DATA ACCESS AGREEMENT IN RESPECT OF CONFIDENTIALITY OF DATA PROVIDED BY THE DATA AND STATISTICS DIVISION, DEPARTMENT FOR EDUCATION

1 We understand that confidentiality and security restrictions apply to the individual pupil level data described in the schedule to this agreement and we will consult the Data and Statistics Division (hereafter known as DSD) a Division within the Department for Education (DfE) in writing before taking any step that could put at risk the confidentiality or security of the data.

2 We have read the Statement of Procedures (annexed to this document) adopted by DSD to protect the confidentiality of individual pupil data in a manner commensurate with the Data Protection Act 1998 (DPA) for personal data and relevant HMG Protective Marking and/or Business Impact Level applied. We confirm that in any use we make of the data provided by DSD we will follow these procedures, both in letter and spirit, to the maximum extent that they apply.

3 We will comply at all times with the DPA and shall not perform our obligations under this Agreement in such a way as to cause DfE to breach any of its applicable obligations under the DPA. We understand that for the purposes of the DPA, DfE is the Data Controller and we are the Data Processor. We agree:

3.1 To process personal data only in accordance with instructions from DSD (as set out in this Agreement);

3.2 To process personal data only to the extent, and in such manner, as is necessary;

3.3 To employ appropriate organisational, operational and technological processes and procedures to keep any personal data safe from unauthorised use or access, loss, destruction, theft or disclosure;

3.4 To take reasonable steps to ensure the reliability of any persons who have access to personal data;

3.5 To ensure that all persons required to access personal data are informed of the confidential nature of the data and comply with the obligations set out in this Agreement;

3.6 Not to allow any person(s), not specifically mentioned within this Agreement, access to personal data without the written permission of DSD and where such permission is given to ensure that the other person(s) comply with the obligations set out in this Agreement;

3.7 To ensure that no persons publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by DSD;

3.8 To notify DSD within five working days if we receive a request from a data subject to have access to that person's personal data or a complaint or request relating to DfE's obligations under the DPA;

3.9 To provide DSD with full cooperation and assistance in relation to any such complaint or request made, by: providing full details of the complaint or request; providing any personal data we hold in relation to a data subject and any other information requested by DSD (all within the timescales required by DSD and as set out in the DPA);

3.10 Not to retain any personal data for longer than is necessary within the terms of the schedule to this agreement. When our use of the information supplied to us (together with any extracts or copies of the original data) is complete the data will be

securely deleted[1] from all media on which it has been stored, unless there is agreement with DSD that the data may be retained for longer.

3.11 That where DSD consents to a transfer of personal data outside the European Economic Area to comply with the obligations of a Data Controller under the DPA by providing an adequate level of protection to any personal data that is transferred; and any reasonable instructions notified to it by DSD.

3.12 We understand that failure to comply with the terms of this agreement may render us either corporately or individually liable to prosecution under the terms of the DPA.

4 After receiving the requested information from DSD we will use it **only** for the purpose specified in the schedule. We will ensure that it is not used for any other purpose without seeking further written permission from DSD.

5 We will not publish any of the data or results based on analysis of the data without the written approval of DSD.

6 We will identify all relevant legislation, protocols and codes of practice that apply to the information supplied under this agreement, and comply with them. We will provide evidence that any required ethics approval for our research project(s) has been obtained.

7 Should aggregate or anonymised data be supplied to us, we will not attempt to establish the identity of any individual pupils to which the data relate.

8 Should it be suspected or confirmed that the data provided (whether as a whole or part thereof) has been copied, compromised or lost; we will report full details of the incident to DSD without delay. The Head of DSD will decide any penalties (such as suspension from access to any further NPD data for a specific period) for such a breach of the agreed terms of access.

9 We will comply with any reasonable request to manage more securely the data entrusted to us, to facilitate the Department's compliance with the HMG Security Policy Framework.

[1] Data should be deleted so it ceases to be copied to backups, and secure file deletion software should be used so that unerase/undelete utilities cannot recover the data. HMG Security Policy Framework requires that all media on which DfE data has been processed should be shredded, destroyed using commercial best practice, de-magnetised, or securely erased (at end-of-life for media in shared infrastructure such as PCs, RAID file servers, SANs, and backup tape archives). Suitable products certified by CESG (Communications Electronic Security Group) or SEAP, or (for erasure of magnetic media up to Impact Level 2 PROTECT) to Common Criteria EAL2, are listed at chapters 6 (Data Erasure) or 15 (external Common Criteria) of http://www.cesg.gov.uk/publications/media/directory.pdf In Chapter 6, media erasure products certified under the 'CCTM' scheme are only sufficient for media re-use within the secure environment of your organisation, and not suitable for end-of-life disposal.

