Department for Education

Data Linking and Security Information for Our Future study participants and their parents and guardians

November 2016

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

Some information contained in the NPD comes from the School Census. The School Census provides 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.

Published: November 2016

The information that is available about you in the NPD depends on the school you attend or have attended. The only information available for linking if you attend an independent school will be examination results and some characteristics about your school.

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.

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.

Linking to other sources of data

In addition to asking about linking to the National Pupil Database, we ask for your permission to add information about you from administrative records held by a number of other organisations, government departments and agencies, to the information that we collect throughout the study.

Adding details from these existing records will greatly increase the value of the information you give us, as it will help us to build a more detailed picture of what life is like for people your age. This opens up new possibilities for researchers from universities, charities and within government who all use the Our Future data to understand the experiences of people your age and to make the services you use and the places you live better.

If you do kindly give permission, we may pass your name, address, sex and date of birth to the following organisations and government agencies, so that your records can be identified and sent to the Our Future research team to be added to your study information. We will not pass any other survey information to them:

- Department for Business Innovation and Skills' (now part of the Department for Education) Individual Learner Record (includes information about your participation and achievement in further education from age 16, as well as details about the college or training centre you may have attended).

- Her Majesty's Revenue and Customs (HMRC) (includes Income Tax, Tax Credits and Child Benefit data, providing information about employment, earnings, tax, pensions and National Insurance contributions).
- Department for Work and Pensions (includes information about benefit receipt and participation in employment programs).
- National Health Service's (NHS) records maintained by NHS Digital (previously the Health and Social Care Information Centre (HSCIC)) (includes information about use of health services, health conditions and treatments provided. For example, Hospital Episode Statistics include information on admissions, outpatient appointments and A&E attendances at NHS hospitals in England).
- Ministry of Justice (MoJ) (includes information about police cautions and convictions).
- Universities and Colleges Admissions Service (UCAS) (includes information about higher education applications and offers).
- Student Loans Company records (records include information about applications for student finance).
- Higher Education Statistics Agency (HESA) (includes information about university participation and attainment).

The transfer of information that could identify you is always a one-way process. So this means that the Our Future team will only receive information from the organisations and government agencies above for anonymous reporting. All of your information will remain confidential and this means that your name and address will never be included in the results.

If you kindly give permission to link any of the administrative records, your permission will remain valid indefinitely and information from these records will be collected on an ongoing basis, unless you contact the Our Future research team to ask us to stop. You can change or withdraw your permissions at any time by contacting the Our Future research team at Kantar Public Freephone: 0800 015 4492 Email: Ourfuture@kantarpublic.com

Responsibility for data linkage

DfE will be responsible for adding other 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.

Information required from you to enable data linkage

If you agree to the Department for Education adding details from any of these data sources, you will be asked to agree to consent at the interview. You may also be asked to confirm your full name, date of birth, address and details of your current school (if relevant). This will allow Kantar Public to provide the necessary details to the government bodies to enable them to identify and then add in the information.

If you agree to data linkage, information from these data sources will be added to survey information on an ongoing basis, even if you drop out of the survey or we are unable to contact you. We will however, stop linking data if you withdraw your consent for us to do so in writing.

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 records linked into survey responses is entirely voluntary and you may change your mind at any time. If you do, you need to contact Kantar Public on Freephone: 0800 015 4492 Email: Ourfuture@kantarpublic.com

Withdrawing your consent will not affect any services which you have or may receive from the Department for Education in the future. The anonymised 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.

Accessing copies of the survey and NPD data

You are unable to see copies of the survey and linked 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 identifying information, 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.

Kantar Public, GfK, 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 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 https://ico.org.uk/for-the-public/

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

If you agree to data linkage, information from these data sources will be added to survey information on an ongoing basis, even if you drop out of the survey or we are unable to contact you. We will however, stop linking data if you withdraw your consent for us to do so in writing.

Further information

For further information about adding education records to the survey please contact ourfuture.study@education.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 Kantar Public Freephone: 0800 015 4492 Email: Ourfuture@kantarpublic.com in the first instance.

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

Kantar Public is compliant with and certified to the international Information Security Management Standard ISO 27001:2013 (certificate number: IS 570113).

Kantar Public is compliant with the 1998 Data Protection Act (registration number: Z2413668). 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 Kantar Public’s data security policy are summarised below.

Kantar Public's ISO 27001 information security management system is fully documented, detailing procedures and working practices, risk management methodology and training materials.

GfK operates to similar standards and guidelines. GfK has also signed a partnership agreement with Kantar Public covering data security guidelines.

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

Kantar Public 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.

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 with to verify the identity of the interviewer.

Interviewers' laptops are Bitlocker AES encrypted with a 256-bit key, which is the most secure of the bit locker encryptions, so that all the files are protected at all times and can only be accessed by interviewers.

Holding and transferring data

Kantar Public 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).