15 November 2017

Data Exchange
'Send Data to DfE Service'

Privacy Impact Assessment Report

Data Exchange Project Team

Department for Education

1. ORGANISATION

1.1 Project/Policy/Process/Proposal Name

Data Exchange – ‘Send data to DfE’ service

1.2 Directorate

Data Group

1.3 Division

Data Modernisation Division

1.4 Team

Data Exchange

1.5 Senior Responsible Officer (SRO)

Deputy Director, Data Modernisation Division

Step one: Identify the need for a PIA

Purpose/Objectives of the Project/Policy/Process

Data is vital to the department achieving its overall vision of improving educational outcomes. Readily available, timely and good quality data will give better insight into the education system and allow us to make better policies and take effective decisions.

Across DfE and its agencies, the mechanisms and supporting processes which we provide for data suppliers to send data to us have remained unchanged for several years. There are over 70 data collections that come in through different routes.

During the Teacher Workload Challenge Survey, 45,000 teachers told us unnecessary data collections significantly increase their workload burden. Modernising technologies is the only way to marry up the reduction in burden with competing demands for more ready access to data to improve decision making and drive up quality of provision

The Data Exchange (DEx) project aims to:

- provide modern, flexible and secure ways of moving data from data providers into DfE and enable others to improve local data sharing
- deliver solutions that are workable for both DfE and system suppliers to schools, colleges, local authorities (LAs) and other data providers
- reduce the human effort associated with validating and moving data, and allow data to move more frequently where there is value in doing so, to support decision making at all levels

Statutory or other justification (If statutory, please insert citation and a brief summary/Explanatory Notes).

N/A

Business Case – Please outline the business case justifying the particular policy or project

The effort associated with current data collection processes is intensive meaning we can only request data periodically and as such, our business processes are developed around rare snapshots of data.

Change is needed to reduce the burden on our data providers, support the sector through the provision of better, more timely benchmarking information, improve the Department's evidence base to enable more effective policy making and spot warning signs more readily. For example:

- We are slow to understand the pressures in the workforce as we only request school workforce data annually.

- Our analysis and publications can lose impact because they are slow to be released.

DfE is slow to capture and process data. Without providing 'rough and ready' data returns (for example, "what are my key stage 1 results compared with others who have submitted so far?") we can't enable the sector to make quicker, better decisions. This also means governing bodies don't always have the data they need at the time in the annual cycle when they are setting school priorities.

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.

From our ongoing user research, we know we need to address the following pain points:

- data is not always of good enough quality when it first moves
- collecting and validating data takes too long
- data does not enable early detection of issues or quick decision making
- inconsistencies between data in school systems and DfE systems
- feedback and reports from data take too long to be of maximum use

Our 'Send data to DfE' service will provide a common, single data collection interface and enable data to be provided to the department via an application programme interface (API), web form or bulk file.

During the Beta phase, we will deliver a method for on-going data validation to help reduce the pressure on schools when data is gathered, provide an API for schools to return census data and show how school leaders could see their data set in context.

Whilst the department recognises that data collection needs to be simplified, designing a solution that meets the needs of all education providers will not be easy. We are using Agile delivery methodology to build and learn iteratively. Of course, all new solutions will need to demonstrate extremely high security standards prior to implementation.

Summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The Data Exchange (DEx) project will modernise the way that data is collected by the department. The need for a PIA was identified to ensure our new service maintains the security needed for collecting, moving and holding pupil level and sensitive data and complies with the Data Protection Act and General Data Protection Regulation.

During private beta we will work with a small number of volunteer schools who will be required to update their privacy notices, explaining to pupils and staff that their data will be shared with the department as part of the DEx project.
As the DEx progresses and we expand the data collected using the service we will update our impact assessment to ensure it takes account of the scaling up of the new service.

Provide details of any previous PIA or other form of new personal data compliance assessment done on this or any related initiative (You may attach the report as an annex if this helps)

This is the only PIA – it is kept 'current' and will be refreshed as the project matures.

Privacy Impact Assessment – Screening Questions

The first step is to identify the need for a PIA.

