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

**Introduction**

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). Further guidance is available online here: [Research, Processing Data for (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx)

While 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) and they therefore must be party to the completion of this document, if not completing it themselves.

If, after completing this compliance check, there are residual high risks which cannot be adequately mitigated then we are required to complete a PIA and potentially consult the ICO.

**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.** Please do not include or cut and paste information which isn’t relevant to the questions.

Guidance and examples are in blue text.

Please provide your answers in the text or drop down boxes provided.

**Background**

i) Compliance check pre-Privacy Impact Assessment

This compliance check is to ascertain if a Privacy Impact Assessment (PIA) is required (Article 25 “Privacy by Design” refers). A PIA is 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 personal data is being processed, and enables colleagues to put measures in place for managing, minimising or eliminating that impact.

**Name of researcher:** Click or tap here to enter text.

**Name of research project:** Click or tap here to enter text.

**Name/s of collaborating institutions or partner organisations:** Click or tap here to enter text.

**For Staff Researchers:**

**Have you completed the University’s Data Protection training for this year?** Choose an item.

If not, here’s the link:[Login](https://web3.workwize.com/logins/companyLogin/5386)

**For Student Researchers:**

**Have you completed the Research Student Oath of Confidentiality and discussed the protection of participant personal data with your Research Supervisor/s?** Choose an item.

If you haven’t completed the Oath of Confidentiality, here’s the link: :[Research, Processing Data for (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx)

**Student Researcher Supervisor Name:** Click or tap here to enter text.

Governance Services provided additional data protection training for researchers – details here:  [https://staff.napier.ac.uk/learningevents/Pages/Default.aspx?SearchFilter=D](%20https://staff.napier.ac.uk/learningevents/Pages/Default.aspx?SearchFilter=D%20)

