 1993 as amended, e.g. for education and research purposes. |  | Please provide your comments here if you have any concerns about the suitability of this legal basis:  *Note: If you do not adhere to the University’s guidance and requirements for the collection, storage and processing of personal data you will be considered the Data Controller and must follow a different process – contact Governance Services.* |
| ii | (Lawfulness) Where special category (sensitive) personal data is being processed the additional bases from Article 9 is:  Art 9(2)(j) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.  Special category personal data includes: health data, biometric, genetic, racial or ethnic origins, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. |  | Details:  *To be completed, if applicable:*  *Use of this basis must be accompanied by explanations of:*   1. *How the use of data is proportionate to the aim pursued* 2. *What suitable and specific measures are in place to safeguard the fundamental rights and interests of the participants* |
| iii | (Lawfulness) You have put additional safeguards in place where processing the personal data of children and vulnerable persons. |  | Detail the additional safeguards here, if applicable: |
| iv | (Transparency – telling individuals how their data will be processed) You have made provision for providing privacy notices e.g. in/with participant information sheets, in public places, etc. as appropriate. |  | Details:  *Note: The University* [*Privacy Notice*](#PrivacyNotice) *template provided below must be used and provided to participants on their Informed Consent Form. If it is impossible or would require disproportionate effort to provide a privacy notice you must take guidance the Research Office or Governance Services and provide details relating to the decision not to provide a privacy notice here:* |
| v | (Fairness) Are you processing or re-using personal data for purposes that data subjects / participants involved reasonably expect? |  | Details: |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **C** | **Principle 2 – Purpose limitation. Collected for specified, explicit and legitimate purposes**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | You have set out all the purposes for processing in the [Privacy Notice](#PrivacyNotice) (template below). |  | The purposes are detailed in 1 above, please provide any additional information here: |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **D** | **Principle 3 – Data minimisation. Personal data collected must be adequate, relevant and limited to only that which is necessary to fulfil the purposes for which the data was collected.**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | You have designed your project to only collect the personal data absolutely necessary to meet the aims and objectives of the project (the minimum necessary) |  | Details:  *Note: Do not collect or keep personal data which is not necessary for your research.* |
| ii | Pseudonymisation/ codification or anonymization will be used at the earliest opportunity to ensure this Principle is complied with. |  | Please detail at what stage of processing this will take place and what method will be used. Please see the [ICO’s Anonymisation Code of Practice](https://ico.org.uk/media/1061/anonymisation-code.pdf) |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **E** | **Principle 4 – Accuracy**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | You will take reasonable measures to ensure that the data you collect is accurate. |  | Detail how you will achieve accuracy and good data quality here: |
| ii | Where appropriate and necessary you will put measures in place to keep the data up-to-date. |  | Detail the measures here: |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **F** | **Principle 5 – Storage limitation**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | You have agreed retention periods for the data with the principle Investigator, RIE or Governance Services and have included this information in your data management plan and privacy notice |  | Detail the retention periods here:  Any additional comments: |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **G** | **Principle 6 – Integrity and confidentiality**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
|  | You have appropriate organisational and technical measures in place, including assessing the security of your work environment and the electronic and manual systems you use, to protect and secure personal data during: | | |
| i | Collection (method and format e.g. equipment and software systems, etc. used) |  | Please detail the assessment done and the measures in place here: |
| ii | Storage |  | Detail the assessment/measures here: |
| iii | Sharing/transfer |  | Detail the assessment/measures here: |
| iv | Use and re-use |  | Detail the assessment/measures here: |
| v | Deletion/Archiving |  | Detail the assessment/measures here: |
| vi | You are only using electronic/computer systems and services provided and approved by the University’s Information Services team. |  | Detail the system/s here:  Note: it is recommended that IS approved systems are used wherever possible. Systems not provided by IS will require additional security and contractual checks. |
| vii | Are you sharing any personal data with 3rd parties external to the University? |  | Detail the parties and what they are doing with the personal data, including any partner organisations, electronic/ computer/ online system or app providers. |
| viii | If the answer to G)vii above is Y, do you have data sharing/processing agreements in place |  |  |
| ix | If the answer to G)vii above is Y, have security checks been completed to ensure those 3rd party/ies comply with Principle 6 |  |  |
| Governance and Information Services comments on unmitigated risks in this section | | | |
|  |  | | |
| **H** | **Principle 7 – Demonstrating compliance**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this Data Protection Principle.* | | |
| i | You have records documenting the decisions taken with regards to the processing of personal data which may include a data management plan, data collection form, privacy notice, etc. |  | Please provide a list of records:  Full completion of this document will cover this requirement. |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **J** | **Personal data not to be transferred to 3rd countries/ territory (outwith the UK and not on the ICO’s ‘**[**adequate**](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)**’ list) without appropriate and adequate protection – GDPR Chapter V refers**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this chapter of the legislation.* | | |
| i | You are transferring personal data to a third country or territory outwith the UK and not on the ‘adequate’ list. |  | Detail which country the data will be transferred to: |
| ii | If the answer to J i above is Y - you have a contract or data sharing agreement in place with the recipient of the data which ensures appropriate safeguards are in place and enforceable data subject rights and effective legal remedies for data subjects are available |  |  |
| iii | You have completely anonymised the data |  |  |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **K** | **Data subjects are able to exercise their rights**  *The information you provide in this section relates to measures to mitigate against the* ***risk*** *of breaching this chapter of the legislation.* | | |
|  | You have made arrangements to comply with the individuals’ rights – in particular: | | |
| i | You have provided privacy notices to provide individuals with details of the processing (Articles 12-14 – right to receive information) |  | Detail the measures here:  Note: those marked \* are subject to derogations and may not apply if exercising those rights impairs the research. To be confirmed |
| ii | You will be able to provide an individual with a copy of their personal data being processed, if requested (Article 15 – [subject access](https://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/accesspersonalinformation.aspx))\*. |  |
| iii | You will rectify, erase, restrict or stop processing of, or destroy data securely, if necessary (Articles 16, 17 & 19, 18 & 19, 21 – Rectification\*, Erasure\*, Restrict processing\* and Object to\*/stop processing respectively). |  |
| iv | You will be able to provide a copy of personal data provided to you, in a machine readable format, if required and provided for by the legal basis for processing (Article 20 – Portability). |  |
| v | You will ensure that no decision which significantly affects an individual is based solely on automated processing or profiling of their data (Articles 4(4) & 22 – Restrict automated decision making with significant effects). |  |
| vi | You will stop using data if it is likely to cause unwarranted substantial damage or distress to any data subject or result in a risk to their rights and freedoms. |  | Detail how this will be done: |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |
| **L** | **Breach notification**  *Not reporting a breach can result in fines of up to £9M* | | |
| i | You will immediately report any personal data breach or other breach of the legislation to the Principal Investigator and they will follow University procedures (and report to Governance Services and/or Information Services, as appropriate).  Definition: ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |  | See section [7.10 online](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/SecurityofPersonalData03.aspx) for the Breach Procedure. |
| Governance comments on unmitigated risks in this section | | | |
|  |  | | |