- Organisations can identify the need for a PIA using their normal project management process.
- The need might arise during discussions with IT Group or DSU colleagues.
- The following screening questions are designed to help business units identify when a PIA is needed and can be used by project managers or other staff who are not experts in privacy matters or data protection.
- PIRAS will provide support and guidance throughout your PIA journey from these screening questions to the completed PIA report.

Business units should consider incorporating the screening questions into their own project and risk methodologies or procedures from the outset. They can give preliminary answers to the questions at an early stage of the project and these can be expanded upon as the work develops. The following question set is designed to help decide whether and what scale of PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise.

The screening questions can be used by project managers or other staff who are not experts in data protection or privacy matters to identify privacy risks and the need for a PIA as part of normal project management procedures. Some aspects of the PIA clearly require more detailed input from specialists within the Department (such as security or technology colleagues where necessary.

No two projects will be alike. However, the screening questions have been generically drafted in order to assess any outlying privacy risk. The most important thing is that the Department has some mechanism within their project and programme management toolkit for identifying the need for a PIA.

At this early stage a business unit should be able to identify why they are planning the project and what they intend to achieve and consider whether the impact on privacy is necessary and proportionate to the anticipated outcomes.

After answering the screening questions PIRAS might advise that the project does not require a formal PIA because there will be a minimal impact on privacy. In these cases it will still be useful to retain a record of the screening question answers so that they can be referred to in future if necessary.

Even if a substantial PIA is not necessary, a business unit should still consider conducting a legal compliance check against the Data Protection Act 1998.

Once the need for PIA has been established, it is important that senior management, including the Senior Information Risk Owner are engaged. Securing this at an early stage is an important factor in ensuring the PIA is effective.

Facing facts early

The key characteristics addressed here represent significant risk factors for the project and their seriousness should not be downplayed. It should also be remembered that the later the problems are addressed, the higher the costs will be to overcome them.

Perspectives to consider

It is important to appreciate that the various stakeholder groups may have different perspectives on these factors. If the analysis is undertaken solely from the viewpoint of the department itself, it is likely that risks will be overlooked. It is therefore recommended that stakeholder perspectives are always considered as each question is answered.

In relation to the individuals affected by the project, the focus needs to be more precise than simply citizens or residents generally, or the population as a whole. In order to ensure a full understanding of the various segments of the population that have an interest in, or are affected by, the project, the stakeholder analysis that was undertaken as part of the preparation step may need to be refined. For example, there are often differential impacts and implications for people living in remote locations, for the educationally disadvantaged, for itinerants, for people whose first language is not English, and for ethnic and religious minorities.

Applying the criteria

The screening question set needs to be considered as a whole; in order to determine what scale of PIA is warranted - whether to be wide-ranging, or focused on particular elements of the project.

Where the answers to questions are “Yes”, consideration should be given to the extent of the privacy impact and the resulting project risk. The greater the significance; the more likely that a full-scale PIA is warranted.

If only one or two aspects give rise to privacy concerns, a small-scale PIA may be justified. In these circumstances the PIA process should be designed to focus on the areas of concern. If, on the other hand, multiple questions are answered “Yes”, a more comprehensive assessment is appropriate.

Data Exchange PIA Screening Questions

1 Is the rationale of policy for this new project/proposal unpublished, unclear or unknown to the data subjects concerned (including the general public)?

YES

NO

If you are relying on legislation to implement your proposal, please list the legislation, act or regulations:

The department currently runs over 70 data collections a year (censuses, surveys, financial returns, and so on). Education data providers often have to submit the same data several times in the same year. This involves numerous purpose-built systems, each with their own logins and different user experiences. We know from the Workload Challenge Survey and our user research that this adds to teachers' workload and diverts resources from other work.

The rationale for Data Exchange (DEx) is based on the need to modernise the way the department receives and uses education data.

As the project has developed, we have publicised our progress at various conferences with schools, local authorities (LAs), multi academy trusts (MATs), suppliers of school and further education (FE) information systems. Additionally, we have worked directly with schools and suppliers as part of our user research to get their feedback on current systems, the potential solution and test what's being developed.

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act and the General Data Protection Regulation. We will also require establishments involved in the project to update their privacy notice to explain to pupils and staff that their data will be shared with the department as part of the DEx project.

