# Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

| Version | Reason | Date | Author(s) |
|---|---|---|---|
| 1.2 | New Data Sharing Agreement | 4th October 2022 | IGfL Working Group on London Young People Survey (Your Choice) |

| | | |
|---|---|---|
| **Project / Work Stream Name** | **London Young People Study (Your Choice)** | |
| **Project / Work Stream Lead** | Name | [redacted] On behalf of IGfL; [redacted], London Borough of Lewisham and [redacted], London Borough of Waltham Forest |
| | Designation | Strategic Intelligence Lead, London Councils<br>And<br>IGfL, Information Governance for London |
| | Telephone | 07886 757464 |
| | Email | [redacted] |

| | |
|---|---|
| **Overview:**<br>**(Summary of the project/work stream)** | Pan-London data sharing to support evaluation of a major new service to reduce deaths and injuries from serious youth violence in London.<br>The London Young People Study (LYPS) is a pan-London project being run by the London Violence Reduction Unit and the Association of London Directors of Children's Services. The program trains workers delivering services to young people (e.g. social workers, youth justice workers, teachers) to deliver high-intensity cognitive-behavioural therapy (CBT) informed support to young people aged 11-17, across the 32 London boroughs. This support, and the work to make it available, is branded 'Your Choice'.<br>Through the LYPS, Your Choice is being evaluated in London in order to determine whether the program is effective, and therefore whether it should receive funding to scale-up across the capital and nationwide. The evaluation will be carried out by the Institute of Fiscal Studies (IFS), who will work with the Anna Freud Centre and the Youth Endowment Fund on the research. This DPIA and the associated Data Sharing Agreement covers the data sharing between the local authorities and the IFS only. IFS will have suitable agreements as necessary for the research work. |
| **Implementation Date:** | December 2022 |
| **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.**<br>*Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.* | The LIIA team overseeing the programme have consulted extensively with London DCS', practitioners and the Young People's Action Group about all aspects of the study.<br>The feedback received has been used to shape the programme and this has been shared back with those consulted to check that they are happy with the final form.<br><br>Supporting information attached regarding:<br>● The challenge of serious youth violence in London<br>● The lack of evidence regarding what works in alleviating it<br>● The promise of this approach<br>● The evaluation design<br><br>MOPAC (2021) 'Understanding serious violence amongst young people in London'. Accessible at https://data.london.gov.uk/dataset/serious-youth-violence.<br><br>With regard to the Information governance requirements the LIIA strategic intelligence lead has had a video call and follow-up correspondence with a senior case officer at ICO, confirming the lawful basis and special condition for processing sensitive and special category data for this project. A working group of IG professionals from the local authorities developed the DPIA and DSA for the project. |

## Step 1: Complete the Screening Questions

| Q 1 | Category | Screening question | Yes/No |
|---|---|---|---|
| 1.1 | Technology | Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy? | No |
| 1.2 | Technology | Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business? | No |
| 1.3 | Identity | Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data? | Yes |
| 1.4 | Identity | Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? | No |
| 1.5 | Multiple organisations | Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners? | Yes |
| **Q** | **Category** | **Screening question** | |
| 1.6 | Data | Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? | Yes |
| 1.7 | Data | Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database? | No |
| 1.8 | Data | Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals? | Yes |
| 1.9 | Data | Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources? | No |
| 1.10 | Data | Will the personal data be processed out of the U.K? | No |
| 1.11 | Exemptions and Exceptions | Does the project relate to data processing which is in any way exempt from legislative privacy protections? | No |
| 1.12 | Exemptions and Exceptions | Does the project's justification include significant contributions to public security and measures? | No |

| | | | |
|---|---|---|---|
| 1.13 | Exemptions and Exceptions | Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation? | No |
| | | | |

