Department for Education

# Data Sharing and Approval Panel (DSAP) – Terms of Reference

## Introduction

As custodians of personal child, pupil, learner, and workforce datasets[1] it is vital that the department's data sharing teams continue to meet information governance standards in processing information and that all processing of information is legal, ethical, proportionate, secure and in line with Departmental and Her Majesty's Government (HMG) standards. It is also it is important to maximise the public benefit of this data through safely facilitating third party research in the public interest.

## Purpose of the Panel

The Data Sharing Approval Panel (DSAP) provides the necessary governance and scrutinises every application for personal child, pupil, learner, and workforce data to external organisations including to third party researchers. DSAP helps to shape overall data sharing strategy and supports the department's data sharing teams and information asset owners in fulfilling their duties.

DSAP acts on delegated authority from the DfE Data Governance Board (DDGB) which is responsible for maximising the exploitation/ optimal use of data assets and, through its sub boards, enabling the GDPR compliance regime to support the department's use of data by minimising risks, duplication, and inefficiencies across its data landscape. The Data Governance Board acts on delegated authority from the Digital, Data and Technology Committee (responsible for the design and implementation of data, digital and technology strategy). This advises the Leadership Team who supports the Permanent Secretary to run the department.

DSAP remit from the Data Governance Board is to govern all external, individual level data sharing by DfE and its executive agencies to ensure that it is proportionate, ethical, secure, legal and maintains GDPR compliance. On occasion, DSAP may escalate issues to the DfE Data Governance Board.

---

[1] National Pupil Database (NPD), the Individualised Learner Record (ILR), Schools Workforce (SWF) data, Children in Need data (CIN), Children Looked After (CLA)

## Role of the Panel

DSAP will consider applications made to DfE for extracts of personal data such as:

- data containing any information relating to an identifiable natural person
- data which carries risk of personal identification including where linkages with other datasets could enable identification.

DSAP will require appropriate safeguards to be in place prior to sharing information.

Whilst performing this function DSAP will:

- provide assurance to the Secretary of State that the confidentiality of personal data is safeguarded in line with the General Data Protection Regulation and the Data Protection Act 2018, and other relevant legislation;
- ensure that requests are technically sound, comply with the regulations which govern the release of personal pupil data, are practical and appropriate to the needs of the project / research, and are ethical in nature;
- consider whether the use of identifying and / or identifiable and 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;
- ensure any associated risks of disclosure are understood and managed;
- where necessary and appropriate, consult and seek input from the Data Governance Board and its sub bodies on issues demanding or needing strategic direction, guidance, or resource. These will be escalated to the Data Governance Board at the chair's discretion;
- provide the DfE Data Governance Board with appropriate management information of all DfE data shares and to ensure the department's resources is sufficient to support a demand-led model.

### In Scope

Cases must be brought to DSAP for:

- data shares from DfE or its executive agencies (ESFA, TRA, STA) to any third party (including non-ministerial departments, NDPBs, etc). This includes all data shares from these parties irrespective of whether they are governed under contract, through a data sharing agreement or via other means. These are in scope as data is leaving DfE to another organisation,
- data shares from non-ministerial department or NDPBs, where DfE is a joint controller, to other third parties. This includes all data shares from these parties irrespective of whether they are governed under contract, through a data sharing agreement or via other means. These are in scope as DfE is jointly making the decision on sharing the data they are controller for.

Cases must be brought to DSAP where personal data to be shared is:

- at an individual, or record, level. This includes data which is:
  - directly identifiable (i.e. including names, address, small geographical areas or other meaningful identifiers);
  - pseudonymised or de-identified (i.e. having direct or meaningful identifiers removed but still referring to an individual);
  - functionally anonymised[2] at point of access (i.e. where consideration of the relationship between the data and the environment within which the data is accessed results in a minimisation of risk to a level of negligibility);
  - synthetic[3](i.e. artificially created or generated which mirrors the patterns or structures of 'real data' without being based on real events)
- aggregated but unsuppressed such that data contains a significant risk of re-identification.

Cases must be brought to DSAP for:

- digital services providing access to pupil, learner or workforce data to external organisations;
- any data shares intending to be managed through a Secure Environment Provider (e.g. Office for National Statistics Research Accreditation Service) where onward sharing to Accredited Researchers is through the Secure Research Service [each onward share will also be approved by DSAP as Data Owner].

## Out of Scope

Cases do not need to be brought to DSAP for approval where:

- data shares are by non-ministerial departments or NDPBs with other third parties where DfE is not a controller, or joint controller, of the data being shared. These are not in scope as DfE is not sharing any data;
- data shares from DfE to its executive agencies (e.g. ESFA, STA). These are not in scope as these are considered internal data shares.

Cases do not need to be brought to DSAP for data that is:

- aggregated with negligible risk of re-identification;
- published data;

---

[2] UK Anonymisation Network definition - Functional anonymisation does not assume that anonymisation can be zero-risk or irreversible; it is meant instead to bring anonymisation practice in line with the art of the possible i.e. a minimisation of risk to a level of negligibility. Key to achieving functional anonymisation is a recognition that whether data are or are not anonymised is not a property of the data alone, but rather determined by the relationship between the data and the environment(s) in which they are held. In practice, this means taking account of both the data to be shared and features of the data environment(s) at the risk assessment stage not just at the risk management stage.