**Section 1 - Processing Activity**

|  |  |
| --- | --- |
| Data Controller | Edinburgh Napier University |
| Purposes for collection/processing | Provide a description of the purposes e.g. the aims of the project (you can cut and paste from project applications, ethics forms , DMP etc., but it must explain the purposes fully).  Click or tap here to enter text. |
| Whose information is being collected | e.g. student, employee, alumni, patients, participants with specific conditions or characteristics, employees of specific organisation/s, etc.  Click or tap here to enter text. |
| Guidance on Personal Data:   1. Personal data is defined as: “any information relating to an identified or identifiable living individual, who can be identified directly or indirectly from it” e.g. relating to anyone who can be identified from that data together with any other available information (e.g. information available online). This includes expressions of opinion about an individual, irrespective of whether the opinion is true. 2. This PIA screening is primarily interested in personal data from which individuals can be identified, NOT anonymised research data from which individuals cannot be identified. 3. For categories of information please see: [Research, Processing Data for (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx) | |
| What type/classes/fields of information are collected  If you are using online collection methods you are likely to be collecting IP Addresses and must include this option here and also provide the statement about IP addresses / online identifiers to participants in your Privacy Notice.  If it is possible that participants may provide their or others’ personal data, which you have not specifically asked for, in the research instruments e.g. questionnaire / survey free text fields or interview responses, please advise them not to do this. | Please consider all stages of processing, e.g.  -recruitment  -research consent collection  -collection via qualitative and quantitative research instruments.  Please tick any of the following categories which are applicable (please note the categories contain a number of options, but you should only collect those personal data fields that are absolutely necessary for your research, not additional fields just because they are included in the same category/ies):  Personal details, including any information that identiﬁes the data subject and their personal characteristics, including: **name, address, contact details**, age (age range is preferred for research), date of birth, gender, and physical description.  Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details.  Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject’s lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations.  Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualiﬁcations, skills, training records, professional expertise, student and pupil records.  Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records.  Financial details, including information relating to the ﬁnancial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, beneﬁts, grants, insurance details, and pension information.    Where online systems are used, servers are likely to collect IP addresses, however these will not be used for the purposes of research, but may be used to ensure ethical integrity.  Indirect data which is linked in such a way that individuals could be identified e,g, spreadsheet containing pseudonymised data with multiple linked fields for each individual.    Other, please detail below:  Click or tap here to enter text.  Special category (sensitive) personal data concerns, reveals or is about:  racial or ethnic origin  health (mental or physical)  religious or philosophical beliefs  political opinions  genetic data  biometric data (if used to identify a natural person)  religious or philosophical beliefs  sex life or sexual orientation  criminal convictions and offences  none of the above |
| Legal Basis  (The black text in the column to the right must be included in your Privacy Notice) | 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 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  Proportionality and safeguards information for special category data:   1. We only use the minimum data necessary to enable us to meet the research aims and objectives 2. In order to ensure that suitable and specific measures are in place to safeguard the fundamental rights and interests of the participants the project has been through the University’s Research Governance processes which include data protection compliance checks   If you have any additional information about how you are minimising data or putting additional safeguards in place to protect special category personal data, please detail these below:  Click or tap here to enter text.  Please note that we are not relying on consent as a basis for processing under the GDPR, and our legal basis for processing is therefore distinct from the research ethics-related use of consent in this study. |
| How many participants are you collecting information from? | Click or tap here to enter text. |
| “Processing” includes the collection of data, transfer of data, the process of anonymising this personal data, any storage of original personal data after anonymisation has taken place (e.g. where anonymised data is used for analysis, but the underlying personal data is still being securely stored), and the process of secure/thorough deletion itself. Thus, if personal data is being retained for potential re-use in future, this must be highlighted within this document. | |
| How are you recruiting participants? Please describe the process giving as much detail as you can e.g. advertising online, via social media, posters, etc. or by referral, word-of-mouth, etc. How are they finding out about your research and getting information about it before they volunteer to participate? | Please tick any that are applicable and provide detail for those that are applicable:  Self-selection via adverts Click or tap here to enter text.  Gatekeepers Click or tap here to enter text.  Snowballing Click or tap here to enter text.  Directly contacting individuals using publicly available personal data – see guidance here: [Research, Processing Data for (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx). Please describe what you are doing in detail:  Click or tap here to enter text.  Directly contacting individuals using personal data provided by a third party e.g. survey company. Please describe what you are doing in detail:  Click or tap here to enter text.  Re-using personal data that is already held by the University. Please describe where the personal data is held and who has given permission for its use:  Click or tap here to enter text.  Other method – please describe what you are doing in detail:  Click or tap here to enter text. |
| How is the personal data being collected / processed?  Consent collection guidance:  Email is not secure, please consider collecting consent via a University provided survey tool (e.g. NOVI Survey). You can use the survey tool to provide participant information, the privacy notice, consent form and, in some cases, the research survey and debrief. | Please provide a description of the process in as much detail as possible, including all/any formats/systems being used e.g. collected in person by the researcher, online form, paper form, recorded interview, survey tool, etc.   1. How is participant personal data being collected during the recruitment phase of the project? Please give a full description detailing how you are collecting participant names, etc., the method of collection and how the personal data is **securely** transferred / provided to the University. Please list all systems you are using for this.               Click or tap here to enter text.   1. Please give a full description detailing how are you collecting **research consent** and all systems being used for this? (Please consider using a University provided survey tool for the collection of consent. Further info in column to left):               Click or tap here to enter text.   1. Please give a full description of how you are collecting personal data for the **qualitative/ quantitative research instruments** (surveys, interviews, etc.) and all systems you are using e.g. Novi Survey, MS Forms, MS Teams, etc?             Click or tap here to enter text.          Click or tap here to enter text.    Click or tap here to enter text.          Click or tap here to enter text.    Click or tap here to enter text.    Click or tap here to enter text. |
| Are you doing anything specifically to safeguard the rights and freedoms of your participants with regards to their personal data? | Click or tap here to enter text. |

**Section 2 – Screening Questions**

|  |  |  |
| --- | --- | --- |
| **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 | Are you using the personal data *exclusively* for research purposes? | Click or tap here to enter text. |
| ii | Are you using the personal data to support measures relating to, or make decisions about, any identifiable living individual?  If so, do the purposes for which the processing is necessary include the purposes of approved medical research e.g. approved by a relevant Health Authority as allowed by the UK GDPR? | Click or tap here to enter text. |
| iii | Are you using personal data 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 e.g. if their data was made available (accidentally, unlawfully, in the outcomes or otherwise) to other people? | Click or tap here to enter text. |
| iv | Will the result/s of the research, or any resulting statistics, be available, disclosed or published in any form that identifies the research participants?  You must comply with the [ICO’s Code of Practice on Anonymisation](https://ico.org.uk/media/1061/anonymisation-code.pdf). | Click or tap here to enter text. |

**Section 3 – Initial Risk Assessment (for IG Team to complete)**

|  |  |  |
| --- | --- | --- |
|  | **Rating** | **Comments** |
| Number of participants | Choose an item. |  |
| Categories of personal data | Choose an item. |  |
| Research topic | Choose an item. |  |
| Quantity of different personal data fields collected | Choose an item. |  |
| Method of participant recruitment | Choose an item. |  |
| Method of processing | Choose an item. |  |
| **Overall rating** | Choose an item. |  |