**Privacy Notice (template)** (to be appended to the Participant Information and Informed Consent Forms)

Name of Research Project:

Description of Project:

|  |  |
| --- | --- |
| Data Controller | Edinburgh Napier University |
| Purposes for collection/processing | Provide a description of the purposes e.g. the aims of the project, or refer to appropriate section in ethics form.  If there is the intention to process for a further purpose, other than that noted above, please provide this information here. |
| Legal basis | Art 6(1)(e), performance of a task in the public interest/exercise of official duty vested in the Controller by Statutory Instrument No. 557 (S76) of 1993 as amended, e.g. for education and research purposes.  Where sensitive personal data is being processed the additional bases from Article 9 is:  Art 9(2)(j) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.  *Use of this basis must be accompanied by explanations of:*   1. *How the use of data is proportionate to the aim pursued* 2. *What suitable and specific measures are in place to safeguard the fundamental rights and interests of the participants* |
| Whose information is being collected | [Student, employee, alumni, etc.] |
| What type/classes/fields of information are collected | [Name, identifying numbers, contact details, sensitive personal data, educational details, financial information, vetting data, etc.] |
| Who is the information being collected from | [From the data subject (directly), named third party, survey distribution company, etc.] |
| Is personal data shared with internal and external to the University | [Data processors, joint controllers, software provider, etc.] *If so a Data Sharing or Processing Agreement must be in place with the required security checks.* |
| How long is the information kept for | [there may be shorter retention periods for voice/image recordings than extracts of transcriptions]  *Undergraduate students will normally keep personal data no longer than the end of the examination/ assessment/ appeals process e.g. once the research has been given a final mark.*  *Postgraduate MSc students may follow the same retention periods as UG students, but depending on the study there may be occasions where it will be longer – your supervisor can advise.*  *Postgraduate PhD students may have longer retention periods depending on the nature of the study, but, if the research data is being kept for 10 years this does not include personal data which is stored for a much shorter period – please discuss with your supervisor.* |
| Will the data be used for any automated decision making |  |
| Is information transferred to a third country? Outside the UK and not included in the adequate countries list. |  |
| You can access all the University’s privacy notices using the following link: <https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/statement.aspx>  You have a number of rights available to you with regards to what personal data of yours is held by the University and how it is processed – to find out more about your rights, how to make a request and who to contact if you have any further queries about Data Protection please see the information online using the following URL: <https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx> | |