PART 1 Privacy impact assessment screening of contract awards for the Leeds Skills, Training and Employment Pathways (STEP) Programme.

1. Will the project involve the processing of information about individuals?

   NO. Providers will not be required to provide personal information about individuals during contract award.

2. Will the project compel individuals to provide information about themselves?

   NO. Providers will not be required to provide personal information about individuals during contract award.

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

   NO.

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?

   NO.

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

   NO.

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

   NO.

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 particularly private.

   NO.

8. Will the project require you to contact individuals in ways which they may find intrusive?

   NO.

PART 2 Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process which is used in this code of practice. You can adapt the process and this template to produce something which allows your organisation to conduct effective PIAs integrated with your project management processes.

Project Manager:	Name:	Craig Skinner
	Title:	Projects and Programmes Senior Manager
	Service:	Employment and Skills
	Telephone:	07891279488
	Email:	Craig.skinner@leeds.gov.uk
Information Asset Owner(s) • *All information assets must have an information asset owner (IAO). IAO's are usually Heads of Service or Chief Officers.* • *For further information regarding IAO's please contact your directorate InCo, details of which can be found in the Managing Information Toolkit on InSite.*	Name:	Matt Wilton
	Title:	Head of Employment Access and Growth
	Service:	Employment and Skills
	Telephone:	07891279677
	Email:	Matthew.Wilton@leeds.gov.uk
Project sponsorship details (if different from IAO)	Name:	Sue Wynne
	Title:	Chief Officer
	Service:	Employment and Skills
	Telephone:	0113 37 83154
	Email:	Sue.Wynne@leeds.gov.uk
System Administrator (if applicable)	Name:	Philippa Elliott
	Title:	Procurement Category Manager (Business and Professional Services)
	Service:	Projects, Programmes and Procurement Unit
	Telephone:	0113 3952139
	Email:	Philippa.Elliott@leeds.gov.uk

1. Identify the need for a PIA
1.1. Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
• *Should be taken from proposal, project plan, PID etc*
This screening covers the award of a three year contract to six specialist providers to deliver on the Leeds STEP programme, commencing April/May 2017.
1.2 Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).
This screening was undertaken in conjunction with the contract award process, and no individual's personal information will be collected through the award process.
2. Describe the information flows
2.1 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.

No personal data will be collected or used as part of the contract award process.

Procurement Projects & Programmes Unit (PPPU) and Employment and Skills staff directly involved in the contract award will access applications information.

Contract information will be stored in the PPPU system and on the Employment and Skills network drives.

The progrmame will not create new or change existing links with other collections of personal data.

Contract information will be sent off site privately to each respective organisation via the YORtender procurement system and will not be moved outside of the EU or EEA.

3. Consultation requirements

3.1 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.

No Individual Privacy risks identified in this PIA.

PIA will be separately completed for the delivery of the STEP Programme. This PIA will be a agreed and overseen by STEP Board.

Any issues / breaches identified through contract management processes or otherwise will be assessed and actioned by the Projects and Programmes Senior Manager.

Where a breach is deemed serious it will be escalated up to the Informaton Asset Owner (Head of Service)

4. Identify the privacy and related risks

4.1 Identify the key privacy risks (assign each risk a reference number) and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

The YORtender website guarantees all organisations' information is kept private and secure.

The network drive storage area is only accessible to Employment and Skills staff and those ICT staff responsible for infrastructure management and backup.

All Employment and Skills staff are trained on Council privacy and Information Governance policies and procedures.

No individual personal data will be collected as part of the award process.

Contract information will not be published or made available outside of the Employment and Skills service

5. Identify privacy solutions

5.1 For each privacy risk identify a solution and note the expected result (risk eliminated, reduced or accepted) and an evaluation of the final impact on individuals after implementation and whether this is a justified, compliant and proportionate response to the aims of the project.

