



Data Protection Impact Assessment – Scottish Crime and Justice Survey

Template produced by Information Assurance and Risk

Version published: July 2023



Scottish Government
Riaghaltas na h-Alba

Data Protection Impact Assessment (DPIA) – Scottish Crime and Justice Survey

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the running of the Scottish Crime and Justice Survey, and the data processing undertaken as part of the project.

2. Document metadata

2.1 Name of Project: Scottish Crime and Justice Survey

2.2 Author of report: Mark Bell

2.3 Date of report: July 2023

2.4 Name of Information Asset Owner (IAO) of relevant business unit: Amy Wilson, DD Justice Analytical Services

2.5 Date for review of DPIA

Review date	Details of update	Completion date	Approval Date
July/August 2018	Adding additional info from SCJS contractor.	25 th July 2018	25 th July 2018
March/April 2020	Annual review.	31 st July 2020	4 th August 2020
August 2020	Adding additional info about telephone survey.	25 th August 2020	26 th August 2020
November 2021	Adding additional info about return to SCJS interviews	11 th November 2021	11 th November 2021
June 2023	Adding additional information about sharing datasets to the Scottish National Safe Haven.	29 June 2023	29 June 2023

3. Description of the project

3.1 Description of the work:

Overview

The Scottish Crime and Justice Survey

The Scottish Crime and Justice Survey (SCJS) is a large-scale, nationally representative social survey which asks adults about their experiences and perceptions of crime. The SCJS provides robust evidence on the extent, prevalence and nature of crime in Scotland, and also collects information on the population's experiences of and attitudes towards the criminal justice system in Scotland.

Interviews are conducted with a sample of adults living in private households. Respondents are interviewed in their home face-to-face using Computer Aided Personal Interviewing (CAPI), and Computer Aided Self-completion Interviewing (CASI) for the self-completion element of the survey which contains more sensitive questions. If a respondent refuses a face-to-face CAPI interview due to concerns about the transmission of COVID-19, they are offered an interview by phone or video chat. In these cases, the respondent is sent an online version of the self-completion survey.

The sample is drawn from the Royal Mail's Postcode Address File, which includes address and postcode information. Personal information such as name and age, and special category data (such as sexual orientation) are collected during the interview. These data are aggregated to enable experiences and trends of different population groups to be examined, in line with the aims of the survey.

Benefits

The main aims of the SCJS are to:

- Enable the Scottish population to tell us about their experiences of, and attitudes to, a range of issues related to crime, policing and the justice system; including crime not reported to the police;
- Provide a valid and reliable measure of adults' experience of crime, including services provided to victims of crime;
- Examine trends, over time, in the number and nature of crimes in Scotland, providing a complementary measure of crime to police recorded crime statistics;
- Examine the varying risk and characteristics of crime for different groups of adults in the population.

The findings from the SCJS are used by policy makers to help understand the nature of crime in Scotland, target resources and monitor the impact of initiatives to improve lives. The results of this survey provide evidence to inform national outcomes and justice outcomes. In particular, the SCJS provides evidence for three National Indicators in the National Performance Framework (crime victimisation rate; perception of local crime rate; access to justice).

The SCJS is also used by Police Scotland and other justice organisations to help monitor performance and understand the public's experiences and interactions with those services. Third sector organisations use the SCJS for evidence on the extent of issues which are not obtainable from other sources (such as the prevalence of partner abuse). In turn these organisations use the SCJS to inform and justify activity. Academics and other researchers use the SCJS to further explore experiences of crime in Scotland – for example, looking at how patterns of different kinds of violence have developed over time. The SCJS facilitates analysis and therefore understandings which are not

currently obtainable from other evidence sources. For instance, whilst Police Recorded Crime data is a valuable resource, it does not include crimes not reported to or recorded by the police and how experiences vary across the population to the same extent as the SCJS.

When the SCJS is made available to the Scottish National Safe Haven, researchers will be able to link it to other datasets to increase the possibilities for research.

Ownership and roles

The Scottish Government (SG) is the data controller and is responsible for the governance of the project. The current contractors, a consortium of Ipsos and ScotCen, are data processors. Both contractor organisations collect the information directly from respondents, before cleaning, checking and preparing the data for analysis, analysing the data, and transmitting finalised dataset and data table outputs to SG. SG then undertakes further analysis of the data as detailed below.

Overview of data processes

Analysis of main survey results

SG's SCJS team receives outputs from the contractors in the form of SPSS data and aggregate tables called data tables and web tables. The SPSS datasets do not include any direct identifiers (such as name, address, postcode). The datasets are stored in restricted folders on the SG's secure servers. The datasets are used to undertake analysis to meet the goals of survey outlined above. Results from the survey are published in reports and online tables based on aggregated groups (e.g. experiences of males, 16-24 year olds etc.). No results are published where the base size is less than 50 respondents. As a result no individuals are identified or identifiable from the published SCJS results.

Only a small number of named analysts within SG have access to and process the datasets provided by the contractors.

Sharing survey data

The Scottish Government also considers requests and, where approved, provides disclosure controlled datasets to reputable researchers / research organisations (such as academics) for the purpose of further research. These datasets are modified versions of the SPSS datasets provided by the survey contractors and do not include direct identifiers (such as name, address or postcode). Further disclosure control methods are applied to these datasets and include the following techniques:

- Re-coding is used on categorical variables to collapse response categories together into larger groups to hide small numbers of respondents in some of the smaller groups;
- Top (or bottom) coding is used on numerical variables such as age;
- Variable removal is used to remove:
 - sensitive variables;
 - variables used to calculate summary variables which can be disclosive if not recoded, or used to help identify respondents in combination with other variables;
 - variables that helped with the administration of the survey fieldwork.

