



Department
for Education

Data linking and security

**Information for parents and guardians of Our
Future study participants**

February 2014

Contents

Linking the National Pupil Database (NPD) to survey responses	3
Information required from you to enable data linkage	4
Data linkage will continue as long as your child continues in the survey and you have consented to it	4
You can change your mind on data linkage and may withdraw your consent at any time	4
Accessing copies of the survey and NPD data	5
Survey and NPD data is kept in accordance with the Data Protection Act	5
Information is kept and stored securely	5
Protecting privacy	5
Linked data are used in many ways	6
Reasons for linking education records to survey responses	6
Responsibility for data linkage	6
Data will not be sold	7
Leaving the study or moving house	7
Further information	7
Data security	8
Trust in use of your data	8
Contractors security procedures (TNS-BMRB and GfK NOP)	9
Holding and transferring data	10

Linking the National Pupil Database (NPD) to survey responses

The National Pupil Database (NPD) is a longitudinal database linking pupil and student characteristics and attainment information for all children in maintained schools in England. It holds pupil and school characteristics, (for example, age, gender, ethnicity, attendance and exclusions matched to pupil level attainment data) collected from schools and local authorities by the Department for Education and awarding bodies and is the source of the data published in the performance tables. Other data on further education, higher education, looked after children and children in need is also held in the NPD.

Information from the NPD can be linked in to your survey responses such as:

- the schools your child has attended
- the courses studied and the qualifications gained
- attendance
- suspensions or exclusion
- whether your child has a special educational need
- whether your child has ever been eligible for free school meals.

Some information contained in the NPD comes from the School Census. The School Census provided information including:

- pupil identifiers (gender, age, year and month of birth, academic year group)
- school identifiers (local authority, school establishment number, school type)
- pupil characteristics (ethnic group, language group, free school meals eligibility, gifted and talented indicator, special educational needs status, type of disability)
- pupils' attendance and exclusions details
- post-16 learning aims.

The NPD also contains attainment information such as the Early Years Foundation Stage Profile and Key Stages 1-5 results. We may also add in details about the local areas where the schools are, such as local employment information or the geographical boundaries which are available from the NPD.

The information that is available about your child in the NPD depends on the school he or she attends or has attended. The only information available for linking if your child attends an independent school will be examination results.

Information required from you to enable data linkage

If you agree to the Department for Education adding these details from your child's NPD records, you will be asked to agree to consent at the interview. You will also be asked to confirm your child's full name, date of birth, address and details of their current school. This will allow TNS-BMRB to provide the necessary details to the DfE to enable them to identify and then add in the information.

Data linkage will continue as long as your child continues in the survey and you have consented to it

Information from the NPD will be added to survey information for as long as your child is involved in the study, providing you agree to it. As soon as your child reaches age 16 we will approach them for their consent rather than a parent or guardian.

This is because the information has an incredibly long 'shelf life' with many researchers likely to be interested in it for many years to come. For example, researchers and analysts still regularly use the data collected from a birth cohort study which is following a group who were born in 1946.

You can change your mind on data linkage and may withdraw your consent at any time

The decision to have your child's education records linked into survey responses is entirely voluntary and you may change your mind at any time. If you do, you need to contact TNS BMRB on 0800 015 4492 or emailing ourfuture@tns-bmr.co.uk.

Withdrawing your consent will not affect any services which you have or may receive from the Department for Education in the future. The anonymised education records which will have already been linked to your survey responses will be kept and used for research and statistical purposes, however we would not link in any future information.

We will remind you of any previous consent you may have given during future interviews and check that you are still happy for this to happen. When your child turns 16 we will ask him or her for their consent directly.

If, for any reason, you are unable to take part in the study, and are therefore unable to 'renew' your consent, future education information linking from the National Pupil Database would stop. No new information from your education record would be added in to your child's survey responses. However, all information which had been linked in up to that point would be kept and used for research and statistical purposes.

If for some reason we are unable to contact you then (and therefore cannot get your consent) we will stop adding in this information.

Accessing copies of the survey and NPD data

You are unable to see copies of the survey and NPD data which we use for research purposes, this is because before we release them to be used, we remove as much of the identifying information as we can, which means we are unable to identify your records.

Survey and NPD data is kept in accordance with the Data Protection Act

The survey and NPD data will be kept indefinitely for the purpose of research and statistics. This is in accordance with Section 33 (3) of the Data Protection Act.