DATA ACCESS AGREEMENT SCHEDULE

Data Request Number (DRyymmdd.nn)	DR120627.01
Name (Block capitals)	[redacted]
Position held	[redacted]
Organisation	CIVITAS
Address	55, TUFTON STREET, LONDON
Postcode	SW1P 3QL
Email address	[redacted]
Telephone number	[redacted]
Date	28/6/2012
Data Protection Reg/ Notification No. (if registered under the Data Protection Act 1998)*	N/A

*An appropriate valid entry in the Register of Data Controllers managed by the Information Commissioner's Office (ICO) is mandatory for organisations requesting "personal" or "sensitive personal" data as defined by the Data Protection Act 1998. Registered organisations will have a registration number.

The National Pupil Database (hereafter NPD) is a longitudinal database linking pupil/student characteristics (e.g. age, gender, ethnicity) to school and college learning aims and attainment information for all children in maintained schools in England. Individual pupil level attainment data is also included for pupils in non-maintained and independent schools who partake in the tests/exams.

The NPD contains the attainment and pupil characteristics data at individual pupil level described in the table below.

Dataset	Academic year available from
Early Years Foundation Stage Profile (EYFSP) (Reception – Age 4) (Unamended, Final)	2002/03
Key Stage 1 (Year 2 – Age 7) (Unamended, Final)	1997/98
Key Stage 2 (Year 6 – Age 11) (Unamended, Amended, Final)	1995/96
Year 7 Progress Tests (Year 7 – Age 12)	2000/01-2006/07
Key Stage 3 (Year 9 – Age 14) (Unamended, Amended, Final) Key Stage 3 Teacher Assessment only	1997/98-2007/08 2008/09
Key Stage 4 (Year 11 – Age 16) (Unamended, Amended, Final)	2001/02
Key Stage 5 (Years 12-13 – Ages 16-18) (Unamended, Amended, Final)	2001/02
Individualised Learner Record (ILR)*	1998/99
Vocational Database (formerly National Information System for Vocational Qualifications (NISVQ)) (Ages 14-23)*	1998/99
School Census (formerly Pupil Level Annual School Census (PLASC)) (Ages 3-18)	Termly January 2006 (secondary schools) Termly January 2007 (nursery, primary

Spring census data is used within DfE as the main reference data, and provides the closest comparison to PLASC PLASC (Ages 3-18)	and special schools) 2001/02-2004/05 (secondary schools) 2001/02-2005/06 (nursery, primary, special schools)
School Census Post-16 Learning Aims (PLAMS) (Ages 16-18)	2006/07
School Census Absence (2 terms, 3 terms)	2006/07
School Census Exclusions (exclusion, enrolment, pupil level)	2006/07
Early Years Census (Ages 3-4) (Annual)	2007/08
Alternative Provision Census (Annual)	2007/08
PRU Census (Annual)	2009/10
Higher Education* (Ages 17-19)	2004/05
Children Looked After* (Ages 0-18)	2006
Children in Need Census*	2008/09

*Sharing of NPD data is governed by the Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009. The asterisked datasets are only available to a restricted audience due to legal constraints and the sensitivity of the data.

The 'latest' version of the data is generally sent out, but if you require a different version of the data please indicate.

Data can be provided either as an SPSS or tab delimited file or in database format. Unless otherwise approved, standard anonymised extracts will be supplied (either with or without spring School Census/PLASC and/or prior attainment).

The data will be sent to you in a password protected zip file. To ensure an appropriate level of encryption is used, please confirm the application/version you will use to unzip the file (eg Winzip Version 11.0).