SCJS datasets are available from UK Data Service through an End User Licence although a special license request must be made in order to access and use sensitive information (such as the victim

form and self-completion data of the SCJS), or directly from the Scottish Government as a [special dataset](#) via a Data Sharing Agreement.

Each request for SCJS data through a special dataset request direct to SG or special licence request to the UK Data Service is assessed on a case-by-case basis and signed off by the Information Asset Owner (IAO) before any datasets are transmitted. Data Sharing Agreements are produced to detail the nature of the processing to be undertaken and also set out retention/deletion policies. Only the data required for the proposed project is shared, and data shared are also taken from the disclosure controlled dataset shared with the UK Data Service, unless a specific request for the full dataset is requested and considered to be appropriate. In line with our own analysis and publication approach, SG recommends that those analysing the data do not publish results where the base size is less than 50.

Full details of the disclosure control methods are published alongside the datasets, at: <https://beta.ukdataservice.ac.uk/datacatalogue/studies/study?id=8498#!/documentation>.

The main survey results are also available to those registered with the UK Data Service through their [NESSTAR](#) platform.

Recontact data

A separate file with direct personal identifiers for those who consent to providing their details for potential follow-up research is collected and provided to SG. A unique serial number is allocated to each respondent in the main datasets and recontact dataset in order to facilitate potential future matching for the purposes of follow-up research. This dataset holding recontact information is only accessible by the SCJS Project Director and all requests to use the recontact list are considered on a case-by-case basis. Where relevant, further details of the processes and protocols around the recontact data are provided throughout this DPIA.

Governance

A governance structure is in place to provide oversight and offer guidance and support in the running of the project. Figure 1, below, shows the key elements of the structure.

Figure 1: Project Governance



The Project Board is chaired by the IAO as Project Executive¹ and consists of senior SG representatives with key stakes in the project. It has overall responsibility and provides oversight for the project. Risks to the quality, value and timing of the SCJS are brought to the attention of the Project Board. In the event of any data breach, the matter would be reported to the Project Board, alongside the standard SG data breach reporting processes being followed.

The Project Management team manages the SCJS on a day-to-day level, including management of the contract. Where tolerances are exceeded, the Project Management team is responsible for elevating issues/providing recommendations and supporting evidence where relevant to the Project Board to help it make effective decisions. The Project Management team consists of a small number of analysts within SG's Justice Analytical Services (JAS). Within SG, the SCJS datasets are largely processed by the Project Management team, and occasionally a small number of additional JAS analysts undertaking/contributing to work on the SCJS (e.g. analysis and report writing).

Analysts within SG's Office for Chief Statistician (OCS) provide technical overview and support, and are also responsible for survey sampling and weighting. Therefore, data processing is also undertaken by a small number of analysts within OCS.

Ipsos and ScotCen (the survey contractors) are responsible for the data collection and provision of quality assured data outputs to SG, as detailed elsewhere in this DPIA. Data are collected and processed under instruction from SG, in line with the main SCJS (Controller-Processor) contract. Necessary steps are in place within each contractor organisation to ensure that data is collected and processed appropriately. For example, access to personal data is restricted to only those who require access to such information in order to produce datasets suitable for analysis.

¹ Prior to the Covid-19 suspension the Project Executive was the Director of SG's Safer Communities Directorate.

Planning mechanisms

Planning is undertaken by the Project Director, in collaboration with the Project Management Team, and forms part of wider business planning undertaken by Justice Analytical Services. With respect to data processing, plans are generally in place and already documented for the range of processing activities undertaken using SCJS data. However, the annual review of the DPIA and annual business planning activity offers an opportunity to consider any planned changes or improvements to data processing mechanisms which have privacy impacts.

Part of the annual planning process also considers who in SG will be working with SCJS data over the coming year, and therefore who requires access to the restricted folder where the data files are stored. Anyone who no longer requires access has the privileges removed.

Reporting mechanisms

Once analysed, SCJS results are published in reports and online data tables by SG at an aggregate level, with no results published where the base size for a particular question/group is lower than 50. This prevents individuals from being identifiable.

The datasets are made available to reputable research organisations/researchers for legitimate purposes as detailed in the 'Ownership' section of this document. Disclosure control processes applied to the data help to reduce the risk of individuals being identifiable.

In terms of data breaches which affect personal data/privacy:

- within SG – data breaches would be reported to the Project Board (including IAO) and the general SG reporting process would also be followed.

- by/within the contractor consortium – as detailed in the contract held between SG and Ipsos/ScotCen, each organisation operates a security incident recording system and any breaches experienced would be communicated immediately to the Scottish Government, who would in turn follow the internal processes as appropriate.

- by research organisations / researchers who obtain data through UK Data Service / Special License Agreement / Data Sharing Agreement (DSA) – datasets provided are generally disclosure controlled to minimise the risk of individuals being identified, and SG recommends that no results based on fewer than 50 respondents should be published. However, if a data breach with an impact on data protection/privacy were to take place the procedures set out in the 'Management of a security incident' section of the DSA would be followed. This includes immediately notifying the Scottish Government.

Risk and Issue Management

A risk log tracks risks associated with the SCJS, with risks assigned to owners, which can also be used to highlight how decisions taken may impact on the identified risks. Live SCJS project risks are currently documented within a Risk Register covering a range of operations and projects delivered by the Scottish Government's Justice Analytical Services. This helps to ensure the IAO and senior officials are aware of project risks.

Most risks are managed by the SCJS Project Team in collaboration with the SCJS contractors, the Project Board and OCS where required. Where project tolerances are exceeded (or where the risks

or issues are owned by members of the Project Board), the Project Board will be responsible for resolution.