[3] Synthetic data is not personal data if it has been properly created, using random data points, as a natural living human being cannot be identified from synthetic data however DSAP would still like to have sight of these cases and include these on gov.uk. If synthetic data has been created using pseudonymised data then there is still a chance that identifiable data can be re-engineered and these cases must be approved by DSAP.

- publicly available (e.g., under Freedom of Information Act, responses to parliamentary questions);
- requested in response to an individual rights request (e.g. subject access request) or by the police and/or courts;
- not related to an individual (e.g. data relating to an educational establishment or course of study).

### Panel Membership

The Data Sharing Approval Panel consists of DfE and non-DfE members. Additional DfE members with particular professional or technical knowledge may also be invited as required.

## DfE Members

Chair - Head of Data Ownership and Data Sharing, Data Operations Division, DfE

Core members:

- Deputy Director, Head of Data Operations, DfE
- Deputy Director, Head of Infrastructure and Funding Directorate Analysis Division, DfE
- Deputy Director, Head of Higher Education Analysis, DfE and/or Head of Higher Education Statistics Unit, DfE
- Deputy Director, Head of Data Insights and Statistics Division and Head of Profession for Statistics, DfE
- Deputy Director, Data Science Service for the Education and Skills Funding Agency, DfE
- Deputy Director, Head of Early Years, Schools and SEND Analysis and Research
- Head of FE and post-16 statistics, DfE
- Data Protection Officer (or delegated representative)

Core members (with case-specific knowledge):

- Team Leader, NPD, and Data Sharing team, DfE
- Team Leader, Data Governance & Assurance in the Education and Skills Funding Agency, DfE

Other:

- Department Security Unit advisor, DfE
- Legal Office advisor, DfE
- Other team members to present DSAP cases, DfE
- DSAP Secretariat, DfE

## Non-DfE Members

The Department appoints up to four non-DfE members who have extensive experience of sharing sensitive data as well as the ethics for doing so. The role is voluntary, non-DfE members can withdraw at any time for any reason. The current non-DfE members are:

- Matthew Homer – Associate Professor, University of Leeds & Chartered Statistician
- David Jesson - Fellow of the Royal Statistical Society (FRSS)

## DfE Member's Responsibilities

Chair is responsible for chairing the meeting and facilitating a fair and balanced debate on each case. Where chair is unable to attend, delegated responsibility will be passed to another member of Data Operations Division to take on all responsibilities as chair. The Chair is a core member of the panel.

- Core members are responsible for reading all of the casework prior to each DSAP meeting, debating the merits or otherwise of each case culminating in a decision of approval, rejection, or a request for further clarifying information.
- Core members (with specialist knowledge) will be called upon for advice as required to ensure relevant legislation is upheld and DfE policies are adhered to.
- Core members (with case-specific knowledge) are responsible for ensuring the cases brought to DSAP for their area are presented appropriately as well as debating on all other cases.

## Non-DfE Member's Responsibilities

Non-DfE members of DSAP are asked to contribute to the monthly DSAP meetings by:

## Offering advice on specific decisions:

- making recommendations as to whether a particular data share or data sharing agreement is suitable or unsuitable;
- challenging DfE to ensure that the department is fair and follows due process; and
- ensuring DfE has clear strategies that maximise benefit of personal data held by the department in ways which are appropriately secure and provide reassurance to data subjects about how their data is handled.

## Offering advice on DfE's data sharing policies and on the progress of data sharing improvement projects:

- Helping DfE make iterative improvements to the process and information asked from requesters;
- Offering advice and input on how to improve DfE's data sharing polices, strategy and direction; and
- Inputting into the frameworks and processes by which DSAP makes decisions when non-DfE members are not present.

If any decisions to share data fall into the following categories, which DSAP would benefit particularly from additional scrutiny, then DfE will look to ensure that the non-DfE members are present to advise as appropriate when the decision is made:

- Data sharing with commercial organisations or for commercial purposes;
- The first time new DfE data sets are shared;

- Data shared with other public sector bodies for purposes other than solely for education;
- Data sharing that involves linking education data to other sensitive data, for example medical data; and
- Any other situations where DfE's data sharing teams believe that DSAP might benefit from external member input.

Non-DfE members will attend either via telekit or in person at a DfE site. They will be sent an agenda and papers at least 2 working days before each meeting. DSAP makes decisions about specific data shares with specific organisations. If there is a conflict of interest in any of these data shares, then the non-DfE members must declare these and not provide any input into those decisions.

## DSAP Member's Standards of Conduct

All members are expected to follow the 7 principles of public life (Nolan Principles) as they apply to the Data Sharing Approval Panel as a whole. All members are also 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 services, or policy information not yet within the public domain. Members of the panel are required to keep such matters confidential;

- panel members 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;

- panel members are encouraged to promote DfE data sharing and the role of DSAP but should refrain from any public, political, media activities about DfE data sharing policy, processes or activities that would undermine or jeopardise the work of the panel;

- 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. The exact form of these records will be determined by the panel and its Secretariat.

