Department for Education

Alternative Provision Census Data Protection Impact Assessment: Public Summary

Version 1.0

April 2019

1. The purpose and aims of the Alternative Provision Census.	
The Alternative Provision (AP) census has been in place since 2008. It is statutory (annual) data collection from local authorities to the Department for Education (DfE). It provides data on individual pupil records for pupils with a local authority commissioned (and funded) alternative provision placement. It is the DfE's primary source of data about children of compulsory school age unable to receive suitable education within mainstream education because of illness, exclusion or for any other reason, where local authorities have a duty to provide an appropriate alternative provision. The evidence and data provides a clear picture of how the AP system is working in order to better target (and evaluate) policy interventions to support these vulnerable children and support decisions (for example, through approval of future free schools) about the level of need for specialist AP provision in certain parts of the country.	
2. Details of the role of any data processor, suppliers or contractors if used.	None used.
3. Details of any data transfer to or from any organisation, and or data sharing.	Local authorities submit AP Census data to DfE via "COLLECT"; a secure restricted access DfE data collection system. AP Census data is securely transferred from COLLECT internally to the National Pupil Database and the Pupil Data Repository. Data is only shared where it is lawful, secure and ethical to do so. All sharing of individual data from the AP census is robustly governed by the DfE Data Sharing Approval Panel (covered within the NPD DPIA). See link below for full details of DfE data sharing: https://www.gov.uk/government/publications/dfe-external-data-shares
4. Is this a change to an existing or previous DfE initiative?	No
5. Which of DfE's functions does this initiative support?	▪ Helping disadvantaged children and young people to achieve more. ▪ Making sure that local services protect and support children

About the scale and nature of processing

6. How many individuals will be having their personal data processed?	Approximately 26k pupils annually.
7. What categories of personal data will be processed?	▪ Identifiers (e.g. name, address, UPN) ▪ Characteristics (e.g. ethnicity, FSM eligibility) ▪ Placement / enrolment details (e.g. establishment, start date, attendance pattern, reason for placement) ▪ Special educational needs See link below for full details published on GOV.UK within the data collection guidance: https://www.gov.uk/guidance/alternative-provision-census#census-documents
8. What is the lawful basis for processing the personal data?	**GDPR Article 6(1)(e) Public task**; the processing is necessary to perform a task in the public interest or for DfE's official functions, and the task or function has a clear basis in law.
9. What personal data of a sensitive or highly personal nature will be processed?	1. Ethnicity, 2. Health - alternative provision reason, type of special educational need.
10. What is the lawful basis for processing special category personal data?	**GDPR Article 9(2)(j);** processing is necessary for archiving in the public interest, scientific, or historical research or statistical purposes.
11. Is the personal data of vulnerable individuals processed?	Yes, vulnerable children.
12. Is new, innovative or unusual technology used to process personal data, including cookies or similar technologies in collecting or other processing of data?	No
13. Does processing personal data involve automated decision-making?	No
14. Does processing personal data involve profiling individuals?	No

Data Protection Summary

The minimum amount of personal data necessary to achieve the objectives is being used.
The lawful basis for processing personal data and Special Category data, has been identified and recorded.
The processes are in place to extract all the personal data relating to a single individual on request to respond to a Subject Access Request.
The processes are in place to address all individual rights of the data subject.
There is a data retention period for this dataset. Data is collected, and processed, for research and statistical purposes in the public interest to promote the education and well-being of children in England. Data is retained for an indefinite period whilst ongoing reviews determine the data remains necessary for the purposes for which it was originally collected
Internal security measure are in place to ensure only those people who have a need to access the personal data can do so. Personal data is processed securely using appropriate technical and organisational measures in line with the “security principle”.
This DPIA will be reviewed in six months (30th November 2019) and then annually.

Data Protection Risk Summary

These risks summarise the top risks identified at the time of publication of this DPIA summary. (Publication 31st May 2019).

This DPIA and risk summary will be reviewed by 30th November 2019.

Risk	Impact	Mitigations
1. The department is prevented from collecting personal information as we are not as transparent as we could be.	Individuals may be reluctant to share their personal information with the department as they do not understand what their information may be used for. This may impact on the department's ability to develop and implement new initiatives to achieve its objectives. Data subjects may not be aware that their personal data may be shared with other organisations.	Annual review of all privacy notices. Gap analysis of existing privacy notices Privacy notice requirements built into DPIA process. Data Governance improvements implements improved controls and support transparency. Approvals for any data sharing must be given by the Data Sharing Approvals Panel (DSAP). The department publishes data sets explaining how and why we process personal information.
2. The scope of use of personal information is not restricted due to insufficient governance controls.	Personal information may be used for a purpose the individual is unaware of. Local Authorities, schools and others are unaware of this additional use and are vulnerable as a result. Individuals and organisations may be reluctant to share their personal information with the department negatively impacting on future initiatives.	Improved Data Governance within the department including the DSAP, enhanced DPIA process and governance escalation to the Data Protection Board and the DPO. Data mapping will identify all data sets held and identify the lawful basis for processing enabling purpose limitation controls. The department publishes data sets explaining how and why we process personal information.
3. Personal information will be held for longer than is necessary.	Personal information will not be deleted in line with retention schedules and policies, in potential breach of data protection legislation. The data subject will be unaware that we are still processing their personal information. If the data subject becomes aware, they may be reluctant to share their personal information in future with the department.	Improved Data Governance including DSAP and the Retention Review Board will implement better controls. The DPIA process requires data retention policies and schedules to be implemented.

Risk	Impact	Mitigations
4. Vulnerable children may be more easily identified.	The data subject could be more easily identified due to the small data set. This could have an adverse impact on a vulnerable child.	Improved data governance controls, DSAP and improved DPIA process identifying and mitigating the impact on the individual.
5. The department may inadvertently breach the data protection principles.	The department may inadvertently breach the data protection principles as a whole due to work processes that are still maturing. Potentially impacting individuals and their information rights.	Planned data protection awareness training for all staff on their responsibilities. Planned data governance implementation including education.
6. There is a risk that the data within [name of system] may be targeted and extracted by external organisations who wish to exploit it for financial or security gains.	A data breach may occur that impacts on the data subject and the department.	The system is protected with cyber security controls which are appropriate for the OFFICIAL data as outlined by the Cabinet Office and the National Cyber Security Centre The system is regularly pen tested by certified testers to ensure that any weaknesses in the system are identified quickly and rectified The network and servers which host the system are regularly patched The system has separate roles and responsibilities so that access to data is limited only to that data which is necessary to undertake agreed processing