# PRIVACY IMPACT ASSESSMENT TEMPLATE

These questions are intended to help you decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

**Will the project involve the collection of new information about individuals?**

**Yes**

**Will the project compel individuals to provide information about themselves?**

**No**

**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**

**Only under very limited circumstances**

**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**

**No**

**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.**

**No**

**Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**

**No**

**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.**

**Yes**

**Will the project require you to contact individuals in ways that they may find intrusive?**

**Yes**

# Privacy impact assessment template

The template follows the process that is used in the ICO’s PIA code of practice.

|  |
| --- |
| **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.  You may find it 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).  A system is required to provide the authority's statutory monthly return to DfE, from which is calculated NEET, participation and other performance measures, including progress for Raising the Participation Age. This requires a system that is compliant with the DfE/NCCIS specification for a Client Caseload Information System (CCIS).  The current Microdec Profile system will only continue to be DfE/NCCIS compliant up to and including April 2016 changes. After this date, no further changes will be made to the system by Microdec and compliance will not be maintained with the statutory return. The DfE usually update the specification on a yearly basis, which means that Profile could potentially maintain compliance up to April 2017 but if in-year changes were introduced after April 2016 we could become non-compliant.  The implications of the project not going ahead would be the inability to accurately support the local authority’s statutory returns. The key requirements of the replacement are contained here:  <https://www.gov.uk/government/publications/nccis-management-information-requirement>  The Connexions IAG service provides information, advice and guidance to young people aged 13-19 or 13-24 for those with learning difficulties and/or disabilities and uses this system to record all its work.  We are also looking for it to be more versatile and be able to record youth service activities. |

|  |
| --- |
| **Step two: Describe the information flows**  You should describe the collection, use and deletion of personal data 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.  Most data will enter the system from the LA SIMS detail for school attended in year 9/10. There will be a transfer of between 3,500-4,000 names onto the system each year of everyone who lives in the City/attends a City school.  For those who attend a County school, but live in the City, there will be no further action until the end of year 11.  Further additions of those joining City schools will be made by cross-referencing to the ONE database, or by personal advisers being informed by their school of new joiners.  A key requirement is to report on the whereabouts of young people in the 3 years after year 11. To support this we have a data transfer agreement with all City schools and colleges which means we have can be notified of all those enrolled, plus early leavers. Training providers also notify us of their starters and leavers.  The guidance is from the legislation in the link below:  <http://www.legislation.gov.uk/ukpga/2008/25/part/1/chapter/2>  As part of this, there will be be bulk transfers of data in and out of the LA, particularly with Prospects who currently have the IAG contract for Leicestershire.  All the data on the activity of years 12-14s is sent, on a monthly basis, to DfE via a secure portal.  Where we have lost track of an individual, we can share details with an authority we believe the person may now be resident in, again via this secure DfE portal.  Data is also transferred from DWP to help track 18/19 year olds who are registered with Job Centre Plus.. The guidance below is the basis for this:    As part of this tracking, we will sometimes text clients. In the new replacement system, there may be a facility to link SMS messages. Bulk e-mails/postal communications may also be sent and recorded on the system.  Very few individuals will be deleted from the system. If they move areas, their original details remain, and with client consent, they are shared with the new LA (if within England). If they are deceased the record is hidden to all but the system administrator. If there is a reason for restricting access, for example the individual is a member of staff, or is involved in a high profile news story, different levels of restrictions can be added.  All records can be archived. |