With respect to data specifically, the main risk is that data which enables individuals to be identified could be released/accessed by those who do not require or merit access. Numerous steps are in place to prevent this from occurring, for example:

- access to SCJS data within SG, Ipsos and ScotCen is restricted to the named individuals who are actively working on the project.
- when datasets are transmitted between Ipsos, ScotCen and SG (or two of the three), a secure FTP site is used, with access restricted to named individuals.
- direct personal identifiers (within the recontact list) are held separately from the main survey datasets, whilst a unique serial code for each respondent allows them to be re-matched. Within SG, only the Project Director (and members of the IT team who oversee the SG servers) have access to the area of the server containing the recontact list and therefore the direct personal identifiers.
- results are published on aggregated groups, with no results published by SG on groups of less than 50 respondents
- datasets available through the UK Data Service are disclosure controlled to prevent individuals from being identified.

As these processes are all standard procedures followed in the production and processing of SCJS data to minimise risk, at present the Justice Analytical Services (JAS) Risk Register does not currently contain a live entry on SCJS data issues. Should a new process or issue emerge which represents an increased or new risk to data protection, then an entry will be added to the JAS risk register and mechanisms put in place to ensure the risk is managed accordingly and to a suitable level. That said, there is an entry within the risk register covering the data processing undertaken by JAS generally to ensure corporate policies around processing data in accordance with data protection legislation are in place.

3.2 Personal data to be processed.

Variable	Data Source
Individual respondent serial number	Randomly allocated by contractor software to each respondent/sample point
Gender	Scottish Crime and Justice Survey interview
Transgender status	Scottish Crime and Justice Survey interview
Age	Scottish Crime and Justice Survey interview
Qualifications held (educational and vocational/professional)	Scottish Crime and Justice Survey interview
Employment details	Scottish Crime and Justice Survey interview
Sexual orientation	Scottish Crime and Justice Survey interview
Ethnicity	Scottish Crime and Justice Survey interview
Religion	Scottish Crime and Justice Survey interview
Physical and mental health	Scottish Crime and Justice Survey interview
Marital status	Scottish Crime and Justice Survey interview
Relationship to other household members	Scottish Crime and Justice Survey interview
Country of birth	Scottish Crime and Justice Survey interview
Household income	Scottish Crime and Justice Survey interview
Convictions (Note: question on whether ever convicted and what sentence received – no specific details of nature of conviction)	Scottish Crime and Justice Survey interview
Name	Scottish Crime and Justice Survey interview (for recontact/follow-up surveys – stored separately from main survey data).
Address	Scottish Crime and Justice Survey interview (for recontact/follow-up surveys – stored separately from main survey data). Address data also used for drawing survey sample – from Postcode Address File.
Postcode	Scottish Crime and Justice Survey interview (for recontact/follow-up surveys – stored separately from main survey data). Used to derive aggregate variables on area characteristics (e.g. urban/rural

	area; SIMD decile) – which are included in main survey dataset. Address data also used for drawing survey sample – from Postcode Address File.
Telephone number	Scottish Crime and Justice Survey interview (for recontact/follow-up surveys – stored separately from main survey data).
Email address	Scottish Crime and Justice Survey interview (for recontact/follow-up surveys – stored separately from main survey data).
Other sensitive data of note	
Victim form variables (questions used to determine whether a crime had occurred and details of that crime)	Scottish Crime and Justice Survey interview
Partner abuse variables (Self-completion dataset, questions used to collect information about experiences of partner abuse)	Scottish Crime and Justice Survey interview
Sexual violence variables (Self-completion dataset, questions used to collect information about experiences of sexual violence)	Scottish Crime and Justice Survey interview

3.3 Describe how this data will be processed:

How will the data be gathered?

The survey sample is drawn from the Royal Mail's Postcode Address File. Sampling information is held by the Office of the Chief Statistician. This is not personal data, but extracts of the Postcode Address File (i.e. address and postcode). They are nonetheless held on a secure server, and samples from 2012 onwards, when this work was brought in-house by the Scottish Government, have been retained.

Interviewers are provided with a batch of addresses (house number, street and postcode) to attempt to achieve an interview from. The sample itself contains no information about the household – all personal information relating to individuals is only collected if an interview is completed. The survey is completed with adults aged 16+ only, and largely collects information about them, but a small amount of information is also collected about other household members (e.g. relationship between household members) and the household as a whole (e.g. household income). This information is important for analysing the results by different breakdowns, and also assists with the weighting applied to the data to ensure it is representative of the Scottish population.

Interviews are voluntary and therefore only conducted where respondents consent to take part, although interviewers encourage people to take part by explaining the value of their contribution. It is important to note that the voluntary nature of the survey is key from an ethical perspective, but consent is not the basis on which the data are processed. The privacy notice highlights that the data are collected and processed in the public interest under the lawful basis of public task.

Answers to survey questions are provided by respondents to the interviewer who records the responses within the software for the respondents' chosen method for completing the survey on a secure laptop/computer - CAPI (Computer-Assisted Personal Interviewing). This includes collection of personal and special category data.

Some more sensitive questions (e.g. on experiences of partner abuse) are self-completed by the respondent, either by direct entry onto the laptop at the end of the CAPI interview via CASI (Computer Aided Self-completion Interviewing) or in their own time by CAWI (Computer-Assisted Web Interviewing). The interviewer does not see these answers in the vast majority of circumstances. In a small number of CASI interviews, respondents may request the interviewer's help with the self-completion section. Responses are inputted in the same way.

Respondents are free to refuse to answer any question they do not wish to, and can withdraw at any time during the interview. Where respondents withdraw, all of their personal data and wider survey responses are erased.

Following the interview, the completed record of interview answers and relevant personal information is uploaded to the contractor's (Ipsos or ScotCen as relevant) secure server for further processing in due course (checking, cleaning, analysing).

