



**Privacy Impact Assessment of  
the Procurement of the Supply of  
Live Online Lessons,  
Asynchronous Learning  
Activities and Associated  
Services**

**Version 0.1**

## **CONTENTS**

INTRODUCTION .....	3
ANNEX A .....	3
PRIVACY IMPACT ASSESSMENT SCREENING QUESTIONS .....	3
ANNEX B .....	4
PRIVACY IMPACT ASSESSMENT TEMPLATE .....	4
ANNEX C .....	13
LINKING THE PIA TO THE DATA PROTECTION PRINCIPLES .....	13

## Introduction

The Council has undertaken a Privacy Impact Assessment (PIA) of its Procurement for a Solution for the Supply of Live Online Lessons, Asynchronous Learning Activities and 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.

**Will the project involve the collection of new information about individuals? No**

**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? Yes**

**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**

## 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).**

The use of an outside provider will enable an enhanced and broad range of online lessons to be offered and will maximise the use of technology to most efficiently meet the statutory requirement to offer 25 hours learning a week to meet the needs of students who cannot attend the normal school provision.

A suitable commercial provider will be able to offer a range of online courses including short term “drop in” style courses to longer term GCSE courses and qualifications. The provider will also be able to offer additional GCSE subjects that are currently unavailable to many of our most vulnerable groups.

It could further support the reduction of staff travel time and costs and make the best use of available staff resources, allowing teachers to communicate with students and lessons to be delivered online as well as facilitating the motivation and monitoring of students and ensures safeguarding requirements with respect to students accessing part of their education provision online are met.

It recognises that not all students learn or engage in the same way and utilises the young person’s own experiences, expertise and enjoyment via the use of the internet and technology. It seeks to build on and enhance their experiences and acknowledges them as having a voice in their own learning processes, utilises a multi-disciplinary approach across services as well as supporting and making appropriate use of support from parents and carers in the home.

Via the administration and tracking systems used by commercial providers, students' progress will be more easily monitored, enabling appropriate personalised learning programmes to be created. Students can easily see the progress they are making, building self-esteem and motivation.

There should be efficiencies in the use of a single commercial provider for online lessons whilst maintaining a management and referral service within the Council not only in the overall annual costs, but also with contract management and procurement. There should also be efficiencies available in providing a solution that also offers the facility for virtual live lessons and virtual communications with students for use by the VC/IPT/OOST teams and other referring agencies, in terms of reduced transport costs and more efficient use of staff time.

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

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

**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?**

### 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.

#### **Live Online lesson provision – Information Flow Chart**

**Pupil Information Form (PIF):** sent from referring agency (via secure Derbyshire County Council email) or EDRM. To enable the Virtual Classroom to create a referral to the online lesson provider. Virtual Classroom Business Services Assistant (BSA) saves on to EDRM, then extracts required information to create enrolment information required by online lesson provider.



**Online Lesson Provider:** Pupil enrolment information is entered directly on to the provider's Learning Management System (LMS) to enable student to be enrolled with the online lesson provider. Information includes: student's name, year group, DOB, preferred start date, subject, academic level, information/issues which may represent barriers to the student's learning. Parents name, address and parental contact phone numbers for use in safeguarding incidents. **Reason:** Information is used to create the students online account and set up their timetable and account on LMS. Data is saved securely in line with Derbyshire County Council (DCC) policy/audit requirements.



**Virtual Classroom** extracts the following information directly from the provider's LMS: Weekly and termly reports and attendance data setting out student's engagement in lessons, participation and attendance. Data is then stored securely on EDRM.



**DCC Staff Data:** (Required to set up new staff user for admin purposes). Name, email address and contact phone number. This data is input directly to the provider's LMS by an existing DCC administrator.



**Online lesson provider:** Data is used to create new DCC staff user account to enable DCC staff to log into LMS to enter new student's data for enrolment purposes and extract weekly/termly report and attendance data.



**Student data** is stored on provider's LMS for maximum of 6 months after a student has left the online provision in line with data security requirements of DCC audit team. This provides time for all data to be extracted by DCC and saved securely with EDRM.