Information is kept and stored securely

Your personal information will be kept securely at all times. Before it is released to be used for research and statistical purposes we will remove as much of the identifying information as we can, so the record is anonymised. This information will then be shared with researchers and analysts via secure mechanisms.

Analysts and researchers are conducting education-related research will be able to securely access the data. In the reports produced by this research no individual or group of individuals will be identified.

Protecting privacy

Your privacy is really important to us. The data which we will collect during the survey and any data which we are able to add in from the Department's administrative records will be kept secure at all times. Data will never be published which could identify you or your child.

TNS BMRB, GfK NOP, and the longitudinal surveys team at the Department for Education will have access to your personal information and will keep it secure at all times. They work to very high security standards including ISO27001 and in accordance with the Data Protection Act.

Like your survey responses, your child's anonymised education information will be used by academics and social policy researchers for non-commercial research and statistical purposes. Analysts in government departments will also make use of the anonymised information to help inform future policies.

Any sensitive information such as detailed disability status would be made available to researchers and analysts under strict access arrangements to ensure the information is used responsibly and safely. Names and addresses are never included in the results and no individual can be identified.

All researchers and analysts who use the linked survey and education information must comply with the laws in their country regarding privacy. All countries in the EEA have legislation which is equivalent to the EU Data Protection Directive. Linked education information taken from the National Pupil Database will not be released to anyone outside the EEA. For the UK, the law that applies is the Data Protection Act 1998. More information about your rights under the Data Protection Act can be found on the website of the Information Commissioner's Office's website. http://www.ico.gov.uk/for_the_public

Linked data are used in many ways

The information produced by linking education records to the survey responses has a very wide range of uses for researchers and analysts to help them better understand our lives and behaviours. For example, in the future it could be used to look at the influence that going to a new academy school has on a young person's life chances; or it could be used to study young people who don't do so well at school, to understand the role that education has had on their lives to see where we need to improve policies and services for the future.

We expect many studies will be published that use this data and when they are, details will be placed on the Our Future web pages so you can find out more about how your data is influencing policy.

Reasons for linking education records to survey responses

Government departments and agencies collect a range of information about all of us for administrative purposes, so they can plan and provide services. While we can learn about people's lives, experiences, behaviours and beliefs by asking direct questions, it can sometimes be quicker and easier to obtain some of this information directly from the government departments which hold them. This is the case for the educational records which are held by DfE.

By linking to information held by DfE on education in England, your survey interview is shorter and the information that will be added in will allow researchers to do wider ranging analyses with the information which is extremely useful for future policy development.

By linking to records which already exist, we are making much better use of them as well as reducing the length of your interview.

Responsibility for data linkage

DfE will be responsible for adding in the education records to your survey data. It will ensure that your information will be kept secure. Under the Data Protection Act 1998, DfE

and its contractors have legal obligations towards you in the way that it deals with information collected from you. DfE uses leading technologies and encryption software to safeguard your information, and keep strict security standards to prevent any unauthorised access to it.

DfE does not pass on your details to any third party or government department unless you give permission to do so, or DfE is obliged or permitted by law to disclose it.

Data will not be sold

Your details will never be sold by the Department for Education or its contractors to be used for marketing or commercial purposes. In addition, researchers and analysts who use your education information will have to agree never to use them for commercial purposes as one of their conditions of access.

Leaving the study or moving house

We will only continue to link in your child's education information from the National Pupil Database if we have your permission to do so. If we are unable to get this permission from you we will stop any future linkages. However we would retain previous linked information to be used for research and statistical purposes.

Further information

For further information about adding education records to the survey please contact ourfuture.study@education.gsi.gov.uk

If you have any concerns about how your personal information is being stored, handled or used as part of this survey, please contact the study team at TNS-BMRB on 0800 015 4492 or emailing ourfuture@tns-bmr.co.uk in the first instance.

You may also contact the Department for Education's study manager, via ourfuture.study@education.gsi.gov.uk.

Alternatively you can contact the Information Commissioner's Office at:

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Tel: 0303 123 1113

Fax: 01625 524510

Website: <http://www.ico.gov.uk>

Data security

Trust in use of your data

The Department for Education is committed to maintaining the confidentiality of the data it receives, stores, processes and disseminates. We are committed to protecting confidentiality to:

- maintain the trust and co-operation of those who own and manage administrative data sources used by us and respondents to our surveys.
- comply with the relevant legislation, including the Data Protection Act 1998.
- comply with Principle 5 of the Code of Practice for Official Statistics, which states that: “Private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only”.