Whilst survey responses and personal information is collected at the same time (i.e. during the interview), steps are taken to separate these two sets of data after collection. After the data has been uploaded by interviewers to the central servers, the main SCJS survey datasets are pseudonymised (i.e. direct personal identifiers are removed) although broad categories (such as gender and age) are included for each respondent for the purposes of analysis. A separate file with direct personal identifiers is held for those who consent to providing their details for potential follow-up research. A unique serial number is allocated to each respondent in the main datasets and recontact dataset in order to facilitate potential future matching for the purposes of follow-up research.

Who will have access?

Within SG, the SCJS Project Team and a small number of other analysts working on the survey within Justice Analytical Services will have access to the datasets containing responses to the main survey, which does not include direct identifiers. Access is controlled through maintenance of a project group within the IT system with access rights which individuals have to be actively added to and removed from by the Information Management Support Officer (IMSO). Membership of the group is reviewed on a regular basis, to take account of staff changes for example. Only the Project Director (and SG IT team who maintain servers) will have access to the file holding the recontact data.

A small number of analysts within the Office of the Chief Statistician also have access to the pseudonymised survey results and the addresses of respondents for the purpose of allocating the sample, calculating the survey weights, fieldwork quality monitoring and for further analysis through the Scottish Surveys Core Questions (SSCQ) dataset.

Within ScotCen and Ipsos, the survey datasets are restricted to named personnel working on the project. They are held in a specific subfolder of the job directory, for which access is restricted by their IT departments. Personal (i.e. contact) details are stripped from the main datasets that the project teams work with.

The pseudonymised datasets of survey responses are submitted (following further disclosure control processes to merge small groups and minimise the risk of individuals being identified) to the UK Data

Service who make them available to researchers who wish to undertake further analysis of the survey data. The more sensitive data collected via the self-completion element of the survey and the victim form datasets are only available through Special License applications, which are assessed by the SCJS Project Team before datasets are transmitted. SG may also directly provide survey data to relevant research organisations on request. All requests are assessed and relevant Data Sharing Agreements drawn up before any datasets are transferred.

SG can also make the recontact data available to research organisations on request and following assessment of any applications. Applications are reviewed by the SCJS Project Director, and if necessary by the Scottish Government's Data Access Panel which is coordinated by the SG's Statistics and Data Access Division: [Scottish Government statistics: request our data - gov.scot \(www.gov.scot\)](https://www.gov.scot/statistics-and-data-access-division).

How will it be transmitted and how frequently?

The sample file is sent by secure file transfer from OCS (SG) to Ipsos for processing and batching. Once the sample has been suitably prepared and shared with ScotCen by secure transfer, the sample information is sent for the printing of advance materials (such as letters sent to addresses to let households know that an interviewer will call at their property). Ipsos printing is undertaken in-house, whilst ScotCen's external printing company sign a confidentiality agreement and files are deleted once printing has taken place. All data are transmitted securely. Printed materials are then issued to interviewers according to their batch allocation.

The main survey data are collected by interviewers on laptops (CAPI survey). This includes special category data and personal identifiers. Following the interview(s), the data are securely uploaded to central server for further processing to produce the survey outputs. On the central systems, the data are only accessible by named individuals working on the project. The data gathered by Ipsos is securely sent by secure FTP to ScotCen for further processing.

Information on address outcomes (interview, refusal etc.) and participant details (name, address etc.) is transmitted and stored separately, and only accessible by the project's field administration teams and system developers. For the purposes of quality assurance, some personal information is provided to a quality assurance team who undertake steps to validate the survey's completion (for approximately 10% of cases). After this, the data are deleted by IT staff and is again only available to the field team/system developers.

Once initially processed by the project team at ScotCen, the survey datasets are transmitted in SPSS format to the Scottish Government each year via a secure FTP site only accessible by the SCJS Project Team within SG (including central survey team in Office of the Chief Statistician). At the data delivery stage, the datasets are quality assured by the Scottish Government in collaboration with ScotCen. This checking can lead to a number of iterations of the datasets being sent over in a short period. These are all versions of the same datasets (in broad terms) and are all transmitted and stored in the same secure way. Superseded versions of the datasets are retained securely by SG for version control purposes. The various iterations of datasets pose no greater risk of individuals being identified.

When SG submit the data to the UK Data Service or share it with research organisations via a data sharing agreement secure file transfer methods are followed.

The recontact file is also supplied to SG via secure FTP at the conclusion of each survey year.

Survey data to be shared and linked to other datasets in the Scottish National Safe Haven will be partially sent by ScotCen to NRS for indexing, and the rest of the data sent to the safe haven where the dataset will be stored in pseudonymised form ready to be linked to other datasets.

How will it be stored?

SG receives SCJS data from ScotCen via an FTP facility. When retrieved from the secure FTP facility, the SCJS datasets are stored in a restricted file on the SG's secure server which is accessible to a small number of named analysts in Justice Analytical Services. When SCJS data is added to the [Scottish Surveys Core Questions](#) dataset by analysts in the Office of the Chief Statisticians (OCS) this is stored securely and separately. Data are also received by SG via the secure FTP facility.

The sample recontact datasets are stored in a separate restricted file only accessible by the SCJS Project Director (and the IT team who maintain the server – although they would only access the file if requested to do so in the event of IT issues, for example).

How will it be disposed of when no longer needed?

The pseudonymised SPSS survey datasets are retained indefinitely by the Scottish Government for the purposes of research. Data Sharing Agreements with research organisations specify the terms around retention and deletion for each specific case. The UK Data Service holds the disclosure controlled datasets indefinitely too, for the purposes of research. The SCJS contractors hold the SPSS datasets for each year for the duration of the current contract, in order to facilitate further processing as specified within the contract or as required by SG within the existing legal basis for processing. At the conclusion of the contract, all data shall be deleted by both Ipsos and ScotCen following a handover/phasing out period. If the study were to end, all data would be transferred to the Scottish Government and deleted by both Ipsos and ScotCen.