## DfE Information Asset Owners' Responsibilities

The secretariat acts as a triage function for each and every case, thereby deciding which cases are ready to go to DSAP and which ones need further scrutiny. The Secretariat will also manage the volume of cases that are submitted to DSAP in order to ensure a steady stream of cases are flowing through the approval system.

For each case (requests for access to personal data will always require escalation to DSAP), the Information Asset Owner (IAO) must ensure he/she has:

- established the credentials of the applicant(s) and the institution or organisation for which they work;
- determined the names and job titles of all individuals who will be accessing the released data;
- discovered 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;
- ensured that the requestor has completed the application pack and associated documentation such that it can be considered by DSAP;
- established with the applicant the minimum amount of information required to satisfy those purposes;
- worked with the applicant to understand the nature of the request and establish whether there are any conflicting needs;
- established that the need for personal level data cannot be met by alternative means;
- described the disclosiveness of the micro-data requested (in terms of sensitivity or identifiability) and any conditions under which the information may become identifiable;
- established whether the recipient's information security standards meet the department's requirements for providing data directly to the applicant;
- encouraged the applicant to conduct their research / analysis in ONS secure research service;
- agreed the finite period of time for which the access will be permitted, and the processes by which the data will be destroyed;
- ensured that requests are technically sound, comply with data protection legislation which govern the release of personal data, are practical and appropriate to the needs, and are for ethical reasons;
- ensured cases have consulted legal, privacy and security experts as appropriate;
- informed applicants of the progress of their applications including decisions made by DSAP:
    - where applications are rejected, and a rejection / right of appeal notice has been issued by the secretariat, IAOs remain responsible for explaining the rationale to the applicant and supporting the applicant through the appeal process if they disagree with the decision
    - where applications are approved, explained what steps would be taken to progress their case.

## DSAP Panel Meetings

All panel meetings will be chaired by the Chair or a nominated deputy. The panel will be quorate when there are three core members in attendance who are able to make decisions on each case. The agenda and minutes for each panel meeting will be provided by DSAP Secretariat.

To ensure DSAP provides a timely service to requestors and DfE, it holds a combination of longer monthly meetings (with non-DfE members) along with shorter weekly meetings.

Presentation of data sharing cases will be carried out weekly. At the monthly meetings, standing agenda items are:

- previous minutes and actions from last meeting
- presentation of data sharing cases
- additional agenda items as pre-agreed with the Chair
- any other business.

The Secretariat is responsible for:

- arranging the weekly meetings;
- deciding whether there is sufficient 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 Department's Data Sharing teams and DSAP since the last meeting,
- maintaining a record of all decisions taken by the panel,
- producing the bi-annual publications of DfE data shares for gov.uk.

## DSAP's decision-making process

DSAP decisions require the agreement of at least 3 core members (including non-DfE members for monthly meetings) AND a majority of those members in attendance. Where there is a deadlock, and a majority is unable to be reached, the decision will be escalated to the DfE Chief Data Officer.

The potential decisions DSAP can take are:

1. Application approved
2. Application approved subject to agreed actions
3. Further information required
4. Rejected with reasons – this does not preclude an applicant re-submitting the application at a later stage with a revised application which will then be freshly considered on its own merits

## Carrying out DSAP business in correspondence

There are three scenarios when requests for access to personal level data may be considered by the panel outside of the usual panel meeting, see below. Any such consideration and subsequent actions will be reported to DSAP at the next meeting.

- where there is insufficient business to justify a full meeting the secretariat may seek decisions by the panel via e-mail correspondence. It is expected panel members will provide a response within 3 working days;
- where the outcome of the DSAP 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 information asset owners and / or the Chair can review and confirm approval ahead

of the next meeting. Where required, it is expected that a response back to the applicant be provided by the panel within 3 working days;

- where there is an urgent request for data that cannot wait until the next DSAP meeting to be discussed the Secretariat can seek decisions by the panel via e-mail correspondence. It is expected that a response back to the applicant be provided within 3 working days of the additional information being provided by the applicant.

## Reconsideration and Appeals Process

DSAP will consider any written dispute against decisions made by the panel, first by reconsideration and then, if required, by appeal. Any dispute must be submitted within one calendar month of the outcome notification date. Following this, the requestor should be notified of the dispute outcome within one calendar month. Separately, DSAP may request additional information from applicants to progress their applications.

To challenge a decision please contact data.sharing@education.gov.uk who will be able to co-ordinate any reconsideration or appeal as required. If the reconsideration cannot be resolved between DSAP and the requester, then any subsequent appeal will be escalated to the DfE Data Governance Board and Chief Data Officer.

## Accountability and Governance

If there is any unresolvable disagreement between DfE and non-DfE members, this will be escalated to the department's Chief Data Officer. An escalation route to the Secretary of State exists where DSAP believes a request is particularly sensitive and cannot be resolved through the appeals process outlined above.

# Review

These terms of reference will be reviewed by DSAP members and with the Data Governance Board yearly.