Description of the information required (please give full details including variables required if more than the standard anonymised extract is requested):

Dataset (eg EYFSP, KS4, School Census)	Version (eg Unamended, Amended, Final)	Linkage eg unmatched dataset or dataset matched to School Census and/or prior attainment)	Academic year (for required dataset and any linked School Census)
KS4	Unamended	Standard linkage only	Most recent full year

Please specify format of data (eg SPSS) and application/version in use to unzip the file:

Stata (ideally) or Tab/comma delimited

Decompression by Windows 7 or 7-zip v.9.20

Purpose for which the information is required

Please ensure the following areas are covered in your description:

Full information about your project including the aims, audience and how it will be presented (giving details of the products/outputs that will be produced from your use of the data e.g. analysis, reports, tables, books);

Civitas provides contributions to topical education debates. Where other commentators cite statistics derived from the National Pupil Database there is value is being able to verify the facts. An example is http://blogs.ft.com/ftdata/2012/06/21/social-mobility-and-o-levels/ In these cases, the audience will be the newspaper-reading or blog-reading public and the outputs will usually be aggregated, headline statistics, summarizing key stage results.
In addition, Civitas publishes reports of its own into aspects of social and educational policy. Particular focus will be on absence and exclusion from school and the effect on pupils' own results and those of others in the school. Outputs are likely to be aggregated headline statistics or tables comparing the summary key stage results for the range of values for variables describing absence and exclusion.

If NPD data is to be matched with information from other sources to create a new dataset please give full details (including evidence to show that individuals covered by other sources are aware that their data will be used in this way and may be passed to DfE to allow matching as required under the Data Protection Act);

N/A

Confirmation of whether the project is on behalf of, or sponsored by, the DfE, including DfE contact names and the DfE reference number for your Research Contract where applicable.

Not for DfE

Please give name(s) of all those who will have access to the data, why they need access and what they will be accessing it for:

[redacted] for production of the aggregate statistics and tables described above.

Data should be stored and accessed on secured servers or secured IT equipment. Where you are requesting access to other than fully anonymised, non-disclosive data, please give details of your organisational security standards and whether the IT systems you have in place meet ISO27001 or the HMG Security Policy Framework. (Note: Laptop computers and other portable devices should not be used for processing personal data. However, where this is unavoidable data must be encrypted[2] and password protected.)

N/A

If your request includes sensitive personal data items (as defined by the Data Protection Act 1998) you must complete the business case below.

[2] Laptops should have full disk encryption using either a CESG CAPS approved product or alternatively a product that complies with the FIPS 140-2 Standard.

BUSINESS CASE FOR A SENSITIVE NPD DATA OUTPUT

There are two types of sensitive data items in the NPD: those that can be anonymised by mapping; and those that cannot be anonymised. The data items included in each section are outlined in the table below:

Type of sensitive data items	Data items	What the data items are mapped to
Data items that can be anonymised by mapping	Date of birth	Age of pupil at the start of the academic year Year and month of birth of pupil
	Ethnic code (extended ethnic codes)	Ethnic group (based on the 20 main ethnic codes)
	Language code (extended language codes)	Language group
	Home address including Postcode	Super Output Area (SOA)
	Output Area (OA)	Super Output Area (SOA)
Data items that cannot be anonymised	UPNs	
	ULNs	
	Names	
	Primary special educational need (SEN) type, e.g. specific learning difficulty, hearing impairment etc.	
	Service children in education indicator	
	Pupil's type of disability	

If you require any of these sensitive items described above, please ensure that each section of the business case is completed, giving as much detail as possible about what the data is to be used for.

Please define the sensitive data item(s) that you require. E.g. Date of birth, Postcode etc.	NA
If you require Date of birth, Ethnic code or Home address (including Postcode), why are the anonymised data item(s) not adequate for your needs? E.g. Why is year and month of birth of pupil not sufficient for Date of birth?	
What will you be using the sensitive data item(s) for?	

Completed data access agreement/business case should be sent by email to NPD.Requests@education.gsi.gov.uk.

If you have any questions please contact [redacted] on [redacted]

Annex 1: Protection of the Confidentiality of Individual Pupil Data: Statement of Procedures

1 Introduction

1.1 The Data and Statistics Division (hereafter known as DSD) is a corporate service within the Department for Education (DfE), providing a wide range of information and statistics on children and schools to address the needs of front line services, as well as the internal requirements of DfE and the wider community. DSD holds and processes various data which has been provided in confidence and may be personal and sensitive (as defined in the Data Protection Act 1998 [3]). These procedures have been adopted by DSD, and must be followed by recipients of data from DSD where they apply, to protect individual pupil data.

1.2 The following paragraphs expand on the specific measures taken to preserve confidentiality and security of individual data.

1.3 These guidelines are consistent with the UK Statistics Authority Code of Practice for Official Statistics available at http://www.statisticsauthority.gov.uk/assessment/code-of-practice/index.html).