Once the interview has been completed, as the survey data are processed under the public interest clause, there is an exemption for research and statistics applied to the individual's right to have their data deleted. This is important for practical reasons relating to the main survey data as, once the survey data has been finalised and analysed, removing individuals responses would change the outputs and results derived from the data and therefore undermine the quality and integrity of the data as an evidence source. However, in practice, if respondents contact SG or the survey contractors within a few days of completing the interview (i.e. before the relevant data are cleaned, processed etc.), it may be possible to remove them from the dataset and such requests are generally progressed in recognition of the voluntary nature of the survey. In practice, this is very rarely requested.

Under GDPR it would be more usual to say that there is an exemption for research and statistics applied to the individual's right to have their data deleted.

Note on recontact data

Whilst the right to erasure does not apply to the main survey data, respondents who express a willingness to be invited to take part in follow-up research provide their contact details and are asked to provide explicit consent for such processing. Whilst these data are gathered in the same way as the main survey data (i.e. face to face) and as part of the interview, respondents are advised that they are free to withdraw their consent to be on the recontact list and therefore have their information *on this dataset* (i.e. personal contact details) erased at any time. Information on how to withdraw consent from this processing is provided within the privacy notice. Respondents are also left with a

letter which confirms they have agreed to be on the recontact list and how to withdraw. Any withdrawal of consent for recontact does not impact on the right to continue to hold and process the main survey data for such respondents (i.e. the datasets without direct personal identifiers).

The recontact data are correct at the time of collection but there is currently no mechanism in place for ensuring the data remains up to date into the future. As such, given that respondents may move address, change telephone number and so on, the Scottish Government assesses that these datasets should be disposed of after a maximum of 5 years. This balances up the assessment of the likely accuracy of the data over time with the potential utility of this dataset, whilst also recognising that it is stored securely with access restricted and that any request for use is robustly assessed on a case-by-case basis. Any further research undertaken with the recontact data will also include a clear opportunity for people to refuse to take part in or withdraw consent from the follow-up work. These data are permanently erased from the SG servers at the end of the relevant retention period.

The SCJS contractors delete the recontact data shortly after this has been received and signed off by the Scottish Government.

Who owns and manages the data?

The Information Asset Owner is Amy Wilson, Head of Justice Analytical Services. The Project is overseen by a Project Board. The Project Management Team manage the project and therefore the data on a day-to-day basis.

How the data will be checked for accuracy and kept up to date?

The survey datasets are correct at the time of collection and are a representation of the views of the respondents at the time. There is no requirement for the data to be later updated, although analysis and results when published are clear about the time frame which results relate to.

In order to assure the accuracy of the data collected, quality assurance follow up checks are completed by the SCJS contractors with a proportion of respondents to ensure that the data collected by interviewers are accurate. This process is detailed in the SCJS contract.

The recontact data are accurate at the time of collection. Currently there is no mechanism in place for ensuring this remains up to date into the future. As such, the Scottish Government assess that this data should be retained for a maximum of five years. All respondents who are approached for follow up research have to opt-in to participate in that project, and respondents on the recontact list can remove themselves from the database at any time by contacting the Scottish Government or the SCJS contractors using the contact details provided.

3.4 Explain the legal basis for the sharing with internal or external partners:

The Scottish Crime and Justice Survey provides evidence on the extent and nature of crime in Scotland, as well as experiences of and attitudes towards various components of the Scottish criminal justice system. This enables Scottish Ministers, other public bodies, relevant stakeholders and the general public to assess the performance of the justice system in Scotland, and provides evidence to help with the development or refinement of policies, programmes and services designed to improve outcomes for the people of Scotland. Therefore, for the same reason SG gathers and analyses the data, the SCJS datasets are shared in order to enable other organisations (public bodies, third sector organisations and academics) to undertake research which can provide evidence on crime and justice in the broader public interest.

GDPR Article 6(1)(e) provides a lawful basis for processing where:
“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.

The legal gateway for processing the data to fulfil the above functions is Section 48 of the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 which states that:
“The Lord Advocate or the Secretary of State may assist (whether financially or otherwise) other persons in conducting research into any matter connected with the law (other than research into any matter referred to in section 75(1) of the Criminal Justice (Scotland) Act 1949).”

Recontact data

Recontact data are gathered and processed on the basis of explicit consent. This details that the recontact data will only be used for the purposes of follow up research, and may be shared with other research organisations who are undertaking this research. Respondents are advised that they have the right to withdraw from the recontact database at any time and are provided with information on how to do so.

As detailed previously, the recontact datasets are held for a maximum of 5 years before being destroyed. All requests/proposals to use the recontact data are assessed on a case by case basis (including how many years' worth of data to supply and what personal information to provide). When approached to take part in follow up research, respondents must explicitly opt-in at that stage too.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish Government - SCJS Project Team, Justice Analytical Services	Data Controller & Project Management.
Scottish Government – Office of the Chief Statistician	Conduct the sampling and assist with weighting the data. Also use SCJS data as part of SSCQ.
Scottish Government – SCJS Project Board, officials within the Safer Communities and Justice Directorates	Overall responsibility and provides oversight for the project.
ScotCen Social Research and Ipsos	Contractor and data processor.
Members of Scottish population	Asked to take part in the survey each year.
Administrative Data for Research Scotland	Sharing datasets to the Scottish National Safe Haven so they can be linked to other datasets for research

4.2 Method used to consult with these groups when making the DPIA.

Regular project correspondence between SCJS team, Ipsos, ScotCen and OCS (emails, meetings etc.) – sharing draft outputs, plans to complete, sharing common sections/contributions where relevant. Steps were also taken to compare and check consistency of approach with other household surveys commissioned by the Scottish Government.