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

**Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.**

| **Step 2: Identify the need for a DPIA** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **2.1** | **Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??** | | | | | | New/Changed | | | |
| | | | | | | | | Changed | | | |
| | **2.2** | **What data will be processed/shared/viewed?** | | | | | | | | | |
| | | **Personal Data** | | | | | | | | | |
| | | Forename | x | Surname | X | Date of Birth | X | Age | X | Gender | x |
| | | Address | - | Postal address | - | Employment records | X | Email address | - | Postcode | - |
| | | Other unique identifier<br>1. Unique Pupil Number<br>2. Unique Learner Number<br>3. LA-specific unique child ID | | Telephone number | - | Driving license number | - | NHS No | - | Hospital ID no | - |
| | | Other data *(Please state):* | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Special Categories of Personal Data** | | | | | | | | | |
| | | Racial or ethnic origin | | x | Political opinion | - | Religious or philosophical beliefs | | | - | |
| | | Trade Union membership | | - | Physical or mental health or condition | | | | | X | |
| | | Sexual life or sexual orientation | X | Social service records | X | Child protection records | | | | X | |
| | | Sickness forms | - | Housing records | - | Tax, benefit or pension records | - | Adoption records | | - | |
| | | DNA profile | - | Fingerprints | - | Biometrics | - | Genetic data | | - | |
| | | Proceedings for any offence committed or alleged, or criminal offence record | | | | | | | | X | |
| | | Other data *(Please state):* | Data relating to criminal conviction: not explicitly requested but may be recorded in free text explanations of why young people have been referred to the program or in a description of their needs and their history of interaction with services (e.g. youth offending teams) | | | | | | | | |
| | | Will the dataset include clinical data? (please include) | | | | | | | | Yes/No | |
| | | | | | | | | | | No | |
| | | Will the dataset include financial data? | | | | | | | | No | |
| | | **Description of other data processed/shared/viewed?** | | | | | | | | | |
| | | See other data section above. | | | | | | | | | |

| | | | |
|---|---|---|---|
| **2.3** | **<u>Business sensitive data</u>** | | |
| | Financial | | No |

| | | | | |
|---|---|---|---|---|
| | Local Contract conditions | | No | |
| | Operational data | | Yes – data could be used to describe the progress of the Your Choice service in London (numbers starting, retention of staff, retention of participants, rate of positive outcomes, etc). This data will only be aggregate data. | |
| | Notes associated with patentable inventions | | No | |
| | procurement/tendering information | | No | |
| | Customer/supplier information | | No | |
| | Decisions impacting: | One or more business function | **Yes/No** | No |
| | | Across the organisation | | No |
| | **Description of other data processed/shared/viewed (if any).** | | | |
| | | | | |

| **Step 3: Describe the sharing/processing** | | | |
|---|---|---|---|
| **3.1** | **List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below* | | Yes/No |
| | | | Yes |
| | Name | Controller or Processor? | Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit |

| | | | |
|---|---|---|---|
| | | | Yes / No |
| | Institute for Fiscal Studies | Controller | No |
| | The 32 London Boroughs | Controller | Expected to be yes, as both are a requirement for local authorities |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| **3.2** | **If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?** | | Yes/No<br>No – a draft DSA is proposed for review alongside this DPIA<br>All 32 Boroughs taking part in the programme have signed a grant agreement – there is a condition to share information with the evaluators as part of that agreement. |
| **3.3.** | **Has a data flow mapping exercise been undertaken?**<br>*If yes, please provide a copy, if no, please undertake* | | Yes – attached |
| **3.4** | **Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?**<br>*If yes, provide a copy of the confidentiality agreement or contract?* | | Yes / No<br>No |
| **3.5** | **Describe in as much detail why this information is being processed/shared/viewed?**<br>*(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)* | | |

To establish the quality of evidence of the program's efficacy which is required to secure investment in youth services, we need to conduct a robust trial – an RCT or a quasi-experimental study. This will establish whether the intervention has the intended impact, and whether it represents value for money[2].

To conduct a study of this nature we have to collect personal data on those receiving the service and link it to data on outcomes. This cannot be achieved without processing personal sensitive data.

A study of this nature also requires that special category data (gender, sexuality, ethnicity, health) be processed so that evaluators can control for the impact of these on outcomes. Without this, we do not know whether the programme works as well for one group of people as for another.

Data relating to criminal conviction may be recorded in explanations of why young people have been referred to the program or in a description of their needs and their history of interaction with services (e.g. youth offending teams). Whilst not covered by this DPIA, it is noted that the research/evaluation phase will process criminal offence data, as reducing the likelihood that a young person will go on to be convicted of an offence is a key outcome of the program and a driver of cost-efficacy.

The IFS require LAs to provide the data contained in sections 2.2 and 2.3 above to evaluate the Your Choice program.

There are two key reasons to carry out this project:

- Firstly, because youth violence is a serious issue affecting Londoners. 5,864 of them last year were victims of the most serious violence and almost one per week was killed[1].

