



Department
for Education

Data Management Advisory Panel (DMAP) – Terms of Reference

July 2016

Contents

Introduction	3
The Data Management Advisory Panel (DMAP)	3
Purpose and Role of the DMAP	3
DMAP decisions	4
Accountability and Governance	4
Appeals Process	5
Membership	5
Meetings	6
Out of meeting actions and approvals	6
General conduct of the Data Management Advisory Panel	7
Secretariat	7
Changes to these Terms of Reference	8
Annex A – Information Tiers	9
Annex B - Identifying and / or Identifiable and Highly Sensitive data items	10
Annex C - Purpose and Role of the NPD Approvals Process	11
Annex D - Version control	13

Introduction

As the custodians of the National Pupil Database and other datasets held by the Department for Education, a significant part of the role of the Department's NPD and Data Sharing team in Data and Education Standards Analysis Group (DESAG) is to process information, including the personal data (of learners, children and of the school workforce) for a range of purposes including research.

It is the role of the NPD and Data Sharing team to ensure that the Department continues to meet information governance standards in processing information and that all processing of information is lawful, secure and in line with Departmental and HMG standards.

The Data Management Advisory Panel (DMAP)

The Data Management Advisory Panel (DMAP) is a Departmental group consisting of senior members of staff from across the Department. DMAP will support the NPD and Data Sharing team in fulfilling its duties by reviewing and deciding whether to approve applications for access to identifying and/or identifiable and highly sensitive data (see Annex A and B).

Note: We will be widening the membership in 2016 to include 2 external representatives. The ToR will be updated when that is complete.

Purpose and Role of the DMAP

DMAP will consider applications made to the NPD and Data Sharing team for extracts of data:

- containing identifying and/or identifiable and highly sensitive (tier 1) data items, where the potential disclosure of that data could cause harm and distress to individuals;
- where linkages with other datasets could enable identification and to advise on any additional safeguards required; or
- where the NPD and Data Sharing team assess the application as complex or sensitive requests and would like to seek further input and assurance.

Whilst performing this function DMAP will:

- provide assurance to the Secretary of State that the confidentiality of individual data is safeguarded in line with the Data Protection Act, and other relevant

legislation, e.g. Section 1 of the Computer Misuse Act 1990 and the Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009;

- ensure that requests are technically sound, comply with the regulations which govern the release of individual pupil data, are practical and appropriate to the needs, and are ethical in nature;
- consider whether the use of identifying and / or identifiable and highly sensitive data is necessary, or whether less sensitive data might suffice;
- confirm the information security procedures (e.g. information handling and retention) demanded of the requesting organisations are appropriate and proportionate to the information being provided and have been accepted by the data requester; and
- ensure any associated risks of disclosure are understood and managed.

DMAP decisions

DMAP decisions require at least 3 core members. The potential decisions DMAP can take are:

- Application approved
- Application approved subject to agreed actions
- Further information required
- Rejected with reasons – this does not preclude an applicant coming back at a later point with a revised application which will then be considered on its own merits

Accountability and Governance

DMAP has primary responsibility for decisions made in relation to the data the Department for Education extracts, holds and processes. An escalation route to the Secretary of State exists where the DMAP believes a request is particularly sensitive and cannot be resolved through the appeals process outlined below. The NPD and Data Sharing team is accountable to DMAP for its actions and decisions, and provides reports to DMAP on a monthly basis.

The NPD and Data Sharing team act as a triage function, deciding upon those requests that require escalation to DMAP. Requests for access to data within Tier 1 will always require escalation to DMAP (See Annex A and B), requests for data within Tiers 2, 3 and 4 will generally be processed by the NPD and Data Sharing team but complex or sensitive requests may be escalated to DMAP, and a sample of cases are copied to the DMAP chair for comment before approval to maintain wider oversight. The purpose and role of the NPD and Data Sharing team's Approvals process is included in Annex C.

Appeals Process

The Data Management Advisory Panel will consider appeals against decisions made by the NPD and Data Sharing team. In addition DMAP will also further consider any appeals against decisions made by the panel itself using any new information that applicants provide.

In the first instance to make such an appeal please contact Richard Lumley on Richard.Lumley@education.gsi.gov.uk who will be able to co-ordinate any appeal as required. These appeals will be heard by the DfE Director of Data if necessary.