**Section 4 - Researchers’ checklist for compliance with data protection legislation**

*Guidance for completing the checklist:*

*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 where required.*

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | **Principle 1 – Lawfulness, fairness and transparency** | | |
| i | *Legal basis/es included in ROPA above* | | |
| ii | You have put additional safeguards in place where processing the personal data of children and vulnerable persons  See the ICO guidance online here: [Children | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/children/) | Choose an item. | Detail the additional safeguards here, if applicable:  Click or tap here to enter text. |
| iii | You have made provision for providing privacy notices e.g. in/with participant information sheets, in public places, publicly online, etc. as appropriate  Please note that we can apply an exemption if it is impossible or would require disproportionate effort to provide a privacy notice, but you must provide the details at the bottom of the detail section in the third column>> | Choose an item. | Note: The following information must be provided to participants with the Participant Information Sheet & Informed Consent Form: 1) Data Controller’s details  2) Legal Basis/es (as provided above)  3) Categories of recipients internally and externally (who personal data is shared with)  4) If personal data is transferred outside the UK  5) How long data will be retained or the rationale for retaining data  6) If any automated decision making or profiling is taking place  7) The following link: staff.napier.ac.uk/dpstatements for further information about processing and rights    If it is impossible or would require disproportionate effort to provide a privacy notice you should take guidance from your Programme Leader, Supervisor or the Research Office before giving the reasoning for the decision not to provide a privacy notice here:  Click or tap here to enter text. |
| **B** | **Principle 2 – Purpose limitation. Collected for specified, explicit and legitimate purposes** | | |
|  | Note for Governance: Included in screening questions above | | |
| **C** | **Principle 3 – Data minimisation and proportionality. 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.**  🛈 Do not collect or keep personal data which is not absolutely necessary for your research.  🛈 Basic (non-system applied) pseudonymisation (also known as codification, key coding or de-identification) typically will be a password encrypted database or spreadsheet in which participants are assigned a pseudonym (name or number) which is recorded against their real name, contact details, other personal data/ direct identifiers, special category data. The encrypted database is kept separate from other research data.The pseudonym is then used when data collection takes place using the research “instruments”. | | |
| 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)? | Choose an item. | Click or tap here to enter text. |
| Ii | Are you pseudonymising / codifying / key coding the personal data you collect? | Choose an item. | 1) *How* are you pseudonymising personal data? Basic pseudonymisation can be done using a password protected spreadsheet where participants are assigned a “pseudonym” e.g. participant number (or name). Basic pseudonymisation guidance online [here](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Documents/Research/Basic_Pseudonymisation_Guidance.pdf).  Click or tap here to enter text.  2) *When* are you starting the pseudonymisation process?  This should start as early in the processing as possible e.g. as you are collecting personal data during the recruitment phase, before data collection for the research qualitative and quantitative instruments. Pseudonymisation is an ongoing process during recruitment, data collection and processing e.g. transcript preparation, etc.  Click or tap here to enter text. |
| **D** | **Principle 4 - Accuracy** | | |
|  | N/A for research, as point in time data direct from participants | | |
| **E** | **Principle 5 – Storage limitation**  🛈 We are only interested in “raw” personal data from which individuals can be identified. Typically, more ’sensitive’ personal data e.g. special category data, audiovisual recordings etc. would have a shorter retention period – probably until the findings of the study have been audited/checked/reviewed for verification purposes, but the legislation allows personal data for research to be kept for longer periods than it would for other types of processing. Consent records would typically be kept for 6 years post-study, or longer if it is necessary to keep the personal data collected for the research for a longer period (with appropriate rationale). Please think what personal data **actually needs** to be kept in relation to the project and the practicalities of destroying it when it reaches the end of its retention period e.g. will the data be needed for subsequent research? Who is going to delete the data and do they have a reminder diarised to do this?  Externally funded projects may have retention periods dictated by funders.  If you leave the University you will need to ensure that a colleague/supervisor can destroy the personal data on the date the destruction is due. | | |
| i | You have agreed retention periods for the **personal data** and will diarise an event in future to ensure that the “raw” personal data is destroyed when the time comes or arrange for someone else to destroy the data e.g. if you leave the University).  This is not the same as the retention period for anonymised research data given in the DMP (usually 10 years). | Choose an item. | How long are you keeping the ‘raw’ personal data for before it is deleted/destroyed? (please read the guidance in blue above)  Click or tap here to enter text.  Have you diarised an event in your Outlook calendar for either yourself or a colleague or supervisor to remind you when the time come to destroy the ‘raw’ personal data?:  Click or tap here to enter text. |
| **F** | **Principle 6 – Integrity and confidentiality (SECURITY)** | | |
