HM Government

Data sharing guidance for researchers seeking permission for secure access to data

January 2022

Ministry of Justice working with HMCTS and Department for Education

Contents

What is this application form for?

Please use this application form for requesting access to data for research purposes from:

- Ministry of Justice
- Her Majesty's Courts & Tribunals Service
- Department for Education (MoJ–DfE datashare only)
- Her Majesty's Prison and Probation Service (Data First Datasets only - MoJ Data First Criminal Courts, Prisons and Probation Linked Dataset, the MoJ Data First Prisoner Custodial Journey Level Dataset, and the MoJ Data First Probation Dataset)

For example, datasets that are part of the Data First project or extracts of the Police National computer.

The form covers requests for access to data:

- held in the ONS Secure Research Service
- within your own secure setting through a Data Sharing Agreement
- collected directly from HMCTS personnel, records or sites.

This is a modular form. Please see the accompanying 'Available data and their modes of access' document to see what sections you are required to fill in for the data and access route you are requesting. Please complete all relevant fields in the application form and provide all required documentation.

Requests that have been approved can be found under the "Approved external data request log". It is recommended that applicants read what research is already being conducted to avoid duplication of research.

Processing of data request applications

When you make a request, we will first make sure we have received all of the relevant documentation and data requirements, before submitting your request to the panel(s) that govern access to the data requested.

When applying for MoJ-held data or HMPPS Data First data[1], the Data Access Group (DAG), a panel comprised of Data and Analytical Services staff, will evaluate your request and a make a recommendation to the Data Access Governance Board (DAGB). Chaired by the MoJ's Chief Statistician, this board will have the final decision on whether data will be shared. Both the DAG and DAGB meet when needed to consider requests, with an expected turn-around time of 1 month.

If approved, you will be directed to the team(s) holding the data to arrange access. If your application is for access through your own secure setting, a Data Protection Impact Assessment and a Data Sharing Agreement will need to be negotiated. After the Data Sharing Agreement is signed by all parties, it becomes live and data will be shared, with annual reviews to ensure compliance with the agreement throughout its lifespan.

HM Courts & Tribunals Service (HMCTS) is a separate Executive Agency within MoJ. Therefore, when applying for HMCTS held data, all requests for existing HMCTS data, new data collections and research using case files or involving interviews/questionnaires with HMCTS court staff or court/tribunal users must be considered and approved by the HMCTS Data Access Panel (DAP). It is essential to contact the Data Access Services Team before making an application to DAP. The team can be reached at: dataaccesspanel@justice.gov.uk.

Once the application is submitted to the Data Access Services team, it will be thoroughly vetted. This is often the longest stage as the team seeks to address any gaps or queries in the application. Following this, there is consideration and approval by DAP. If approved, the panel and the team will work with you to facilitate access.

When applying for access to the MoJ DfE data share, it will be considered both by DAG/DAGB and by DfE's Data Sharing Approval Panel (DSAP). Where DSAP agree to provide you with access to data, you will be provided with an Agreement and Schedule that you will be required to sign and return. By signing this, you will be agreeing to the terms and conditions set out in the Agreement. Please keep a copy of all the documents, including completed forms, for your own records. You must also have completed the ONS Researcher Accreditation Process before accessing your data.

[1] MoJ Data First Criminal Courts, Prisons and Probation Linked Dataset, the MoJ Data First Prisoner Custodial Journey Level Dataset, and the MoJ Data First Probation Dataset

Publication of details of requests

As part of our commitment to openness and transparency we publish information about data that has been shared outside of the department as part of the Data First project on GOV.UK webpages. There may be exceptions where we do not publish information – for example, to protect the privacy of researchers working on particularly sensitive topics. The information published includes the following:

- Title of the research.
- A brief description (150 words) of the project including summary of data shared.
- The name of the requesting organisation.
- Project timescales.

We will not publish personal details of applicants.

What information do I need to provide?

We can only share data if there is a legal basis to do so. As a Data Controller we must also comply with all applicable data protection legislation including the Data Protection Act 2018 and General Data Protection Regulation (GDPR) for to ensure safe, necessary and proportionate handling processing of data.

Section One: Data Access

This section of the application form will ask for what data you are requesting and how you would like to access the data.

