children's hearings scotland

The Children's Panel – life changing.

PRIVACY IMPACT ASSESSMENT – template

Screening questions

1. **Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected, below.**

2. **Will the project compel individuals to provide information about themselves? If yes, please detail the information to be provided, below.**

3. **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access, below.**

4. **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.**

5. **Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.**

6. **Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.**

7. **Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. If yes, please describe the information to be collected, below.**

8. **Will the project require you to contact individuals in ways that they may find intrusive? If yes, please describe how the individuals will be contacted, below.**

Step one: Identify the need for a PIA

What does the project aim to achieve?

What will the benefits be to the organisation, to individuals and to other parties?

Is there a project proposal? If yes, please provide the link, below.

Why was the need for a PIA identified (refer to screening questions above)?

Step two: Describe the information flows

How will the information be collected and transferred to the organisation?

Who will have access the information?

Where will the information be held?

What will the information be used for?

How long will the information be retained? How will it be destroyed/deleted?

Who will be the owner of the information?

Will the information be shared with anyone? If yes, who?

Please insert an information flow diagram below.

Consultation requirements

What practical steps have been taken to ensure that you identify and address privacy risks?

Who has been / will be consulted internally and externally about the privacy concerns / risks?

How was the consultation carried out? How will any future consultations be carried out?

What were the outcomes of the consultation? What privacy concerns were raised internally / externally? How will you report on any future consultations?

Step three: Identify the privacy and related risks

Please outline the risks to individuals, the organisation and compliance below.

Privacy issue	**Risk to individuals** (see examples at annex A)	**Compliance risk** (see examples at annex A)	**Organisation risk** (see examples at annex A)

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (please see examples at annex B).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented? When will the PIA report be produced and who will be responsible?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Annex A

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.
- Non-compliance with the DPA. Please see further information and answer the questions below.

Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

1.1 Have you identified the purpose of the project? If yes, please detail the purpose below.

1.2 How will you tell individuals about the use of their personal data?

1.3 Do you need to amend your privacy notices? If yes, please describe how below?

1.4 Have you established which conditions for processing apply? If yes, please detail below?

1.5 If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

1.6 Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act?

1.7 Have you identified the social need and aims of the project? If yes, please detail below.

1.8 Are your actions a proportionate response to the social need?

Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

2.1 Does your project plan cover all of the purposes for processing personal data?

2.2 Have you identified potential new purposes as the scope of the project expands?

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.1 Is the quality of the information good enough for the purposes it is used?

3.2 Which personal data could you not use, without compromising the needs of the project?

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

4.1 If you are procuring new software does it allow you to amend data when necessary?

4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

5.1 What retention periods are suitable for the personal data you will be processing?

5.2 Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.

6.1 Will the systems you are putting in place allow you to respond to subject access requests more easily?

6.2 If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7.1 Do any new systems provide protection against the security risks you have identified?

7.2 What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

8.1 Will the project require you to transfer data outside of the EEA?

8.2 If you will be making transfers, how will you ensure that the data is adequately protected?

Annex B

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.