Membership

The Data Management Advisory Panel consists of the following membership:

Job role	Function
Deputy Director, Head of Data Modernisation Division	Chair and core member To provide challenge on requests brought to DMAP
Deputy Director, Head of Education Standards Evidence and Dissemination Division	Core member To provide challenge on requests brought to DMAP
Deputy Director, Head of Infrastructure And Funding Directorate Analysis Division	Core member To provide challenge on requests brought to DMAP
Deputy Director, Head of Strategic Analysis and Research Division & Chief Economist	Core member To provide challenge on requests brought to DMAP
Team Leader, NPD and Data Sharing team	Core member To provide challenge on requests brought to DMAP
Legal advisor (DfE)	As required To provide legal advice where requested

Privacy and Information Rights Advisory Service - PIRAS (LAO, DfE) advisor	As required To provide advice as requested
Department Security Unit (DSU) advisor (DfE)	As required To provide advice as requested
NPD and Data Sharing team member	Secretariat
Other NPD and Data Sharing team member(s)	As required To present cases for consideration and provide additional background to DMAP members

Additional members with particular professional or technical knowledge may also be invited as required. As the NPD and Data Sharing team liaise with colleagues in LAO, PIRAS and DSU in the lead up to submitting requests to DMAP, it was decided that representation from these parties would only be required in exceptional circumstances.

Meetings

DMAP will meet on a monthly basis.

The Secretariat will consider the agenda and decide whether there is enough business to justify a full meeting at least 3 working days in advance of the meeting.

In the event that a full meeting is required panel members will be provided with summaries of the applications at least 2 working days in advance of the meeting.

Out of meeting actions and approvals

There are 3 scenarios whereby requests for access to data within Tier 1 may be considered by the panel outside of the usual panel meeting:

1. Where there is insufficient business to justify a full meeting the secretariat can seek decisions by the panel via e-mail correspondence. It is expected that a response be provided within 5 working days.
2. Where the outcome of the DMAP meeting is that further clarification or information is required in order for the application to be approved, the panel members can

agree that, where this is provided by the applicant and in line with the panel request, that officials in the NPD and Data Sharing team and / or the Chair can review and confirm approval ahead of the next meeting. Where required, it is expected that a response be provided by the panel within 5 working days.

3. Where there is an urgent request for data that cannot wait until the next DMAP meeting to be discussed the secretariat can seek decisions by the panel via e-mail correspondence. It is expected that a response be provided within 5 working days.

Any such consideration and subsequent actions will be reported to DMAP at the next meeting.

General conduct of the Data Management Advisory Panel

In conducting its business, members of DMAP will be expected to adhere to a simple code of conduct:

- The panel may receive information of a confidential nature, e.g. commercially sensitive information relating to the development of new products or service, or other information not within the public domain. Members of the panel will be required to keep such matters confidential;
- members of the panel will review papers prior to meetings to ensure they are fully prepared to consider requests for access to data;
- the Secretariat will keep records of the Panel's considerations and recommendations, although the exact form of these records will be determined by the panel and its Secretariat;
- members of DMAP must declare any potential conflicts of interest which might affect matters being considered, or their objectivity as a member of the panel, as soon as that potential conflict becomes apparent.

Secretariat

The Secretariat will be responsible for:

- Arranging the monthly meetings;
- deciding whether there is enough business to justify a full meeting or whether to seek decisions via e-mail correspondence;
- preparing the agenda (where a full meeting is to take place);
- preparing and issuing a summary of all data requests to be considered by the panel, including a recommended course of action;

- providing the panel with a summary of data requests received and processed by the NPD and Data Sharing team and DMAP since the last meeting,
- maintaining a record of all decisions taken by the panel; and

Changes to these Terms of Reference

These terms of reference may be varied by DMAP from time to time following appropriate consultation with other parties such as the NPD and Data Sharing team and Departmental Security Unit. Any changes will be clearly labelled in this document.