Please be aware that some data are only available through specific access routes. If you are unsure, please see the 'Available data and their modes of access' document.

Section Two: Applicant details

This section of the application form will ask for basic contact details of the requesting organisation and researchers (this must include the name of the person or organisation to whom we would permit the use of data within a secure setting). It has additional information concerning the relationship between the requesting organisation and other organisations (e.g. commissioning, funding, sponsoring or contractual).

Section Three: Project details

The various data panels scrutinise applications to ensure all external requests for individual data are legal, ethical, proportionate and secure. This is a key section for consideration of whether the project proposal is in line with the permitted uses of the data and in the public interest so please build a clear, concise and compelling case for why you should be granted access to the data requested.

As such, requesters must provide evidence to the panel on:

- the brief purpose and intended outputs of the project for the panel to assess purpose limitation. This may also be used to publish details of external and third party data shares on GOV.UK quarterly
- how your project will achieve a benefit to the public,
- how your request for data is specifically, explicitly and legitimately required for the project purpose,
- Evidence to demonstrate explicit consent (where relevant) and further evidence on how individuals' rights are managed throughout the project.

Section Four: GDPR

We also ensure all external requests for individual data complies with Data Protection Legislation (Data Protection Act 2018 and General Data Protection Regulations) by

- ensuring we have Data Protection Officer (DPO) contact details for all third parties
- encouraging development of Data Protection Impact Assessments (DPIAs) for research projects
- assessing the volume of data requested in order to adhere to data minimisation principles
- assessing and agreeing the appropriate classification of the data share
- being transparent around the classification of data shared with third parties
- agreeing proportionate licence periods and destruction dates

As such, requesters must provide with details on how they meet their obligations under GDPR.

Section Five: Safe Data

The purpose of this section is to evidence that the data you are requesting is entirely aligned to the research goals, that the sensitivity is understood, and that sensible steps to minimise the amount of individual level data accessed have been taken. As such, requesters must provide:

- Their data requirements and justification for the volume of data requested
- If relevant, an explanation as to how often the project needs to refresh its data to reach a satisfactory outcome
- The length of time the project needs access to the data and why

Section Six: Data Linking

The purpose of this section is to gather further details on applicants who plan to link the data they are seeking to access to any other data.

Section Seven: MoJ data

The purpose of this section is to gather further details on applicants applying specifically for data held by MoJ.

Section Eight: MoJ/DfE data share

The purpose of this section is to gather further details on the applicants applying for the MoJ/DfE data share.

Each permitted user must submit:

- A copy of a ‘basic disclosure’ certificate that is no more than 2 years old for each permitted user.

Access to the DfE extract of the share is provided by the ONS SRS. Access to the ONS SRS is provided through Safe Settings. These are either Physical ONS datalabs (currently in Newport, London, Titchfield, Belfast or Glasgow), or SRS remote connectivity sites if your organisation has successfully applied for full connectivity, partial connectivity or safe room connectivity.

Please be aware that if you do not have connectivity within your organisation, you will only be able to use ONS SRS Physical datalabs. Please contact research.support@ons.gov.uk if your organisation wishes to apply for remote connectivity.

If you require access to the MoJ extract, please contact DataLinkingTeam@Justice.gov.uk to discuss the access mechanism.

Section Eight B: MoJ/DFE data share: DfE extract

This is a further section for respondents wishing to apply for DfE's extract of the MoJ DfE data share.

Classification of the Data Share

DfE has revised the classifications that we use to describe external and third party data shares of individual level data to "individually identifiable" data or "de-identified individual" data and sensitivity level A to E.

In order to determine the most appropriate classification of the data share, each data variable within each dataset has been categorised for identification risk and sensitivity in the data tables.

