PRIVACY IMPACT POLICY AND PRIVACY BY DESIGN POLICY

This policy will be used by National Association of Retired Police Officers whenever any new project is undertaken whether in relation to IT and Communications, Marketing, Human Resources, or any other activity.

The aim is to ensure that we review carefully the effect of any project on the privacy of individuals and limit the personal data we collect to only that which is necessary and consider how we use this personal information.

We will on every occasion ask ourselves the following screening questions:

1. Will the project involve the collection of new information about individuals?
2. Is the information necessary?
3. Will the project compel individuals to provide information about themselves?
4. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
5. Are we using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
6. Does the project involve us using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
7. Will the project result in us making decisions or taking action against individuals in ways that can have a significant impact on them?
8. 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 particularly private.
9. Will the project require us to contact individuals in ways which they may find intrusive?

These questions and the answers to them will assist us to decide whether a Privacy Impact Assessment (PIA) is required.

Procedure to be followed

We will adopt a template approach to determine whether a PIA is required and to organise the PIA. This shall be as follows:

Step one: Identify the need for a PIA

- Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
- If helpful to link to other relevant documents related to the project, for example a project proposal.

- Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).
- Who will be responsible for the PIA

Step two: Describe the information flows

- The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

- Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.
- Consultation can be used at any stage of the PIA process.

Step three: identify the privacy and related risks

- Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
- Privacy issue
- Risk to individuals
- Compliance risk
- Associated organisation / corporate risk
- Identify the legal ground for processing
- See schedule 1 for additional questions to be asked.

Step four: Identify privacy solutions

- Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).
- 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?
- 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 which may arise in the future?
- Action to be taken
- Date for completion of actions
- Responsibility for action
- Contact point for future privacy concerns

Schedule 1

Answering these questions during step 3 of the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

1. Have you identified the purpose of the project?
2. How will individuals be told about the use of their personal data?
3. Do you need to amend your privacy notices?
4. Have you established which conditions for processing apply?
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?
6. Will it be necessary to have a positive opt in?
7. If your organisation is subject to the Human Rights Act, you also need to consider:

    - Will your actions interfere with the right to privacy under Article 8?
    - Have you identified the social need and aims of the project?
    - Are your actions a proportionate response to the social need?

8. Does your project plan cover all of the purposes for processing personal data?
9. Will individuals have the opportunity or right to refuse to provide the information?
10. Have potential new purposes been identified as the scope of the project expands?
11. Is the information you are using of good enough quality for the purposes it is used for?
12. Which personal data could you not use, without compromising the needs of the project?
13. If you are procuring new software does it allow you to amend data when necessary?

14. How are you ensuring that personal data obtained from individuals or other organisations is accurate?
15. How will information be updated?
16. What retention periods are suitable for the personal data you will be processing?
17. Are you procuring software which will allow you to delete information in line with your retention periods?
18. Will the systems you are putting in place allow you to respond to subject access requests more easily?
19. If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
20. Would it be possible to use pseudonymous data?
21. Do any new systems provide protection against the security risks you have identified?
22. What training and instructions are necessary to ensure that staff know how to operate a new system securely?
23. Do you need to appoint a Data Protection Officer (DPO)?
24. Do you have signed agreements with all data processors?
25. Will the project require you to transfer data outside of the EEA?
26. If you will be making transfers, how will you ensure that the data is adequately protected?