Annex A – Information Tiers

Information Tier	Information Type	Description
1	Individual pupil level data - Identifying and / or Identifiable and Highly Sensitive	<p>Individual pupil level extracts that include identifying and highly sensitive information about pupils and their characteristics including items described as ‘sensitive personal data’ within the Data Protection Act 1998.</p> <p>Examples of identifying data items include Names, Address and Date of Birth.</p> <p>Examples of highly sensitive data items include Looked After Status, In Need Status, Full Ethnicity, Full Language and Primary and Secondary SEN Type, reasons for exclusions and absence.</p>
2	Individual pupil level data – Identifiable and Sensitive	<p>Individual pupil level extracts that include sensitive information about pupils and their characteristics including items described as ‘sensitive personal data’ as defined by the Data Protection Act 1998 which have been recoded to become less disclosive.</p> <p>Examples of sensitive data items include ethnic group major, ethnic group minor, language group major, language group minor, Special Educational Needs and eligibility for Free School Meals.</p>
3	Aggregate School level data – Identifiable and Sensitive	<p>Aggregated extracts of school level data from the Department’s School Level Database which include items considered ‘sensitive personal data’ within the terms of the Data Protection Act 1998 and could include small numbers and single counts.</p> <p>For example, there is 1 white boy eligible for Free School Meals in school x that did not achieve level 4 in English and maths at Key Stage 2.</p>
4	Individual pupil level data – Identifiable	<p>Individual pupil level extracts that do not contain information about pupils and their characteristics which is considered to be identifying or described as sensitive personal data under the Data Protection Act 1998.</p> <p>For example, the extracts may include information about pupil attainment, prior attainment, progression and pupil absences but do not include any obvious identifying data items like names and addresses and any information about pupil characteristics other than gender.</p>

Annex B - Identifying and / or Identifiable and Highly Sensitive data items

Identifying data items requiring approval by DMAP:

- Pupil Matching Reference (Non Anonymised)
- Unique Learner Number
- Unique Pupil Number
- Name(s)
- Date of Birth
- Home Address
- Postcode
- Exam Candidate Number
- Exam Candidate ID

Highly Sensitive data items requiring approval by DMAP:

- Looked after status
- In need status
- Adopted from care
- Primary & secondary special educational need type
- Pupil's type of disability
- Extended ethnicity codes
- Extended language codes
- Service child
- Reasons for absence
- Reasons for exclusion
- Census output area (COA) code

Annex C - Purpose and Role of the NPD Approvals Process

The NPD and Data Sharing team's approvals process will continue to authorise requests for access to identifiable and identifiable and sensitive data (tiers 2, 3 and 4) with oversight from the DMAP chair on sample basis.

The NPD and Data Sharing team's approvals process will act as a triage function, deciding upon those requests that require escalation to DMAP. Requests for access to data within Tier 1 will require escalation to DMAP (See Annex A and B), requests for data within Tiers 2, 3 and 4 will generally be processed by the NPD and Data Sharing team but complex or sensitive requests may be escalated to DMAP.

Regardless of whether a request is destined for approval at DMAP or for approval by the NPD and Data Sharing team, the relevant NPD and Data Sharing team member responsible for processing of the request will undertake the following activities:

- establish the credentials of the applicant(s) and the institution or organisation for which they work;
- determine the names and job titles of all individuals who will be accessing the released data;
- discover all the intended uses for the data, and that these are consistent with those of the Department and the reasons for which the data can be lawfully disclosed;
- establish with the applicant the minimum amount of information required to satisfy those purposes;
- work with users to understand the nature of their requirements and establish whether there are conflicting needs;
- establish that the need for individual level data cannot be met by alternative means;
- describe the disclosiveness of the micro-data requested (non-sensitive, sensitive, highly sensitive and identifiable) and any conditions under which the information may become identifiable;
- establish the recipient's physical and electronic security standards meet or exceed those required of recipients by the Department for the tier of data requested;
- for highly sensitive and identifiable data releases, agree the finite period of time for which the access will be permitted, and the processes by which the data will be securely deleted;

- ensure that the requestor has completed the application pack and associated documentation such that it can be considered by the approvals panel and / or presented to DMAP if necessary;
- ensure that requests are technically sound, comply with the regulations which govern the release of pupil data (including establishing the data protection act conditions for processing), are practical and appropriate to the needs, and are for ethical reasons; and
- inform applicants of the progress of their applications including decisions made by the NPD and Data Sharing team and DMAP:
 - Where applications are rejected it will provide the reasons for its rejection, and explain what steps would need to be taken for a resubmitted bid to be considered.
 - Where applications are approved it will keep applicants informed of progress towards meeting their request.

As part of this process, the NPD and Data Sharing team will consult as needed with legal, privacy and security experts within the Department.

Annex D - Version control

Version	Date	Summary Of Changes
June 2016	14 th July 2016	Initial Publication



Department
for Education

© Crown copyright 2016

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

To view this licence:

visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2

email psi@nationalarchives.gsi.gov.uk



Follow us on Twitter:
[@educationgovuk](https://twitter.com/educationgovuk)



Like us on Facebook:
facebook.com/educationgovuk