Identification risk

This is the risk of identifying the individual when sharing individual level records and can be described using the following classifications:

Label used in transparency publication	Type of identification risk	Description	Example
Individually identifiable data	Instant identifiers	These are things which allow you to instantly 'point to' a person in data	Full name, Full Address
	Meaningful identifiers	These are things that very quickly allow you to identify someone or link with other known datasets	Unique identifiers (e.g. ULN, UPN)
De-identified individual data	Meaningless identifiers	These are things that are used within a dataset, but have no meaning beyond the dataset's boundaries	Pupil Matching Reference (PMR) number

Label used in transparency publication	Type of identification risk	Description	Example
	Other high risk data variables	These data variables do not in themselves identify individuals, but may in combination with other data variables increase the risk of identification	Home Postcode, Educational establishment codes, Free School Meal flag, Salary Spine Point

Sensitivity level

This is the sensitivity (including special categories of data) of the individual level data that will be shared). It is categorised into the following:

Sensitivity level	Description	Example
A	Public commitment never to share this data with anyone outside DfE	Pupil's nationality, Pupil's country of birth, proficiency in English language, NCCIS characteristic1 variable, Alternative Provision placement reason
B	Highly Sensitive: Highly Sensitive: Contains data about interactions with Children's Services	Data from children in need and children looked after datasets
C	Sensitive data not classed as a special category under GDPR but a public expectation would be that we treat it equally	Free School Meals, Some elements of Special Educational Needs.
D	Sensitive data captured as a special category under GDPR	Ethnicity, Gender, Sex, Language, Disability, Health, Religion, Some elements of SEN that have health angles.
E	Other, non-sensitive data variable	Exam Results

Section Nine: HMCTS data

The purpose of this section is to gather further details on applicants applying specifically for data held by HMCTS such as magistrates' courts data or other primary research drawing on HMCTS sources.

Section Ten: HMCTS primary data collection

The purpose of this section is to gather further details on applications applying for HMCTS primary data collection.

Section Eleven: Accessing data through your own secure setting

The purpose of this section is to gather further details on applicants applying to access the requested data through their own secure setting via a data share agreement.

Storage

Please understand that some data held is extremely sensitive and if lost or released, could cause considerable harm or distress. While this risk will be reduced by pseudonymising and minimising the data shared, additional steps must be taken to further reduce this risk. Please be aware that due to the sensitive nature of this data, your ordinary methods of storing data may not be sufficient.

Specifically, we would favour storage on a system certified at ISO 27001, holding Cyber Essentials accreditation, or compliant with the Information Governance Toolkit. Should your system not be compliant with these standards, we will refer you to guidance by the National Cyber Security Centre and may require it to be approved by our internal cyber security advisors.

Transfer

There is no ideal method of transferring data which suits every request. While we prefer using Criminal Justice Secure Mail (CJSM) where possible, we acknowledge that this may not always be a suitable option, and we can adjust depending on the needs of the individual share. While we encourage you to make suggestions should CJSM not be suitable, we may in some circumstances need the proposed method of transfer to be approved by our internal cyber security advisors. We require all mechanisms to be HGM Security Framework compliant. The HMG Security Framework can be found via the following link: https://www.gov.uk/government/publications/security-policy-framework

Deletion

The final step of a data share will be the deletion of the data which we have shared with you. Ordinarily we will accept written confirmation of the deletion via widely available commercial software. In some circumstances we may require you to provide proof of deletion from a National Cyber Security Centre approved contractor. However, such methods will only be necessary where the data shared is of a particularly sensitive nature.

Section Twelve: Accessing data through ONS Secure Research Service

The purpose of this section is to gather further details on applicants applying to access the requested data through the ONS SRS.

Check and Send

This section is an aide memoire for researchers to check they have filled in all the relevant information on the application form and have gathered all the appropriate documentation for submitting with the application form. Researchers may also find the following section helpful when filling in the form.

If you have any queries regarding the application form and/or the process of applying for data, please do contact the relevant email dependent on the data you are requesting:

- MoJ held data: datalinkingteam@justice.gov.uk
- HMPPS Data First data: datalinkingteam@justice.gov.uk
- HMCTS held data: dataaccesspanel@justice.gov.uk
- MoJ/DfE share
    - DfE extract: data.sharing@education.gov.uk
    - MoJ extract: datalinkingteam@justice.gov.uk

If you have any queries regarding the ONS secure research service, please do contact research.support@ons.gov.uk

This section provides further guidance on how to complete each section of the application form

Section One: Data Access

Data you require access to	This application form is for data held by MoJ, data held by HMCTS, HMPPS Data First data[2] and the MoJ DfE share. Please state what data you are requesting, if you are unsure what your request falls under please see the 'Available data and their modes of access' document.
How do you want to access the data	There are various options for accessing data depending on what data you request. Please see the 'Available data and their modes of access' document for your options for accessing data.