All education providers have a duty, under Section 537A of the Education Act 1996, to provide pupil level data to the department. The Education (Information about Individual Pupils) (England) Regulations details the data items the department can collect. DEx will use the same legislation to collect pupil level data. During the private beta phase DEx will work with suppliers and volunteer schools to trial an application programme interface (API) mechanism to send school census data directly to the department from their management information system (MIS). This will run alongside the existing school census collection through the COLLECT system.

In short, the initial beta phase will focus on changing the method of collection, rather than what data is collected.

When and how do you propose to publicise this new proposal?

The project has already engaged with schools, local authorities (LAs) and software providers for schools and FE colleges to make them aware of this project in an appropriate way, relative to the stage it is at. We're aiming to strike the right balance between getting a good mix of schools interested and shaping the future, but not 'overselling' with heavy communications to schools, as new solutions could still be some way off, and the exact nature of the solutions may still change. As we move through Beta and timescales for the change, and what the changes involve for schools, we will also provide regular updates on the DfE Digital blog, as well as the department's social media accounts. All the information needed to use DEx will be publicly available on GOV.UK

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

YES

NO

Please describe the new purpose or way the information is to be used

We're collecting the same data for the same purposes as the department currently does, we will just be capturing data in a new way. We will trial the use of APIs during the private beta phase of the project, using an open data specification to move data more frequently from the sector into DfE. Data providers will continue to manage their data in their systems, and the DEx service, 'Send data to DfE', will move the data securely, according to agreed schedules. After this private beta phase, the system will be extended to cover more of the department's data collections.

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

YES

NO

Please list the personal data fields to be collected and indicate those fields that are new to this project/proposal

In the private beta stage, no personal data will be moved that is not currently collected. Should this change, our PIA will be updated to take account of the changes to data items to be collected.

4 Will the information about individuals be of a kind particularly likely to raise privacy concerns or expectations? (For example, health records, criminal records or other private information)

YES

NO

Please explain what type of privacy concerns or expectations you anticipate and how likely these may be raised

As Data Exchange (DEx) will be capturing the same pupil level data that education providers already provide to the department, it should not create any new privacy concerns or expectations. Privacy concerns/expectations are already high in existing processes, and ensuring data moves appropriately and securely is a key aspect of the change work. During private beta the project will work with a Security and Information Risk Advisor (SIRA) to identify any technical security issues for the proposed new service. The service will also be subject to regular IT health checks. We will also work to ensure the project complies with all relevant legislation, including the Data Protection Act and General Data Protection Regulation. Any privacy risks identified will reviewed regularly by the project and managed via the project risks, assumptions, issues and dependencies (RAID) log. Cross cutting privacy risks are currently being managed at a directorate level by the project SRO.

5 Will the project involve handling a significant amount of data about individuals, or a large population/group size?

YES

NO

Please describe in what way this is significant/large:

Ultimately, the intention of DEx is to have the potential to provide the means for all required data to be sent to DfE. The amount of data DEx could eventually be bringing in could be 2 to 3 terabytes per year. However, in the private beta stage, it will be a small number of schools for a few thousands pupils.

To ensure the security of any data held the project will be working with a SIRA. The role of the advisor will be to ensure DEx complies with the department's policies regarding the protection of data.

6 Will the proposal involve any contact or engagement or other processes that individuals may find onerous or intrusive?

YES

NO

Please describe these processes:

Once established DEx will be less burdensome for data providers than the current process, which involves using multiple systems for over 70 different data collections. We are working with our users to ensure our services will meet their needs in simple and intuitive ways.

In what ways might individuals find these onerous or intrusive?

7 Will the project compel individuals to provide information about themselves or collect personal information without explicit consent?

YES

NO

Please list the information that needs to be provided

The collection of school and pupil data is a legislative requirement and schools do not need the further consent of parents or pupils to collect and provide this information to the DfE. That is the legal status now, and will be the conditions relied upon by any new transport provided by the Data Exchange (DEx) project. So, whilst data collections do compel individuals to provide information about themselves, it is not the project that compels people. People are compelled to provide it, and the project provides a more modern way to achieve it. However, education providers involved in the testing of the new service will be required to update their privacy notice, to explain to pupils and staff that their data will be shared with the department as part of the DEx project.