Members of the public were not consulted in the development of the DPIA. However, upon publication, it was highlighted on the SCJS website along with other information relevant for respondents and details on the SCJS privacy policy. Any comments received will be given due consideration and an updated DPIA (plus amended procedures) can be developed if required. The end of this document also advises that anyone wishing to provide comments can do so using the contact details provided.

4.3 Method used to communicate the outcomes of the DPIA .

Correspondence with survey contractors. Confirmation on SCJS website that DPIA has been completed. DPIA published on SCJS website, alongside note of when last reviewed and next to be reviewed. Any notable changes in DPIA to be noted on website where DPIA published as well as within DPIA.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

The Scottish Government commission and are responsible for the governance of the survey. SG is the data controller, holding and processing the survey data.

Ipsos and ScotCen have been commissioned as a consortium to deliver the survey on behalf of the Scottish Government. In respect to personal data, they are responsible for the collection of the survey and initial processing of the survey data (cleaning, quality assuring and analysing the data). Both Ipsos and ScotCen have taken steps to review and document their roles in the SCJS and their processing of the data. For example, risks to privacy are reduced by access to the data being restricted to named individuals working on the project in each organisation, whilst any data transmission between organisations and with the Scottish Government is done using secure FTP facilities.

Disclosure controlled datasets are made available to research organisations through the UK Data Service or Data Sharing Agreements between SG and relevant third parties for the purposes of further research. The disclosure control processes further reduce the risk of individuals being identified, and whilst the Data Sharing Agreements ensure the data is only used for legitimate research purposes in accordance with the legal basis for processing.

5.2 Anonymity and pseudonymity

The main SCJS data are split into multiple datasets and pseudonymised. In short, the questionnaire responses are contained within datasets which do not include direct personal identifiers, but do contain anonymised personal information like gender and age. A separate dataset of recontact information (including name, address, telephone number and email address) is held for those who have consented to providing this.

A serial number is assigned to each respondent and these are consistent across all SCJS datasets relevant to each individual year, so datasets can be matched if required – following necessary scrutiny and approval processes. This represents the biggest risk to individuals being identified. For this reason, the recontact dataset are stored securely and separately from the main survey dataset, and is only accessible by the Project Director in the Scottish Government. The recontact data (matched with survey data or on its own) can be provided to research organisations for the purposes of further research, but Data Sharing Agreements would be created before such processing takes place.

5.3 Technology

Within Scottish Government, personal data is held electronically on restricted areas of the SG secure server as previously described.

Scottish Government Data Protection and Information Assets team, in iTECS, are responsible for assessing each new or additional information technology for privacy intrusion. The SCJS Survey team only uses technology cleared by Scottish Government experts.

Personal data is collected by the survey contractors using laptop/tablet CAPI computers. Ipsos and ScotCen are responsible for the integrity of these devices and the technology used to process the data. Both organisations have produced and maintain a data flow document which outlines how data is processed within and between the organisations, including the range of secure software and processes used.

Ipsos MORI's survey management software (iField), used to carry out market research fieldwork, is hosted within a data centre by a provider - RackSpace UK. Rackspace UK datacentres conform to ISO 27001/2-based policies with an annual review, documented change management procedures, secure document and media destruction policies, incident management and business continuity plans as well as continuous monitoring and third-party reviews. All applications and data are managed by Ipsos.

5.4 Identification methods

A unique serial number is assigned to each respondent within the SCJS datasets. Whilst personal information such as name and address are stored separately from the main survey response data (for respondents who have consented to being recontacted), the unique serial number is common to all datasets to enable these data to be matched if required.

Only the SCJS Project Director (and necessary IT staff) has access to the recontact database containing names and addresses and this is only used for legitimate research purposes, in line with the legal basis on which these data are held. Research organisations can make applications to use the recontact data, as detailed elsewhere in this document.

5.5 Sensitive/Special Category personal data

Special category data collected via the SCJS includes:

- Ethnicity
- Religion
- Physical and mental health
- Sexual orientation

From 2021/22 onwards the SCJS will ask new questions relating to sex and gender, including asking the respondent about their transgender status. This is in line with the SG guidance: [Sex, gender identity, trans status - data collection and publication: guidance - gov.scot \(www.gov.scot\)](https://www.gov.scot/resources/documents/2021/06/sex_gender_identity_trans_status_data_collection_and_publication_guidance.pdf).

The SCJS also collects data on experiences of violent crime and property crime, as well as partner abuse, sexual victimisation, and stalking.

The SCJS collects information on whether respondents have ever been convicted of a crime and related sentence (if any) they received.² No specific details of convictions are recorded and this is only used for research/statistical purposes. Respondents are free to refuse to answer these questions, and any others, as they see fit.

² This data will not be collected in the 2021/22 SCJS.

No individual respondents are identifiable in any results published by SG, and sensitive information is stored separately from direct personal identifiers (name, address etc). Furthermore, steps are taken to ensure that datasets provided to the UK Data Service or shared with reputable research organisations have disclosure control processes performed on them to further reduce the risk of individuals being identifiable through the survey responses.

5.6 Changes to data handling procedures

Datasets are stored securely with access restricted to key named individuals. No changes to data handling procedures are envisaged at this time. Data retention policies were reviewed and updated in the process of completing this DPIA in 2018. The DPIA outlines the approach to data retention which will be used going forwards.