Section Two: Applicant Details

Name of requesting organisation. (This must be the name of the person or organisation who is requesting access):	The "Requester" is "The person or organisation to whom it has been agreed to permit the use of Data under this Agreement, as specified in the Schedule". Please state the name of the requesting organisation and the type of the organisation (e.g. academic organisation, independent think tank, public authority under FOIA, commercial organisation) etc).
Primary, Secondary and DPO contact details	Please ensure email address and phone number are included. Under the GDPR, you must appoint a DPO if: • you are a public authority or body (except for courts acting in their judicial capacity); • your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or • your core activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences. If you do not have DPO, please supply an explanation as to why you do not have one.

[2] MoJ Data First Criminal Courts Prisons and Probation Linked Dataset, the MoJ Data First Prisoner Custodial Journey Level Dataset, and the MoJ Data First Probation Dataset.

ICO number	There is a new Information Commissioner's Office (ICO) registration and fees model. It is a three-tier system based on staff numbers and turnover. Every organisation or sole trader who processes personal information needs to pay a data protection fee to the ICO, exemptions still apply. Please provide your ICO registration number or evidence of a valid exemption.
Contact details of institute/ organisation funding, sponsoring or commissioning the project	It is important for us to understand the key stakeholders involved in the project and the bigger picture / context in which the project sits in order to make a robust decision as to whether or not to support the data share. Please provide all relevant details and the nature of the relationship between those organisations. Please state “N/A” if some of the contact details are not necessary for the data share.
Data protection training, Analytical skills and experience with types of data	It is important for us to understand the skills of the team to assess the application. For example: what level of qualification or years of professional experience do the team have (e.g. PhD with 1 year academic research experience, BSc with 5 years as data analyst)? What kind of data protection training has been done and how recently? Have you worked with this data previously, or with similarly structured datasets or on related topics? Have you previously used the requested platform to access data?

Section Three: Project details

Brief Purpose	This summary should be no more than 150 words. It must be succinct but comprehensive. It must accurately describe the project in layperson's language and in the third person with no jargon. It is strongly recommended that the summary follow the structure below to ensure consistency and ease of reading when publishing alongside other data shares.
	
	We recognise that this is a difficult task for some projects and will gladly help applicants summarise their project. We have the right to amend the summary, in consultation with the applicant, to ensure the wording complies with GOV.UK guidance on all publications.
	
	[Organisation 'A'] wishes to analyse [dataset 'B'] for ['C' last x years' worth of data or y data for z year(s)]. With this data, [Organisation A will ['D' insert a 3–4 sentence description of the research]. The public benefit of this work will be ['E' insert here… how do current or future members of the public, particularly subjects of the dataset, benefit from this?]]
	
	Where:
	• A is the organisation who is applying for the data
	• B should consider:
	  • the relevant dataset(s) the requestor is applying for
	  • whether there is any linking involved
	  • whether there is any matching involved and the sample sizes or control groups involved
	• C should consider:
	  • how many x years' worth of data would be required
	  • whether every z years would be enough (e.g. every 3rd year)
	• D is 3–4 sentences describing the research aims and objectives of the project or the specific question the organisation is seeking to answer. This should also cover the intended outcome and publication method.
	• E is an explanation of how current or future members of the public, particularly subjects of the dataset, benefit from this. This may also include an explanation of the benefits to wider policy development (if known)

Fuller description of your project	Data must only be collected, and shared, for specified, explicit and legitimate purposes. It must not be used in a manner incompatible with the specified purpose. There are limited exceptions for archiving, scientific and historical research.
	