No Individual Privacy risks identified
6. Sign off and record the PIA outcomes
6.1 For each risk note the approved solution and record the approval. Who has approved the privacy risks involved in the project? What solutions need to be implemented?
No Individual Privacy risks identified
7. **Integrate the PIA outcomes back into the project plan**
7.1 Record name of person(s) responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Record who is responsible for implementing the solutions that have been approved? Finally record future contact names of persons responsible for maintaining the PIA through the project?
No Individual Privacy risks identified Projects and Programmes Senior Manager Craig Skinner is responsible for maintaining the PIA throughout the three year contract.

Annex - Identifying risk relevant to the PIA

1. Linking the PIA to the data protection principles

Answering these questions during 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, such as the Human Rights Act.

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.

- *Have you identified the purpose of the project?* *YES*
- *How will individuals be told about the use of their personal data?* No individual's data collected
- *Do you need to amend your privacy notices?* No
- *Have you established which conditions for processing apply?* No individual's data collected
- *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?* No individual's data collected
- *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?* No individual's data collected
- *Have you identified the social need and aims of the project?* *YES, to award contracts to delivery providers*
- *Are your actions a proportionate response to the social need?* *YES, to award contracts to delivery providers*

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.

- *Does your project plan cover all of the purposes for processing personal data?* Yes however, no individual's data collected
- *Have potential new purposes been identified as the scope of the project expands?* Yes, following contract awards and before the start of the delivery phase a new PIA will be undertaken to review the ongoing use of all Management Information Systems and data sharing sites e.g. Sharepoint that all contracted providers will be using.

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

- *Is the information you are using of good enough quality for the purposes it is used for?* YES, no individual's data collected

- *Which personal data could you not use, without compromising the needs of the project?* No individual's data collected

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

- *If you are procuring new software does it allow you to amend data when necessary?* No individual's data collected

- *How are you ensuring that personal data obtained from individuals or other organisations is accurate?* No individuals data collected

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

- *What retention periods are suitable for the personal data you will be processing?* No individual's data collected

- *Are you procuring software which will allow you to delete information in line with your retention periods?* No individuals data collected

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

- *Will the systems you are putting in place allow you to respond to subject access requests more easily?* No individual's data collected

- *If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?* Promotion of the contract awards via Council communications team, Updates via YORtender, no individual's data collected

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.

- *Do any new systems provide protection against the security risks you have identified?* No individual's data collected

- *What training and instructions are necessary to ensure that staff know how to operate a new system securely?* No individuals data collected, staff trained on Council IG and privacy policies

- *Standard security risks might include*
    - *Methods of transmitting /sending data(fax, standard email, IM, text, secure email, website, courier, by hand , external post, telephone)*
    - *Contingency plan for losing data, unavailability of information or system if relevant, interruption to business*
    - *Access controls poorly designed or operated*
    - *Data quality and accuracy*
    - *Obtaining and managing consent; maintaining it.*

- *Information handling procedures*

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.

- *Will the project require you to transfer data outside of the EEA?* No individual's data collected

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

2. Linking the project to major sources of Data Protection risk (not exhaustive)

The following questions are designed to identify significant areas of potential Data Protection risk within the project.

Technology

1. Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

   No individual's data collected

   Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Identity

2. Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

   No individual's data collected
   Examples of relevant project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.

3. Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

   No individual's data collected
   Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.

Multiple organisations

4. Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?

   Yes (agencies are YORtender, Leeds Council and providers), no individual's data collected

   Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation

to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.

Data

5. Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

   No individual's data collected

   The Data Protection Act at s.2 identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

   There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.

   Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.

6. Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

   No individual's data collected

   Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

7. Does the project involve new or significantly changed handling of personal data about a large number of individuals?

   No individual's data collected

   Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.

8. Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

   No individual's data collected

   This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.

Exemptions and exceptions

9. Does the project relate to data processing which is in any way exempt from legislative privacy protections?

   No individual's data collected, Standard Council policies and organisational due diligence will take place via PPPU

   Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.

10. Does the project's justification include significant contributions to public security measures?

    No individual's data collected

Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.

11. Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

    No individual's data collected

    Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

    Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.

3. Tracking outcomes of the PIA

Suggested format PIA outcomes table

DP issue	Risks	Risk ref no	Proposed solutions	Result	Evaluation of final impact.	Approved solution	Action ref no.	Approved by	Completion expected	Who responsible?	RAG status