|  |
| --- |
| **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.  You can use consultation at any stage of the PIA process.  A data processing agreement has been inserted as a schedule to the contract, which sets out the responsibilities of the data controller (LCC) and the data processor (Supplier)  Support from ICT procurement team, the standard data protection question has been asked in the tender and the terms have been drafted by Legal services.  Information Governance & Risk Team |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step three: Identify the privacy and related risks**  **Definition of personal data:**  Data which relate to a living individual who can be identified –  (a) from those data, or  (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.  **Definition of sensitive personal data:**  Personal data consisting of information as to -  (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c ) his religious beliefs or other beliefs of a similar nature,  (d) whether he is a member of a trade union, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.  **The 8 Data Protection Principles:**   1. Personal data shall be processed fairly and lawfully 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. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 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. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.   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.  **Principle 1** **- Personal data shall be processed fairly and lawfully**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | Have you identified the purpose of the project? | The current product has reached the end of its life. The new project enables the authority to deliver a statutory duty. | | Is there a lawful reason you can carry out this project? | <https://www.gov.uk/government/publications/nccis-management-information-requirement> | | How will you tell individuals about the use of their personal data? | Parents sign a data exchange form at school. There is a box which allows an opt out not to share with the LA.  The data is then transferred from the LA schools database to the NCCIS compliant one.  Once Connexions staff meet a young person face to face, it is explained their information is held on the database and it would only be shared if there was a risk to the person, or someone else. Currently, the Youth Service do not have an electronic recording system so this needs to be considered in how they talk to their service users about the data held.  We do not draw attention to what to do if they are unhappy with the data held. Perhaps this needs to be considered? | | Do you need to amend your privacy notices? The Council’s main one can be found [here](http://www.leicester.gov.uk/your-council-services/council-and-democracy/key-documents/internet-disclaimer/). Do you have service specific ones? | Every interview an adviser does should start with a privacy statement and an explanation that their details will not be shared unless there is a risk of harm.  There is also a written statement explaining this in the interview spaces in the Connexions Centre.  Will send a copy to Information Governance.  Will need similar statement for Youth Service? | | Have you established which schedule 2 conditions for processing apply? (The conditions can be found [here](http://www.leicester.gov.uk/your-council-services/council-and-democracy/data-protection-and-foi/information-sharing/partner-tools/).) | 1 - With the consent of the data subject  2 – To establish or perform a contract with the data subject  3 – to comply with a legal obligation  5(c) – Public interest nature - Dfe is the government department for whom it is gathered. | | If sensitive personal data is involved, have you established which schedule 3 conditions for processing apply? (The conditions can be found [here](http://www.leicester.gov.uk/your-council-services/council-and-democracy/data-protection-and-foi/information-sharing/partner-tools/).) | 1 – explicit consent  3 – To project the vital interests of the data subject or another person - Looked after children - Safeguarding  7 – Public interest nature  9 – for equal opportunity ethnic monitoring | | 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? | If consent is withheld, we remove the address/phone number and click a “do not survey” option. | | Will your actions interfere with the right to privacy under Article 8 of the [Human Rights Act](http://www.leicester.gov.uk/your-council-services/council-and-democracy/data-protection-and-foi/information-sharing/partner-tools/)? If yes, is it necessary and proportionate? | Yes but it is proportionate, and necessary and the following criteria is met.   * The economic well-being of the country * Protection of the rights and freedoms of others. | | Have you identified the social need and aims of the project? | No social need. | | Are your actions a proportionate response to the social need? | n/a |   **Principle 2** **- Personal data shall be obtained only for one or more specified and lawful purposes**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | Does your project plan cover all of the purposes for processing personal data? | A technical assessment has been part of the project plan and a separate panel have scored the responses in this section. | | Which personal data could you not use, without compromising the needs of the project? | Only minimum data is required at the first stage.  Names, address, phone number, schools attender, gender, ethnic origin.  More is added as contact increases. |   **Principle 3** - **Personal data shall be adequate, relevant and not excessive**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | Is the quality of the information good enough for the purposes it is used? | For addresses, Gazetta data is used.  All efforts to be made to ensure the accuracy of personal data held. | | Which personal data could you not use, without compromising the needs of the project? | Only minimum data is held. It increases with more contacts, especially with more vulnerable young people, but principal 1 will be met in this event. |   **Principle 4** **- Personal data shall be accurate and, where necessary, kept up to date**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | If you are procuring new software does it allow you to amend and / or delete data when necessary? | Yes | | How are you ensuring that personal data obtained from individuals or other organisations is accurate? | It is updated at least annually.  All destinations have a shelf life so need to be reviewed. |   **Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | What retention periods are suitable for the personal data you will be processing? How long will you keep the data for? | All personal information is subject to principal 5 of the Data Protection Act 1998, and it doesn’t make a distinction between types of information. It expects you to keep information for the minimum time required. I understand the current advice | | Are you procuring software that will allow you to delete information in line with your retention periods? | Yes, but it will not do so automatically. We would need to instruct them to do so as it is a hosted system.  As part of the current guidance around data held on vulnerable young people (and the potential for historic child abuse allegations) we will not delete the data until further guidance. We will be seeking advice on whether we can delete data on those we have not had contact with so there is no information that would be of use for future investigations. |   **Principle 6** **- Personal data shall be processed in accordance with the rights of data subjects**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | What process is in place to answer ‘Subject Access Requests’ (requests for personal data)? | LCC has an information governance policy which requires all data protection requests/complaints to be logged centrally with the Information Governance Team. |   **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.**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | Do any new systems provide protection against the security risks you have identified? | Yes, a higher level security setting than current system. For example, a password expiry every 60 days. | | What training and instructions are necessary to ensure that staff know how to operate a new system securely? | Training will be provided for all users. There will be guides created by our own trained staff  There will be a password to access the database. It will log out after 20 minutes of being idle. | | What training on data protection and / or information sharing has been undertaken by relevant staff? | LCC policies and protocols will be followed.  Use of the Leicester Learning Pool for updates. |   **Principle 8** - **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection.**   |  |  | | --- | --- | | **Privacy issue** | **Comments** | | Will the project require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection? | No | | If you will be making transfers outside of the EEA, how will you ensure that the data is transferred securely? | n/a | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step four: Identify privacy solutions**  Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg 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? | | Incorrect data/duplicate data  Loss/theft of data  Purpose creep | Regular cross-checks with other LA/education data. Checks with clients when in contact.  Will be safely transferring data using a VPN. Courier has been used by other LAs, as have drop boxes. Will aim to avoid this at all costs. | Reduced |  |   Please also see completed risk assessment template in spreadsheet below |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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 | | All of the above |  |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | | ISA signed  Data migration onto new system  Testing of new data before going live to check is accurate |  |  |  |  | | --- | |  | |  | |