	This section allows the applicant to elaborate on their project's aims and objectives, intended methods, outputs and benefits, which meets the 'public good'. Please provide concise but comprehensive information sufficient to allow the corresponding panel to make a robust decision. You should include the following:
	• the project's purpose, please state:
	  • any research questions being addressed,
	  • how it meets MoJ's areas of research interest,
	  • connection to the policy of goals of the data owner(s),
	  • any organisations or processes reliant on this data request for their needs and why (e.g. completed as part of a public duty, i.e. 'public task'),
	  • whether any re-use of data is wholly aligned to the project's original purpose
	  • whether there have been similar projects carried out and whether this project is designed to fill a gap.
	• the project's intended methods, please consider:
	  • sample size requirements
	  • control group requirements
	  • statistical methods you might use
	  • how you will ensure quality
	• Data obtained under the Digital Economy Act for research purposes should consider its benefits to public interest. Research in the public interest is research whose primary purpose is, for example, to:
	  • to provide an evidence base for public policy decision-making;
	  • to provide an evidence base for public service delivery;
	  • is research whose primary purpose is, for example, to:
	  • provide an evidence base for public policy decision-making;
	  • provide an evidence base for public service delivery;
	  • provide an evidence base for decisions which are likely to significantly benefit the economy, society or quality of life of people in the UK, UK nationals or people born in the UK now living abroad;
	  • replicate, validate, challenge or review existing research and proposed research publications, including official statistics;
	  • significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; and/or,
	  • improve the quality, coverage or presentation of existing research, including official or National Statistics.

Project Outputs	The project's intended outputs and their uses, please state whether it is: • Internal work (publication not intended at this stage) • Freely available research findings / reports • Chargeable research findings / reports • Research findings / reports for use by the media • Free software products / web tools for data analysis (open access / restricted access) • Chargeable software products / web tools for data analysis (open access / restricted access) • Research commissioned by public sector bodies including government departments Other – please state. Note: if a piece of research is freely available in some way, but also exists within a journal requiring a submission, 'freely available research findings' can still be ticked.
Publishing Results	We strongly encourage researchers to publish their results. If you are not intending to publish your outputs, please explain why. A justification will be necessary for access to be granted.
Providing results two weeks prior to release	One of the conditions of accessing data is that researchers must provide any written or record outputs that will be made available publicly (e.g. books, articles, etc.), at least two weeks prior to release. However, all academics and researchers are free to publish all results/findings without interference from the MoJ other than to ensure our responsibilities under law, e.g. Data Protection Act 2018, are not breached.
Impact of not acquiring the data	Please provide the impact on your research if you do not get the data you are requesting.
Data sought from another source	Please consider whether the data being requested can be sought from another source.
Main limitations	Please provide the main limitations of your research proposal.
Timeframes	Please provide the timeframes for your research / project. Please include in your response any milestones that are critical and explain why. This is to help us prioritise your request.
Ethics	To ensure the appropriate approvals are in place for the data share, please disclose any previous research ethics panel approvals (e.g. university ethics board) and provide an overview of their considerations. Please also provide a summary of your main ethical considerations and mitigations.
Risk register and mitigation	What are the key risks of your proposal and how do you intend to mitigate them.

Section Four: GDPR

GDPR conditions for processing data	All researchers must tick a box that accurately describes the condition for processing data. Please refer to the ICO website if you are not sure which condition applies.
Justification	You must justify why you have chosen a particular condition and how you believe the condition is met. If relying on consent, please ensure you understand the changes in DPA2018 and GDPR, and provide adequate evidence (e.g. a copy of the consent form and privacy notices that are to be used for the project). These assessments will be verified or challenged during the approval process.
GDPR conditions for processing special categories of data	In addition, if your data request is for special categories of data (e.g. ethnicity, language, gender) you must also tick a box that accurately describes the condition (a to j) for processing special categories of data. Again, please refer to the ICO website if you are not sure which condition applies.
Schedule 1, Part 1 conditions	If your project is relying on (b), (h), (i) or (j), which condition of DPA 2018 Schedule 1, Part 1 does your project meet. You must justify this.
	If your project is relying on (b), (h), (i) or (j) of Article 9(2) of the GDPR and DPA 2018 Schedule 1, Part 1 (4) “Research”, please state whether it’s for archiving purposes, scientific or historical research purposes or statistical purposes and provide evidence on how your processing meets this condition (in particular how your processing meets Article 89(1) of the GDPR). You must provide evidence of compliance.
Schedule 1, Part 2 & 4 conditions	If your project is relying on (g), which condition of DPA 2018 Schedule 1, Part 2 does your project meet. You must justify this.
	Please also state how your project complies with DPA 2018 Schedule 1, part 4. You must provide evidence of compliance.
Further Justification	Extra space to provide further explanation if not already covered above.