- Secondly because there is a lack of evidence today about what works to reduce this violence, and this lack of evidence is preventing us from mobilizing resources and from designing the best services to reduce the problem and its impact.

This is a priority for London's Directors of Children's Services and the Mayor – not least because of its intersection with other priority issues including poverty, racial inequality, and health inequalities.

If the evaluation shows that the program is effective, then we can deliver better services to vulnerable young Londoners, and there is also potential to roll it out across England and Wales so that all young people in this cohort can benefit.

## Step 4: Assess necessity and proportionality

**4.1 Lawfulness for Processing/sharing personal data/special categories of personal data?**

| UK GDPR | | DPA 2018 | | Other Lawful Basis | |
|---|---|---|---|---|---|
| | | | | | |
| **LAs:** | | N/A | | N/A | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 6.1(c)Public Task<br><br>**Institute for Fiscal Studies:**<br>6.1(f) Legitimate Interest | | N/A | | N/A | |
| | Special Category Personal Data Sharing | | | | | |
| | **Local Authorities:**<br>9(2)g Substantial public interest<br><br>**Institute for Fiscal Studies:**<br>9(2)j Research in the public interest | | Sch 1 Pt 2 Safeguarding of children and individuals at risk<br>Criminal data – Sch 1 Pt 3 Extension of Sch 1 Pt 2<br><br>Sch 1 Pt 1 Research | | N/A<br><br>N/A | |

| | | | |
|---|---|---|---|
| **4.2** | **Will the information be processed/shared electronically, on paper or both?** | Electronic | X |
| | | Paper | - |

| | |
|---|---|
| **4.3** | **How will you ensure data quality and data minimisation?** |

The data items required are the end result of a long process from January 2022 through to the beginning of July of reduction, refinement and clarification of the data items required for the evaluation. Practitioners, Evaluators and the LIIA team have been involved in whittling the items down to those felt essential for a robust evaluation of the programme. This has seen items dropped, eg Religion & information about parents; Other items reduced in scope or to broad categories eg disability, practitioner information and standard definitions being used wherever possible eg ethnicity.

The workbook captures the data typically 'owned' by the LA for statutory service delivery. Other information that is specifically related to the study or comes from the young person themselves are collected through a series of survey forms and subject interviews in the data collected directly by IFS and AFC and covered by their DPIAs.

Appendix A below systematically describes the data model, justification for each item.

It should be noted that the following items requested on the spreadsheet contain free text entries that may contain personal sensitive data

- Reason for involvement with other services
- Summary of work with the young person
- Reason why YP didn't want to be part of the study

A detailed user guide has been developed to accompany the LA LYPS workbook. A section on the free text boxes makes it clear that clinical or similarly sensitive data should not be entered in these fields.

**Data Quality**

The key data quality operations are therefore:

- Clear explanation of the data model to all LAs, and documentation of the same in the data collection template
- Creation of a template which restricts LAs ability to create errors in data transcription (e.g. extensive use of drop-downs in place of free text data entry)
- Second line testing (at the IFS) for conformity with data model and basic logical consistency – applied at the IFS when data is received from LAs, with clear protocols for raising questions with LAs and situating authority to make changes or explanations with them.

| | | |
|---|---|---|
| **4.4** | **Have individuals been informed about the proposed use of their personal or special categories of personal data?**<br>*For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?* | |
| | Yes.<br>1. IFS will provide a privacy notice for all LAs to use with all Young People agreeing to be part of the LYPS.<br>2. Staff involved in the programme will be trained to explain in plain English what data is being collected, why, how it is handled, and what rights data subjects have in respect of it.<br>3. Plain English documentation has been created to cover the same issues as (data, processing, purpose, rights) to be issued to data subjects. | |
| **4.5** | N/A | |
| | | |
| **4.6** | **Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?** | |