**EDRM storage times:**

70 years – LAC (Looked After Children)

35 years – SEN/EHCP students

25 years – For all other students accessing provision through DCC referral process

*Maximum 80 Students per year will access the provision,  
Maximum of 80 DCC staff mentors for students accessing the provision  
Maximum of 4 DCC administrators*

### 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.**

Audit Services and the Information Security team will review the Invitation To Tender documents and perform due diligence on the selected highest scoring tenderer which includes site visits, penetration tests and data centre visits to ensure that data is held in a secure manner at every stage. Unless the Solution is compliant it will not be allowed to go live.

Once the Solution is live, the Contractor will be expected to undertake regular security checks to ensure that the data cannot be breached as will be defined in the Contract.

Contract management meetings will include an operational review of any incidents relating to individuals.

### 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
<b><u>1. Storage of Data</u></b>	If released could cause harm and distress to individuals	Could be accessed or hacked if not secure.	Could contravene legislation, such as the Data Protection Act (1998).
<b><u>2. Release of Data</u></b>	If released could cause harm and distress to individuals	Person(s) accessing the data and using it for unauthorised means.	Could contravene legislation such as the Data Protection Act (1998).
<b><u>3. Misuse of Data</u></b>	If released could cause harm and distress to individuals	Person(s) accessing the data and using it for unauthorised means.	Could contravene legislation, such as the Data Protection Act (1998).



#### 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?
Could be accessed or hacked if not secure.	Data to be stored on secure servers, which are confirmed as secure following penetration testing and acceptable under DCC policy during the due diligence process. Data is only stored for timespans in line with DCC requirements and compliance with Data Protection legislation.	Risk is reduced	Measures carried out are as far as is reasonably practical. Situation monitored via DCC contract management review and operational review process

Person(s) accessing the data and using it for unauthorised means.	All staff who have access to the data are DBS checked. Secure storage of data complies with Audit requirements as part of due diligence process and all access to the data requires password protection in line with DCC requirements and all access produces an audit trail for additional security.	Risk is reduced	Measures carried out are as far as is reasonably practical. Situation monitored via DCC contract management review and operational review process
---	---	-----------------	---

**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
Could be accessed or hacked if not secure.	Data to be stored on secure servers, which are confirmed as secure following penetration testing and acceptable under DCC policy during the due diligence process. Data is only stored for timespans in line with DCC requirements and compliance with Data Protection legislation.	
Person(s) accessing the data and using it for unauthorised means.	All staff who have access to the data are DBS checked. Secure storage of data complies with Audit requirements as part of due diligence process and all access to the data requires password protection in line with DCC requirements and all access produces an audit trail for additional security.	As 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
Project team to review PIA outcomes and ensure implementation plan reflects the approved solutions.	Expected to be by the implementation of the system	Project Team Situation monitored via DCC contract management review and operational review process

Contact point for future privacy concerns

DCC administrators in the first instance, then Information Security Team

## 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? As **part of the enrolment process parents would be informed what data was going to be held by the Provider. Parents sign an agreement to allow this. If not signed then students would not be able to access the provision.**

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? **If signed consent not given then students withdrawn from provision.**

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? **No (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? **We only provide the required data to the provider.**

### **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? **Yes**

How are you ensuring that personal data obtained from individuals or other organisations is accurate? **PIF data is cross referenced with Data held on EDRM and the DCC PSS System.**

### **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?

#### **EDRM storage times:**

70 years – LAC (Looked After Children)

35 years – SEN/EHCP students

25 years – For all other students accessing provision through DCC referral process

**Student data** is stored on supplier's LMS for maximum of 6 months after a student has left the online provision in line with data security requirements of DCC audit team. This provides time for all data to be extracted by DCC and saved securely with EDRM.

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

Data retained by the provider will be contractually required to be deleted from their system by one of their Administrators after 6 months.

### **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? **Yes**

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

### **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? **Yes**

What training and instructions are necessary to ensure that staff know how to operate a new system securely? **The Contract requirement is that 4 DCC Administrators are fully trained to enter data and use the provider's LMS.**

### **Principle 8**

**Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or 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**

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/>