Section Five: Safe Data

Data requirements	Please provide as much information as you can about the data your project requires.
	
	If requesting access to an existing dataset, system extract, or records you must provide the dataset or source name and the start and end dates required as well as any details of the subset of records needed for your project.
	
	If collecting primary data (e.g. interviewing court staff) please give detail about the sampling and scope of the data which you intend to gather.
	
	You should consider the following questions to support your application around the GDPR principle of data minimisation when applying for data:
	• Is the number of individuals / number of years / volume of records proportional for the stated purpose?
	• Do I really need data that I have listed?
	• Can you think of ways to minimise the data your require for your project, for example:
	  • request every 3rd year of data (i.e. years 1, 4, 7, 10) instead of the every year in the past 10 years
	  • request ethnic group instead of ethnic code

What data items to you require	Please provide us with an accompanying file such as an excel document that lists the variables you require and a justification for each variable. For example, is it a key outcome of interest for a research question; for subgroup analysis; or to be used as a control variable. Names and descriptions of data items available for some defined datasets is available on gov.uk. Please see the relevant data catalogues for Data First datasets and please contact the relevant secretariat for non-Data First datasets.
Future re-fresh of data	Please state whether your project requires one extract once or whether it relies on updates to the extract (e.g. every year) to reach a satisfactory conclusion. If we are satisfied with your reasons for refreshes of data, we do not require you to re-apply each time however, we reserve the right to review this agreement at any time in the future. You will be expected to be proactive in contacting us 2–3 months before new datasets are released to request a refresh of data.
Research licence end dates	We need to know how long researchers require the data for and what they need the data for in each stage of their project so we can assess whether that is a justifiable length of time.

Safe Outputs	Please detail your current policies on statistical disclosure control and how you plan to ensure no sensitive data is released. SDC should comply with the Government Statistical Service (GSS) Guidance on Anonymisation and Data Confidentiality (https://gss.civilservice.gov.uk/policy-store/anonymisation-and-data-confidentiality/). All outputs must also comply with the DPA and GDPR. A minimum cell count of 10 shall apply unless written permission is obtained on a case-by-case basis. The SDC applied by the Data Processor shall ensure that no person, organisation and/or business will be; • Specified in the information • Able to be deduced in the information • Able to be deduced from the information taken together with any other publicly available information And further ensure that: • Self-identification is not possible • Appropriate disclosure control has been applied to the position of zeros in any output tables (not just cell counts) • It is not possible to use information in tables to deduce information about the characteristics of a person, organisation or business.

Section Six: Data Linking

Data you want to link	Please provide us with details on the data you would like to link, including fuller details of any data held independently from this application request.
Linking data	Please describe how you plan to link the data. Which identifiers will be used as the link to carry out the data matching?
Requirement for data linking	Please describe why your project requires data linking and the impact of you not being able to link data.
Consent	Please state whether you have explicit consent to link. If not, please state the legal basis for linkage. If so, please provide a copy of the consent used.

Section Seven: MoJ data

Data held	If the answer is yes, please describe any data that you already hold from the Police National Computer and the retention period.
National Research Committee	If the answer is yes, please provide details on how you have engaged with the National Research Committee and the results of any application for related data.
Contacts in MoJ	Please give contact details for anyone you have consulted on this request or that you know has an interest in its outcome. We may contact those listed to seek their views on its value.

Section Eight A: MoJ/DfE data share

Do you require access to MoJ or DfE's copy	Access to the DfE extract of the share (to contextualise it with the wider pupil population) is provided by the ONS SRS. Access to the ONS SRS is provided through Safe Settings. These are either Physical ONS datalabs (currently in Newport, London, Titchfield, Belfast or Glasgow), or SRS remote connectivity sites if your organisation has successfully applied for full connectivity, partial connectivity or safe room connectivity. If you require access to the MoJ extract, please contact DataLinkingTeam@Justice.gov.uk to discuss the access mechanism.
Individual checks	Each person who will be using the data must provide hold a 'basic disclosure' certificate that is **no more than 2 years old** and have signed an individual declaration form that forms the basis of the DfE data sharing agreement. Please provide contact details of all individuals. You must submit these with the application form. Your application will be rejected if the majority of certificates are not submitted. However, you need not delay your application if you are waiting for 1 or 2 individuals if you have the majority of 'basic disclosure' certificates. The data will be made available to those individuals once they have received their 'basic disclosure' certificates. In some cases, applicants cannot find their DBS certificate. With the individual's consent DfE can gain permission to their DBS certificate on the DBS database. Please state "Yes" in the relevant individual's row if you would like us to do this on your behalf. In order to gain access to data from the SRS, each person must have gone through the accreditation process. It is advisable for each individual to contact research.support@ons.gov.uk before submitting this application form.