The intention is for the DPIA to be reviewed at least annually to consider whether any updates are required. Any notable changes to data handling procedures will be assessed from a data protection/privacy perspective, will lead to the DPIA being proactively updated, and changes to the Privacy Notice as appropriate.

5.7 Statutory exemptions/protection

The processing of the data meets Article 6(1)(e) of the GDPR as it is necessary to perform a task in the public interest and the task has a clear basis in law. This means that the right for data subjects to object to processing is more restricted. The privacy notice makes this clear.

The Data Protection Act 2018 also provides some exemptions for the purposes of research and statistics. It notes that: The listed GDPR provisions do not apply to personal data processed for (a) scientific or historical research purposes, or (b) statistical purposes, to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question.

The listed GDPR provisions are the following provisions of the GDPR (the rights in which may be derogated from by virtue of Article 89(2) of the GDPR)—

(a) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country³ transfers);

(b) Article 16 (right to rectification);

(c) Article 18(1) (restriction of processing);

(d) Article 21(1) (objections to processing).

The exemption is available only where

(a) the personal data is processed in accordance with Article 89(1) of the GDPR (as supplemented by section 19), and

(b) as regards the disapplication of Article 15(1) to (3), the results of the research or any resulting statistics are not made available in a form which identifies a data subject.

³ "Third country" means a territory or country outside the United Kingdom.

5.8 Justification

The information collected in the survey provides reliable evidence to the government and others on the extent and experiences of crime in Scotland, as well as perceptions and experiences of the criminal justice system in Scotland. This information is used to inform policy, monitor performance/changes over time and assess inequalities amongst the population. This evidence is not currently available from other sources, and no viable alternative to collecting this data is currently available. The SCJS datasets are therefore collected and processed to undertake tasks in the public interest. Steps are taken to minimise the risks to privacy associated with processing.

The recontact datasets are held and processed on the basis of explicit consent. Data Subjects are made aware of their rights and this data is placed under strict restrictions and has a bespoke retention policy.

5.9 Other risks

N/A

6. General Data Protection Regulation (GDPR) Principles

Principle	Compliant – Yes/No	Description of how you have complied
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	<p>Processing is undertaken under the public task clause of GDPR (Article 6(1)(e)), with a relevant legal gateway having been identified. Special Category data are processed in accordance with Article 9(2)(j).</p> <p>The Scottish Government can process data on criminal convictions and offences under article 10 as it has a lawful basis under article 6(1) and as an official authority it can carry out the processing. The SCJS collects limited and non-specific information on whether respondents have ever been convicted of a crime for use as an analytical variable.⁴</p> <p>The survey's advance materials and website act to provide necessary information to data subjects, whilst interviewers also provide additional information face to face. Together these elements form the SCJS privacy notice.</p> <p>Respondents are asked for explicit consent for their names, addresses and contact details to be held for the purposes of follow-up research. Signatures record this consent. Respondents are provided with information of how to later opt-out and this information is also provided on the SCJS website.</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.2 Principle 2 – purpose limitation	Yes	<p>SCJS data are only collected and processed for the specified, explicit and legitimate purposes communicated to respondents – i.e. for the purposes of research into crime and justice in Scotland. However, GDPR Article 89(1) also applies here, which provides an exemption to the purpose limitation for '...scientific or historical research purposes or statistical purposes'.</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.3 Principle 3 – adequacy, relevance and data minimisation	Yes	<p>The survey content is regularly reviewed to ensure that there is a continued need for the data to be collected.</p>

⁴ This data will not be collected in the 2021/22 SCJS.

		In terms of personal data (such as gender, age etc.) – collection and processing of this data is done using established questions which produce meaningful data for the purposes of research and statistics. Personal information collected is essential for understanding how experiences of crime and perceptions of the justice system in Scotland vary across different groups in order to monitor performance and inform policies.
Principle	Compliant – Yes/No	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	Yes	<p>Accurate: The information is obtained directly from data subjects. The questionnaire includes a range of built-in logic checks, whilst further quality assurance checks are performed by the contractor.</p> <p>Up-to-date: The data are accurate at the time of collection. As further processing uses the data and ties it to the point of collection (i.e. looks at results in a particular year), the data is always accurate to and representative of that point in time. A new sample of respondents is drawn for each survey year.</p> <p>There is currently no mechanism in place for updating the recontact dataset. Therefore, we assume this is correct at the time of collection and (for most people) for a period thereafter. The recontact datasets are supplied to SG at the conclusion of each year of data collection. However, it is important to note this data may no longer be accurate for many people after a period of time (i.e. as people may move address, change contact details and so on). Balancing this consideration against the purpose for collecting the data, and the consent given by data subjects when providing this information, SG holds recontact data for five years and then deletes it. In practice, applications to use the recontact data are considered on a case-by-case basis, including how many years' worth of data are requested and can be appropriately used from the maximum of up to five years' worth of data. Often it is sufficient and therefore more appropriate to only use data from the last two years.</p>

		<p>Deletion: As data are processed in accordance with the public task clause, the right to erasure does not apply. However, this does apply to the recontact data where consent is the legal basis for processing. Data subjects are provided with contact details to enable them to withdraw their consent and remove themselves from the recontact database (prior to the broader deletion policy being applied as a whole).</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes	<p>The main SCJS datasets are held indefinitely by the Scottish Government for the purposes of research and statistics. These datasets are pseudonymised as they do not include direct personal identifiers, thus reducing the risk of individuals being identified.</p> <p>The recontact datasets are held securely and separately from the main survey datasets, and retained for a maximum of five years. Each data subject has a unique identifier in each dataset which allows them to be matched. This processing only takes place to facilitate legitimate further research with a sound legal basis, and following ethical considerations and necessary approval processes being completed.</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.6 GDPR Articles 12-22 – data subject rights	Yes	<p>Data subjects have rights defined under GDPR. The survey’s advance materials and website explain how data are handled, rights of data subjects and where more information can be found.</p> <p>Whilst most subject rights under GDPR apply, as the SCJS data are processed under the public task clause Individuals’ rights to erasure and data portability do not apply. As the survey is carried out for reasons of public interest (rather than a legal obligation) and appropriate safeguards are in place to minimize the risk to privacy, the right to object is more limited as the processing is necessary for the performance of a task carried out in the public interest – as per Article 21(4). However, participation in the survey is voluntary, so data are only collected from willing participants. The data are not used for direct marketing, and is</p>