| | | |
|---|---|---|
| | Yes | |
| **4.7** | **Will the processing of data include automated individual decision-making, including profiling?**<br>*If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject* | No |
| **4.8** | **Will individuals be asked for consent for their information to be processed/shared?**<br>*If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.* | No |
| | the processing relies on another lawful basis (see section 4.1)<br>Police, Crime, Sentencing and Courts Act 2022, section 8(3)c - Imposing a duty on local authorities and others to "*prepare and implement a strategy for exercising their functions to prevent and reduce serious violence in the area"*<br>Children's Act 1989, section 17 - Imposing a duty on local authorities to "*safeguard and promote the welfare of children in need in their area"* | |
| **4.9** | **As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the embedded questionnaire.** | Yes – Appendix C has the relevant detail in the separate cloud security questionnaire. |
| **4.10** | **Where will the data will be stored**<br>*Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.* | |
| | Local authorities will store data within their social care system(s) as part of the normal record of social care delivery.<br>**Where IFS is the Controller:**<br>Data will be stored on an encrypted network of the Institute for Fiscal Studies (IFS) in a secure folder with access restricted to named researchers who need to work on the data for the purpose of the evaluation. Access to folders is controlled by ICT with approval from the Head of Data Services.<br><br>All IFS ICT systems are managed by staff directly contracted by ISF. IFS use Azure cloud storage for back up. Azure complies with ISO27001 as well as a number of other compliance standards.[9]<br><br>The IFS information security management system is ISO27001 compliant, and the IFS has an Information Classification and Handling Policy which sets out a comprehensive set of guidelines for handling all types of data and information (including highly confidential information). | |

| | | |
|---|---|---|
| | IFS also is Cyber Essentials Certified. All project team members will follow strict procedures in this policy and adhere to the IFS Information Security Policy when using or collecting data. All project team members will have received appropriate GDPR and data security training. All researchers on this project are ONS accredited researchers.<br><br>At the end of the efficacy part of the LYPS (currently scheduled for the second half of 2024), identifiable data will be stored separately within the IFS Data enclave.<br>The System is comprised of an isolated secure network of 5 Dell Desktop PCs and a server.<br>The system is standalone and does not form part of any larger network. Access to portable media interfaces (USB ports, DVD drives, disc drives) is disabled for everybody except IT Support & Head of Data Services. Users of the Enclave will not have access to a printer.<br>The server contains two internal hard disk which are configured to use RAID1 (mirroring) to allow for continuity if one fails.<br>The server is contained in a locked room separate from the Enclave. Security is maintained by port authentication. | |
| **4.11** | **Data Retention Period**<br>*How long will the data be kept?* | |
| | Local authorities will store data within their social care system(s) as part of the normal record of social care delivery, following their normal retention periods for such data.**Where IFS is the Controller:**The original data provided by each LA will be combined with the data that the IFS is collecting directly from the young people and practitioners to create a new dataset.<br><br>At the end of the efficacy trial (or the end of the pilot phase if the decision is made to not proceed to efficacy) the original LA data files will be destroyed.<br><br>The IFS are the Data Controller of the new dataset that they create. The LA is not a Data Controller for this new dataset.<br><br>Whilst being stored at the end of the efficacy phase, the identifiable parts of the data will be separated from the main bulk of the dataset and stored securely within the IFS data Enclave. Please refer to the separate document *'IFS Enclave security policy'* for more details. | |
| **4.12** | **Will this information be shared/processed outside the organisations listed above in question 3?**<br>*If yes, describe who and why:* | Yes/No |
| | 1. The data provided by the LAs in the LA LYPS workbook will remain with the IFS.<br><br>2. The new dataset the IFS create using the data provided by the LAs and combined with other data will be used for the purpose of evaluating the LYPS. This is covered by the IFS DPIA. | No |
| | | |
| **5.1** | **Is there an ability to audit access to the information?** | Yes/No |
| | | |

| | | |
|---|---|---|
| | Yes –the IFS will be able to provide audit logs describing who has accessed the data, for what purposes, and with what checks applied to ensure that the persons and purposes were legitimate. | Yes |
| **5.2** | **How will access to information be controlled?** | |
| | All data are stored on a secure network. Network access is restricted by strong individual passwords for all staff. Network passwords are changed every 91 days unless staff are accessing specific types of information where there is a requirement for the password to be changed more often. An enforced PC screen lock is in place after a defined period of time. The network is monitored by the IT Manager to check for security breaches. All members of IFS staff also have a responsibility to report security incidents.<br>Access to data via the network is only ever given to named individuals who have obtained the correct permission to use them. Permissions are controlled by the IT and Data Managers.<br>Identifiable data will be stored separately in the IFS data enclave. | |
| **5.3** | **What roles will have access to the information?** (list individuals or staff groups) | |
| **IFS:**<br>Information management team – responsible for ensuring information security and governance policies are being followed appropriately (e.g. that all personal sensitive data is appropriately logged and that review and retention policies are being followed).<br><br>Approved IFS Researchers – responsible for conducting the evaluation for which this data is being shared.<br><br>All IFS staff receive mandatory IG training which is reviewed regularly. Only employed IFS staff work on this project.<br><br>The IFS data enclave can only be accessed by Approved Enclave Users who will be required to sign the Data Enclave Access Agreement and have BPSS (Baseline Personnel Security Standard) clearance. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **5.4** | **What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?** | | | | | |
| | Username and password | x | Smartcard | | key to locked filing cabinet/room | **X** |
| | Secure 1x Token Access | | Restricted access to Network Files | | | x |