Legal Gateway	Please tick the legal gateway you believe is relevant for the data share. If you think there is a legal gateway missing please contact data.sharing@education.gov.uk
Individual Rights	In this section of the form, DfE have provided advice on how we handle the rights of individuals. Requesters should use this section to demonstrate how their organisation handles the rights of individuals. Whilst some of these individual rights might not be applicable to the project, we would expect every organisation to at least have a privacy notice on their website so that the public can understand how the organisation handles personal data.
Commercial Aspects	There are a few questions relating to whether or not your data share is intended to generate a financial profit or not. The more information you can provide the better so that we can consider your request properly and in a timely manner. Otherwise, we may have to seek clarifying information which may slow down your application.

Section Eight B: MoJ/DfE data share: DfE extract

Sensitivity of the data requested	You are asked to familiarise yourself with DfE's classification system (section 7 above) and work out the sensitivity level (B, C, D, E) for your data request. Data variables of sensitivity level A are not available for data sharing from DfE. You must tick all of the sensitivity levels that apply for your data request. To undertake this exercise you must look at the data variables you want in the data tables and the data variables in the standard extracts and their corresponding sensitivity level. If you tick sensitivity level D, you must make sure you provide an additional condition of processing for special categories of data in section.
Justification	If you require data variables with sensitivity levels B and D, you are asked to justify why you require this data.
Identification risk of the data requested	You are asked to familiarise yourself with DfE's new classification system (section 7 above) and work out the identification risk level (1, 2, 3, 4, 5) for your data request. You must tick the highest risk level that applies for your data request. To undertake this exercise you must look at the data variables you want in the data tables and their corresponding sensitivity level.
Justification	If you require data variable with identification risk 1 and/or 2 and/or any data requested from the data tables top table.

Section Nine: HMCTS data

Jurisdiction	Please outline what jurisdiction your research/data collection covers.
Data	Please outline what data you are seeking access to?
Contacts	Please outline any contacts in HMCTS with whom you have discussed the value or feasibility of this research.

Section Ten: HMCTS primary data collection

Collection Method	Extracts from IT systems: It may be possible to extract data from an existing IT system. The Data Access Services team will make enquiries as necessary once the application has been received and it is clear what data is being requested. If you know which IT system the data is to be extracted from, please provide details Interview: Please see box below Examination of case files: Please see case identification box Other: Covering anything not mention above with full explanation in the methodology
Interviews or Questionnaires	If you are seeking to collect data or information via interviews please detail one of more of the options below. • **HMCTS admin staff** You must supply an outline of the areas under discussion and the questions in advance. • **HMCTS legal staff** You must supply an outline of the areas under discussion and the questions in advance. • **Court/Tribunal users** You must supply an outline of the areas under discussion and the questions in advance. • **Judiciary** If your proposed activity is to interview the **Judiciary only**, no DAP application is required but contact should be made with the Data Access Services team. Senior Judicial Agreement is required and must be obtained by applying directly to the Judicial Office researchrequest@judiciary.uk. Further guidance relating to **Judicial Participation in Research Projects** can be found at: http://www.judiciary.gov.uk/publications/judicial-participation-in-research-project
Case Identification	Research requests will often seek to involve access to case files. Inevitably, data held in case files and other court or tribunal records (including electronic systems) can be of a sensitive and personal