		only processed for legitimate research purposes as specified in the privacy notice.
Principle	Compliant – Yes/No	Description of how you have complied
6.7 Principle 6 - security	Yes	<p>Within the Scottish Government, the survey datasets are stored on a section of the government’s secure server with access restricted to a small number of analysts working on the project. Only aggregated information is published in reports and tables, whilst disclosure control processes are applied to further limit the potential for individuals to be identified before datasets are submitted to the UK Data Service or shared with research organisations under Data Sharing Agreements. All SG staff complete necessary Data Protection training at least once per year to ensure staff are aware of regulations.</p> <p>Contractor process: The SCJS data are collected and processed in a secure manner. Access to personal data and survey datasets are restricted to only individuals who require access at different stages of the process. Once the survey datasets are in their final format only the project team in ScotGen and Ipsos have access to the data. A data flow has been produced and is maintained to outline the data processing which takes place and the secure software and processes used.</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.8 GDPR Article 24 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	Yes	The survey datasets are generally not shared with any research organisations that operate or sub-contract operations outside of the EEA. Should a data sharing request be received which would involve transferring data outside of the EEA, this would be considered by the Scottish Government’s Data Access Panel.

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
<p>Personal information about an individual is lost/leaked during fieldwork</p>		<p>Interviewers sign confidentiality agreements before they start work and receive information security training.</p> <p>Both Ipsos and ScotCen have secure systems, software and processes in place for transmitting interview information from interviewers' laptops to central servers. The information is then deleted from the interviewers' laptops.</p>	<p>Risk reduced</p>
<p>Personal information about an individual is accidentally leaked or release during or after processing.</p>		<p>Steps are taken to ensure that direct personal identifiers in the recontact dataset are stored separately from the main survey datasets containing pseudonymised respondent answers. Access to the different datasets is restricted to named individuals working on the SCJS within ScotCen and Ipsos. A unique identifier is assigned to each respondent in each dataset to allow them to be later matched for the purposes of follow-up research (where respondents have consented to this).</p> <p>Once the recontact data containing the direct personal identifiers has been transmitted to SG it is deleted by the survey contractors.</p> <p>Survey datasets are transmitted securely to SG via an FTP facility at the conclusion of each year of data collection. These are stored safely in a restricted section of the SG server only accessible by a small number of named analysts within Justice Analytical Services. The recontact datasets, containing direct personal identifiers, are only accessible by the SCJS Project Director (and necessary IT staff).</p> <p>Scottish Government staff with access to the data have all passed the Baseline Personnel Security Standard,</p>	<p>Risk reduced</p>

		are trained in the safe handling of data, and have a legitimate need to access the data.	
A person is identified from the survey datasets provided to UK Data Service or shared via a Data Sharing Agreement.		<p>Statistical disclosure control procedures are performed on the SCJS datasets before they are made available to end-users. These processes are in line with controls used by the other two SG major population surveys and have been approved by the Office of the Chief Statistician.</p> <p>Requests for further or additional data under special license are assessed by the SCJS Project Team against the SG data risk matrix in the first instance. Any request with a score over 12 are referred to the SG data access panel.</p> <p>SG analysis of the data does not publish figures based on less than 50 respondents, and this approach is also recommended to others undertaking analysis of SCJS data.</p>	Risk Reduced

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Personal information about an individual is lost/leaked during fieldwork		Interviewers are trained on data security and must report any data loss during fieldwork to fieldwork management teams within their organisation immediately. Contract between SG and Ipsos /ScotCen specifies that SG must be notified of any data breaches immediately.	SCJS Project Director (at time of review Mark Bell)
Personal information about an individual is accidentally leaked or release during or after processing.		Access to SCJS data in SG, ScotCen and Ipsos is restricted to named individuals working on the project. Any data breaches must be brought to the attention of SG immediately, as specified in the SCJS contract. Changes to project teams should mean that individuals have access granted and removed as required, in a timely manner.	SCJS Project Director (at time of review Mark Bell)
A person is identified from the survey datasets provided to UK Data Service or shared via a Data Sharing Agreement.		Data Sharing Agreements specify requirements around not releasing results based on less than 50 respondents. Clear processes are in place for assessing any requests for additional data under special license considerations.	SCJS Project Director (at time of review Mark Bell)

9. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of collecting and processing data associated with the Scottish Crime and Justice Survey has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	Date each version authorised
Nicola Edge, Head of Justice Analytical Services	25 th July 2018
Amy Wilson, Head of Justice Analytical Services	4 th August 2020
Amy Wilson, Head of Justice Analytical Services	26 th August 2020
Amy Wilson, Head of Justice Analytical Services	11 th November 2021
Amy Wilson, Head of Justice Analytical Services	29 June 2023

Comments/Feedback:

If anyone reading this document, particularly SCJS respondents, has any comments or suggestions for changes, please get in touch with the Scottish Crime and Justice Survey Project Team – scjs@gov.scot



© Crown copyright 2023



This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

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

This publication is available at www.gov.scot

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-83521-108-3 (web only)

Published by The Scottish Government, July 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1308402 (07/23)

W W W . g o v . s c o t