Privacy Impact Assessment of the Procurement for a Solution for the Supply of an ESFA compatible Adult Learning Management Information System, online enrolment and integrated payment facilities with associated services.

CONTENTS

Contents	**Page**
Introduction	3
Annex A	4
• Privacy impact assessment screening questions	4
Annex B	5
• Privacy impact assessment template	5-10
Annex C	11
• Linking the PIA to the data protection principles	11-13

Introduction

The Council has undertaken a Privacy Impact Assessment (PIA) of its Procurement for a Solution for the Supply of an ESFA compatible Adult Learning Management Information System, online enrolment and integrated payment facilities with associated services.

Annex A

Privacy impact assessment screening questions

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.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

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

Will the project compel individuals to provide information about themselves?

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

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

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.

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

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.

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

Annex B

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 that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

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).

Privacy Notice

How We Use learners Personal Information

This privacy notice is issued by Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 2018, the DfE is the data controller for personal data processed by the DfE.

Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a Personal Learning Record (PLR).

Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is incompliance with the Data protection Act 2018.

For further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:

https://www.gov.uk/government/publications/esfa-privacy-notice

In procuring an MIS system the standards and criteria applied currently will need to be upheld in any new or revised contract with a supplier and any subsequent SLA concerning the management of the contract.

The PIA screening questions were answered and provide 'yes' answers to the following questions:

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

Will the project compel individuals to provide information about themselves?

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

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

Given the above there is a need for the PIA.

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.

1. Data is collected from Enrolment form and input into the MIS system at a designated MIS computer. MIS data input staff have limited system rights
2. The enrolment form is held securely in the centre or origin
3. The MIS data is stored on the host servers
4. MIS system administrators are able to interrogate the data and use it to produce performance reports, status report and projected ESFA income/
5. MIS system administrators collate, verify and upload data to the ESFA via the Individual learner record reports; which is used to provide evidence to the ESFA so they can release funding to DACES
6. Both paper and electronic records have to be held in accordance with audit requirements.

DACES collected enrolment information from all its learners and in the 2016/17 academic cycle there were 12,000 individual learners, enrolled on over 3,000 courses.

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.

Consultation requirements are met via the learners being advised that a condition of their learning being funded by the ESFA is that the delivery providers are contractually obligated to collect data and treat the data in accordance with the privacy statement contained on the enrolment form; which they retain a copy.

The paper based information is stored in accordance with the information and classification handling requirements

Data inputting is onto secure servers and systems, compliant with data protection and organisations being recognised data controllers.

DACES data handling will be subject to the routines of Audit Services and the Information Security team alongside the contractual data a handling requirements of the ESFA and Ofsted.

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.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Storage of Data	If released could cause harm and distress to individuals	Could be accesses or hacked if not secure.	Could contravene legislations, such as the Data Protection Act (2018).
Release of Data	If released could cause harm and distress to individuals	Persons accessing the data and using it in for unauthorised means	Could contravene legislations, such as the Data Protection Act (2018).
Misuse of Data	If released could cause harm and distress to individuals	Persons accessing the data and using it in for unauthorised means	Could contravene legislations, such as the Data Protection Act (2018).

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 the individuals after implementing each solutions a justified, compliant and proportionate response to the aims of the project?
Information loss, data breach	Clear process & compliance standards are subject to regular inspections & Audit	Risk would be minimised and accepted.	Risk to individual is mitigated to an accepted level

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
Information loss, data breach	Internal management & Audit	

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
Integrate PIA into soft market test and tender specification	October 2017 Revised Aug 2018	

Contact point for future privacy concerns

Annex C

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, for example 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 you tell individuals about the use of their personal data? By use of the Privacy notice which is shown in step 1 in Annex B

Do you need to amend your privacy notices? No

Have you established which conditions for processing apply? Yes

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? N/A

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

Have you identified the social need and aims of the project? Yes

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

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

Have you identified potential new purposes as the scope of the project expands? The scope of the project will not expand.

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

Which personal data could you not use, without compromising the needs of the project? None

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? This will be a requirement.

How are you ensuring that personal data obtained from individuals or other organisations is accurate? Learners have to self-declare that the information they supply is accurate and affirm this when they sign the enrolment form

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? ESFA retention period is a minimum of 7 years.

Are you procuring software that will allow you to delete information in line with your retention periods? This will be a requirement.

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? Not sure – not seen any yet.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose? Does not involve marketing. Yes and there is an opt-out facility.

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? This will be a requirement.

What training and instructions are necessary to ensure that staff know how to operate a new system securely? Training will be a requirement of the procurement.

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? Do not know as not got to tender stage yet; but this would be very unlikely

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

Conditions for processing under the Data Protection Act can be found at;

https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/