|  | 🛈 You have appropriate organisational and technical measures (security) in place, including assessing the security of your work environment and the electronic and manual (e.g. paper, samples, etc.) systems you use, to protect and secure personal data during processing.  The legislation requires all processing, in transit (when being sent between entities or systems) and at rest (when in storage in a data repository or system) to be to be secure e.g. **electronic data must be encrypted at all times**. Guidance for both electronic and physical data security can be found here: [Security of Personal Data (napier.ac.uk)](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/SecurityofPersonalData.aspx). Email is NOT a secure method of transferring /sending personal data, unless encrypted, see: [Email Encryption (napier.ac.uk)](https://staff.napier.ac.uk/services/cit/infosecurity/Pages/EmailEncryption.aspx).  If transferring physical documents (paper) or assets (encrypted audio recorder, etc.), please consider how you will keep those secure both outside University premises (e.g. when in use/ travelling) and on Campus.  Using University provided ICT systems and Apps will ensure processing is secure. If systems or companies/individuals/Apps which are external to the University are used there are procurement implications and a Data Sharing or Processing Agreement must be in place, v to vii below refer. The approval of new suppliers can take time, so please take this into account and give us plenty of notice. Using systems already approved for use within the University means that there will be no new system approval delays.  Audiovisual recorded interviews should be stored as MP3 files unless the ‘visual’ aspect of the recording is necessary for the project e.g. gesture/expression analysis. If using an external transcription service only MP3 files should be provided.  Please advise how the personal data will be securely processed for each of the steps below: | | |
| i | You are only using electronic/computer systems and services provided and approved by the University’s Information Services team. Please see: [All apps | AppsAnywhere (napier.ac.uk)](https://apps.napier.ac.uk/apps/all) for University provided systems / Apps. | Choose an item.  If you have chosen ‘No’ please list the other (non University Information Services provided) systems:  Click or tap here to enter text. | |
| ii | Please detail any specific measures you are taking to keep personal data secure which is not mentioned elsewhere e.g. encryption, password protection, etc. | Security measures for electronic personal data:  Click or tap here to enter text.  Security measures for manual/paper personal data:  Click or tap here to enter text. | |
| iii | Sharing/transfer of personal data (with external parties, between researchers or between systems)  Personal data should not be shared by email or other insecure means. | Detail ***how*** any sharing/transfer of personal data will take place, if any:  MS Teams  MS Sharepoint  Secure online portal, please provide name and portal provider below:  Click or tap here to enter text.  Other  Click or tap here to enter text. | |
| iv | Deletion/Archiving (e.g. paper in University confidential waste consoles, secure electronic deletion within the University network (e,g, deleted from University folder/ repository/system and the recycle bin), full formatting/wiping of portable devices, etc.) | Detail ***how*** you will securely dispose of personal data, select those which apply:  paper in University confidential waste consoles  portable devices to be fully formatted / wiped  secure electronic deletion within the University network e.g. deleted from folder / repository / system and any recycle bin/s.  other  Click or tap here to enter text. | |
| v | Are you sharing any personal data with 3rd parties external to the University?  The University has Data Processing Agreements with Trusty Transcriptionists and 1st Class Secretarial for transcription services. | Choose an item. | Detail the parties and what they are doing with the personal data, including any system or app providers.  Click or tap here to enter text. |
| vi | If the answer to G)vi above is Y, do you have data sharing/processing agreements in place | Choose an item. |  |
| vii | If the answer to G)vi above is Y, have security checks been completed to ensure those 3rd party/ies comply with Principle 6 | Choose an item. |  |
| **G** | **Principle 7 – Demonstrating compliance** | | |
|  | Note for Governance: This document along with the Privacy Notice above and DMP should provide adequate documentation. Potentially an additional risk table if that is considered necessary and appropriate to the risks. | | |
| **H** | **Personal data not to be transferred to 3rd countries/ territory (outwith the EEA 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** | | |
| i | You are transferring personal data to a third country or territory outwith the UK and not on the ‘adequate’ [list](https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/)? | Choose an item. | If yes, detail which country the data will be transferred to:  Click or tap here to enter text. |
| 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 | Choose an item. |  |
| iii | You have completely anonymised the data | Choose an item. |  |
| **J** | **Data subjects are able to exercise their rights** | | |
|  | You have made arrangements to comply with the individuals’ rights – in particular: | | |
| i | 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 | Choose an item. |  |
| ii | You will keep your data in such a way that should participants wish to receive a copy of their personal data you will be able to provide it. | Choose an item. |  |
| iii | Are you doing anything specifically to safeguard the rights and freedoms of your participants with regards to their personal data? |  | Click or tap here to enter text. |
| **K** | **Breach notification** | | |
| i | You will immediately report any personal data breach or other breach of the legislation to your research supervisor and they will follow University procedures.  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. | Choose an item. | See section [7.10 online](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/SecurityofPersonalData03.aspx) |

**If you would like to provide additional information, please do so here:**

**Section 5 – Risks and mitigations (Governance Services to complete initially, Researchers may be required to provide additional information)**

|  |  |
| --- | --- |
| **Governance will complete this** | |
| **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):** |  |

**Updated: 20221116**