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

YES

NO

Please list what decisions or actions arise from this project/proposal

As this project has the potential to improve the regularity of data received along with data quality, this has potential to improve:

- Evidence based planning and decision making at all levels within the sector including DfE
- Monitor development and be more responsive, with a greater understanding of 'in year' trends.
- Understand and unpick issues that can create school funding issues (for example duplicate pupil resolution).

The private beta stage is unlikely to impact individuals any differently to current data collections that the department runs. Any changes will result in the review of our current PIA.

Please list how these decisions or actions arise

Please list the possible impacts/effect of these decisions or actions and how likely these may be

9 Does the project involve new or significantly changed data handling processes for the personal data concerned?

YES

NO

Please describe how the processes are new or changed:

The only change to data handling processes during private beta will be for the data providers testing this new service using APIs to transfer data to the department. They will also continue to upload and submit their data using the department's existing data collection system (COLLECT). Dual running of both systems will allow the project to check that the DEx technology works, whilst also comparing the data received to ensure it is consistent. The long term aim of the project is to create a single route for sending data into DfE, replacing the current processes required for the 70+ collections. If the new collections require new data handling methods the PIA will factor this in when it is updated.

10 Does the project involve new technology that might be perceived as being privacy intrusive? (For example, CCTV, biometrics, facial recognition.,,)

YES

NO

Please list the new technology and how it is to be applied

11 Does the proposal involve multiple organisations, whether they are public or private sector organisations, as delivery agents or business partners?

YES

NO

Please list the other parties and why/how they are involved:

DEx will modernise the flow of data from data providers. Schools, MATs, LAs, suppliers of school systems are all involved. During the private beta stage, we will work with a small number of volunteer suppliers and data providers to ensure the evolving service meets their needs in a simple and intuitive way.

12 Will the project involve new or changed linkage of personal data with data held in other collections or new consolidation, cross-referencing or matching of data from multiple sources?

YES

NO

Please list the other data collections/sources and the reasons for the linkage, use:

During the private beta stage, data will be linked and matched in the same way as current systems and processes.

13 Will information about individuals be disclosed to organisations or people who have not previously had access to this information, including where the information was previously anonymised?

YES

NO

Please list the newly disclosed information

DEx will ensure that organisations can't receive data without permission. During private beta all organisations will send data to the DfE via their own suppliers, which mirrors the existing access arrangements.

14 Will the project involve new or changed data security arrangements that may be unclear, unspecified or in variance to HMG standards? (please consult with the Department's Security Unit (DSU) if unsure)

YES

NO

Briefly describe the security arrangements and how these might be unclear, unspecified or in variance to HMG standards:

A SIRA consultant will support the project through its development phase.

From design work so far, it is anticipated that access to the service will be via a registration process on GOV.UK. Suppliers will need to register with the DEx service and then request permission to use an API and test it with us. We will then issue a 'token' saying that their product is fit for purpose.

We will work out the best way for data providers and suppliers to register and request permission to send data to us during private beta. User research and implementation of the architecture will inform the design.

We will also look at whether security arrangements will differ to those currently in place throughout the development and review our PIA once private beta stage is underway.

15 Will the project involve data processing which is in any way exempt from legislative or common law privacy protections??

YES

NO

In what way is the processing considered exempt?

16 Will the project involve new or changed data retention arrangements that may be unclear, unspecified or extensive?

YES

NO

Please describe the proposed data retention schedule:

RAG analysis-1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	=
+C																	10
+Q																	3
+R																	3

Key

RAG		***Definition***	#
	+C	C=Comment	
	+Q	Q=Question	
	+R	R=Recommendation	
	Red	Requires substantial action	
	Amber	Further clarification/action required	
	Amb/Grn	Minor points/clarification/action required	
	Green	Closed - No issues/clarification required	

Conclusions

A summary of the conclusions from the Data Protection Principles Compliance Check. This could include indicating whether some changes or refinements to the project have been agreed (see Mitigating Design Features above

Privacy Justification (The justification for the features that give rise to significant impact upon individuals where these exist)

This part of the PIA should contain a clear and well-argued case for the project as a whole, and particularly for those features that have greatest potential for significant negative impacts on data subjects. It will also help identify and examine risks incurred as a result of the proposal.

Additional details may be needed in the case of projects involving new technologies eg. smartcards, locator technologies and biometrics.)

Annex

Space for supporting project materials