Our arrangements for protecting confidentiality fall into the following three areas:

Personnel - All staff who work with data about individual persons, e.g. pupils in schools, receive appropriate security checks and training in protecting information. Secure working areas are provided for staff who work with confidential data about individual persons.

Data - Our arrangements for protecting private information about individual persons include:

- providing detailed data security operational guidance for our staff;
- using secure data transfer methods to transfer data to and from external bodies such as local authorities;
- contracts with external organisations include data security clauses where appropriate;
- external bodies who wish to access our data are required to complete a confidentiality agreement. Where the agreement is approved by the head of profession for statistics, only the minimum data needed for the specified purpose are released;
- service level agreements when sharing data with internal users and other governmental groups.
- respondents to our data collection exercises receive privacy notices detailing what the data will be used for and our undertakings with respect to confidentiality;

- raw data cannot be downloaded from our systems;
- raw data cannot be downloaded onto CDs, through USB ports, to laptops etc.

Statistical disclosure control - We identify three types of disclosure risk in relation to the data about individual persons or the statistics derived from the data:

- **Identity:** If a person or persons can be identified (by either the persons themselves or someone else) then there is an identity disclosure risk.
- **Attribute:** If confidential information about a person or group of persons is revealed and can be attributed to the person or each person in the group then there is an attribute disclosure risk.
- **Residual:** If outputs from the same source or from different sources or databases can be combined to reveal information about a person or group of persons then there is a residual disclosure risk.

Contractors security procedures (TNS-BMRB and GfK NOP)

TNS-BMRB is compliant with and certified to the international Information Security Management Standard ISO 27001:2005 (certificate number: 0498).

TNS-BMRB is compliant with the 1998 Data Protection Act (TNS BMRB registration number: Z8211155). It also abides by professional codes of conduct established by the Market Research Society and Social Research Association, to ensure that all data are kept strictly confidential.

The key aspects of TNS-BMRB's data security policy are summarised below.

TNS-BMRB's ISO 27001 system is fully transparent and they are happy to allow access to their information security manual, detailed procedures and working practices, risk management handbook and processes, and training materials to external auditors and/or authorised visitors upon a signed confidentiality agreement.

GfK NOP operates to similar standards and guidelines. GfK NOP will also be required to sign a partnership agreement with TNS BMRB covering data security guidelines.

Physical access to the TNS-BMRB building and server/communications room is restricted to individuals who require such access to perform their job responsibilities.

TNS-BMRB check employment history for five years and for senior hires (director and above) they conduct background screening using a WPP supplier.

All staff members receive specific security training, which is tailored to their role and responsibilities, and regular cycles of internal security audits are conducted feeding into their continuous improvements.

How do I know interviewers will keep young people's details safe?

Interviewers are required to undertake comprehensive training which includes an understanding of the MRS Code of Conduct and the Data Protection Act. All personnel working on the survey have appropriate security checks.

Before starting work interviewers are required to inform the local police that they are working in the area. The local police will stamp a form to confirm that they have been informed. The interviewers will be able to show you a copy of this form if required.

Interviewers are all required to carry ID cards verifying that the organisation is a member of the Market Research Society. Interviewers will show you this on the doorstep. The card will include a freephone number which you can call should you wish to verify the identity of the interviewer.

Interviewer's laptops are FIPS 140-2 encrypted so that all the files are protected at all times and can only be accessed by interviewers.

Holding and transferring data

TNS BMRB uses Accellion File Transfer System to securely transfer confidential datasets or any other restricted data, including respondents' personal data. Secure file transfer system architecture integrates into existing infrastructure rather than duplicate existing systems. The system is:

- suitable for secure ad hoc file delivery;
- incorporates login security to ensure identity of sender and recipients;
- uses SSL (Secure Socket Layer) to securely encrypt the transport layer of delivery; and
- provides an audit trail.

Removable media is not used to store personal data. If transfer of personal data is required, it is transferred by Accellion File Transfer or as DfE requests. When data are transmitted to face-to-face interviewers to enable them to undertake interviews, the identifying data are always held separately from the interview data. All data are password encrypted (with the exception of the individual case open at the time of interview).



Department
for Education

© Crown copyright 2014

You may re-use this document/publication (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v2.0. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2 or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at www.education.gov.uk/contactus.

This document is available for download at www.gov.uk/government/publications.

Reference: DFE-00052-2014