	nature and access to those records is subject to legal restrictions – most notably the Public Records Acts 1958 & 1967, Freedom of Information Act 2000 (FOIA), Constitutional Reform and Governance Act 2010, Data Protection Act 2018, and General Data Protection Act 2018 (GDPR). However, the Departmental Records Officer (DRO) will consider granting permission to view such records under supervision to researchers whose DAP applications have been approved. If this is granted, researchers will be required to sign a Privileged Access Agreement (PAA) which sets out the terms of the access and reuse of the records. This is a privilege which we offer outside of the FOIA regime. PAAs are not required for researchers employed by HMCTS or the MoJ or for research requests covered by a Data Sharing Agreement. If a PAA is required for your application, we will contact you about next steps.
Applying for a Privileged Access Agreement (PAA)	In an agreed and secure way, you will need to identify the case files you wish to inspect before the DRO will consider granting a PAA. Please set out in the application form or methodology the exact data you hope to extract from the files and what arrangements, if any, you have made to identify the cases involved. Court and tribunal staff must receive a list of specific cases to be able to retrieve the files, or appropriate parameters from which to select files (e.g. all trials on a day). You may however, be uncertain about whether case files contain the information you need, or how to identify a sample of case files for your study. In these circumstances, we suggest that you complete all parts of this application as fully as possible and request a two-stage approach. 1. A feasibility stage to test the availability of data and if this is successful, 2. A main stage of data collection. A PAA may be required ahead of the feasibility stage. If this applies to your application, we will contact you about next steps. The Data Access Services team will find out what support and guidance court staff might be able to provide to help identify suitable cases. A substantial proportion cases can be identified through central electronic databases held by HMCTS. The feasibility stage would involve your request to conduct a limited study to ascertain whether the information is held in the case files and how you will select files for your study. You should clearly set out in your application, details of the information you want to find. The likely points to be clarified include: • a list of specific types of case kept; • how are the cases logged; • how are the files stored;

	• can the specific cases be identified; • what data are contained on the 'file'; • how can a list of cases be created so it can be attached to the PAA, or if the aim is to be completely random, how best that can be achieved and be statistically robust? It must be stressed that agreement to the feasibility stage does not necessarily imply agreement to the main study. Each application will be assessed on the comprehensiveness of the information supplied and the impact of the research on the operation of the courts and hearing centres. These are subject to time and case volume pressures and staff may not be able to accommodate additional demands.
Number of cases to be reviewed	Attention should be given to the balance between (i) the effort to find and extract the number of files; (ii) the location of the files; (iii) whether the files are completed or on-going cases; (iv) the likelihood the files contain the required data and in what way.
Impact Assessment	Please give an estimate of the burden for each HMCTS Business Area affected, indicating in 'person days' how long it will take each area to complete the exercise. In the table please state in the column 'Per Court/Office' the number of 'person days' for each business to provide the information. A 'person day' is equal to 7.2 hours. If your request includes looking at data with personal identifiers held within case files, you must remember to consider the time it will take for HMCTS staff to retrieve and replace files, from various (including off-site) storage arrangements. General access to court files is not allowed. In the column 'Number of locations to be visited / affected', please provide the number affected against each business area.

Section Eleven: Accessing data through your own secure setting

Transfer	Please explain how you plan to transfer the data. There is no ideal method of transferring data which suits every request. While we encourage you to make suggestions, we may in some circumstances need to run the proposed method past our internal cyber security advisors. We require all mechanisms to be HGM Security Framework compliant.
Storage	Please explain how you plan to store the data. Specifically, we would favour storage on a system certified at ISO 27001, holding Cyber Essentials accreditation, or compliant with the Information Governance Toolkit

Incident reporting	Please detail your policy around incident reporting
HMG Security policy framework	The HMG Security Framework can be found via the following link: https://www.gov.uk/government/publications/security-policy-framework
Destroying the data	Please detail how you plan to destroy the data. You must ensure it is destroyed to government standards for secure and complete destruction.
Legal Gateway	Please detail the legal gateway you believe is relevant for the data share.

Section Twelve: Accessing data through ONS Secure Research Service

File Formats	ONS SRS can provide access to your data extracts in SPSS, SQL database or tab-delimited text file. If these are not suitable for your analysis please contact research.support@ons.gov.uk to see if your chosen software can be supported.
Software	ONS SRS provide a wide range of software suitable for many different types of analysis. Requesters will need to justify why they believe more niche software products are required for their analysis.