2 Control of data use

2.1 Access to individual data must be authorised in writing by DSD. Such data should be handled in a manner appropriate to their sensitivity, including appropriate physical and procedural security controls. Personal data held for statistical purposes may not be used for other purposes, except where expressly permitted by legislation; or where the prior permission of the data subjects has been obtained. Personal data should not be removed or transmitted to geographic locations outside the European Economic Area (EEA) (in line with Cabinet Office guidance) and any personal data provided by DSD on a voluntary, research or non-contract basis may not be removed or transmitted to geographic locations anywhere outside the UK without the express written permission of DSD.

3 Legal and ethical obligations

3.1 DSD will comply with all relevant legislation, protocols and codes of practice[4] relating to the collection, storage and use of the data it holds and will obtain ethics approval for research where it is required.

---

[3] Personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Sensitive personal data is defined in the Act as consisting of information relating to: racial or ethnic origin; political opinions; religious or similar beliefs; membership of a trade union; physical or mental health; sexual life; commission or alleged commission by of any offence; any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

[4] Section 537A of the Education Act 1996, The Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009, Data Protection Act 1998, UK Statistics Authority Code of Practice for Official Statistics, HMG Security Policy Framework

4 Avoiding disclosure

4.1 Statistics are not published (or otherwise released) unless DSD are satisfied that relevant controls are in place to ensure the security of the data. For each of our publications (eg Statistical First Releases, Statistical Bulletins) DSD assesses the risk of disclosure based on

- Level of aggregation of the data
- Number of tables produced from each dataset
- Possibility of an attempt to identify individual pupils
- Size of the population under consideration.

5 Internal access

5.1 Personal data are only made available to a limited set of individuals within DSD, all of whom must have an approved business need. Data may only be accessed in a secure environment by staff who have enhanced CRB clearance.

6 External access to DSD data for research purposes

6.1 Personal data (and aggregate or anonymised data which are not publishable because they do not meet the criterion of virtually no risk to confidentiality) may be made available for appropriate and fully specified statistical research purposes, but only where:

- all legal, research ethics and other constraints have been considered and observed by DSD; and
- approval for release of the data has been given in writing by DSD.

6.2 Data access arrangements will only be entered into with private individuals where there is an appropriate sponsoring organisation or referee (eg a research organisation or university). All researchers will be required to complete a data access agreement and to comply with any relevant principles to maintain ethical standards in research. The data supplied will be the minimum needed to meet the agreed study objectives, may not be transmitted onwards and must not be published without the prior approval of DSD. Requesters will be required to undertake not to attempt to establish the identity of any individual either from the data that is supplied to them by DSD or by linking this data to any other data that they have in their possession or that might later come into their possession.

7 Consultants and contractors

7.1 Consultants and contractors employed for research purposes by DfE are subject to the same confidentiality constraints and disciplines as DfE staff. They are required to sign a data access agreement appropriate to the work on which they are employed.

8 Use of personal identifiers

8.1 Some DSD activities require the collection and storage of names and addresses. Records that include names and addresses or other information that may identify an individual are subject to strict controls to prevent unauthorised linkage with

other data. Access to such files is restricted to a small number of individuals with an approved business need, and can only be authorised by DSD.

9 Linkage

9.1 By combining data from separate sources it may occasionally be possible to meet new information needs without placing further demands on respondents. Subject to authorisation as necessary, DSD may, for specific statistical purposes, link data sets that it holds. The authorisation will include specification of any enhanced security requirements for the linked data and will specify who may access the linked data and for what purpose the data may be used. All confidentiality undertakings will be respected by DSD when any personal data are received from other organisations.

10 Intended use

10.1 DSD informs those who directly provide it with personal data of DfE's intended use of these data (http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/). Where personal data is received from other organisations, any confidentiality undertakings given at the time of collection will be respected.

11 Administrative sources

11.1 Data initially collected for administrative purposes, and to which the DSD has been granted access, may be used for statistical purposes provided that no undertakings have been given to the contrary and that all appropriate procedures to protect confidentiality are followed.

12 IT security

12.1 DfE staff have received appropriate training in IT security matters and are aware of standards and guidelines which are available to help ensure that IT security is maintained. (Data Security Guidance for the Analytical Community (AC) is available on the AC Portal and Departmental IT Security Guidance is available on the Departmental Security Unit (DSU) website both on the DfE Intranet. Additionally the DSU may be consulted for advice on appropriate security controls. DSD will not release details of IT systems and security measures that might compromise the confidentiality, integrity and availability of data they hold. IT security measures will be reviewed annually by carrying out a risk assessment.