| | |
|---|---|
| | Other: *Provide a Description Below:* |
| | IFS data Enclave:<br>The system (except the server and some cabling) is contained entirely within a physically secured room. The door is locked with an access card reader and a keypad.<br>The Enclave server is contained within a separate secure room which is locked with a key.<br>The access card system is used throughout the IFS to control access to different areas. Access is assigned by IT Services. Ability to enter the Enclave is only given to staff who have been approved to use the Enclave as outlined in Section 2.4 and who have signed the Data Enclave Access Agreement (hereafter referred to as "Approved Person(s)").<br>As a secondary security measure, Approved Users will also need to obtain the number code to unlock the door from the Head of Data Services, the Head of ICT or the IT Support and Systems Administrator.<br><br>*Audit*<br>Visits to the Enclave are recorded via the Door Access System. Logs are kept for three months.<br>Logs of data access are recorded electronically using the in-built computer auditing tools.<br>Details of any outputs removed from the Enclave will be recorded in a Log Book<br>Spot check on outputs removed from the Enclave are carried out by the Head of Data Services<br>Directory access is strictly controlled and regularly reviewed by the Support and System Administrator and the Head of Data Services.<br>Access to portable media interfaces (USB ports, disc drives) are disabled for everybody except IT Support and the Head of Data Services. |

| | | |
|---|---|---|
| **5.5** | **Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:**<br>SLSP is required for new systems.<br>*SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.* | Yes/No<br>No – not for this project specifically.<br><br>The IFS have system level security policies which govern their portfolios of projects handling personal sensitive data. |
| **5.6** | **Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?**<br>*Please explain and give reference to such plan and protocol* | Yes/No<br>Yes, IFS maintain BCP and disaster recovery plans with key mitigations including secure offsite backup. |

| | | | |
|---|---|---|---|
| **5.7** | **Is Mandatory Staff Training in place for the following?** | Yes/No | Dates |
| | ● Data Collection: | n.a. – | n.a.<br>new data not being collected for this processing |
| | ● Use of the System or Service: | | n.a. role is very simple (transcribing information from local systems into a spreadsheet template) and so the approach is to provide documentation, user guide for LA LYPS Workbook and on-demand support rather than up-front training (although that is available on request). |
| | ● Information Governance: | Yes | Annual at IFS |
| **5.8** | **Are there any new or additional reporting requirements for this project?** | Yes | |
| | ● What roles will be able to run reports? | | |
| | Approved IFS researcher already working on the data for evaluation purposes (so no marginal addition to disclosure) | | |
| | ● What roles will receive the report or where will it be published? | | |
| | c. 200 decision makers in London boroughs and supporting organisations such as London Councils and the London Violence Reduction Unit.<br>The output of the study will be answers to the questions<br>1. Are young people who receive this service more or less likely to experience serious violence than those who do not receive it?<br>2. Are the young people who receive this more or less likely to experience (positive or negative) criminal justice and education outcomes than those who do not?<br>3. What known factors (e.g. demographics, service organisation) modify these outcomes;<br>4. What is the cost per outcome when they are delivered through Your Choice and how does this compare to alternatives?<br>It will contain only aggregate data.<br>An example of how the evaluation report will look can be found here;<br>https://ifs.org.uk/publications/improving-early-childhood-development-rural-ghana-through-scalable-community-run-play | | |
| | ● Will the reports be in person-identifiable, pseudonymised or anonymised format? | | |

| | | |
|---|---|---|
| | Anonymised | |
| | ● Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format? | |
| | Redacted | |
| **5.9** | **Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed) | **Yes/No**<br>Yes |

| **Step 6: Identify and Assess Risks** | | | |
|---|---|---|---|
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| *Note: risks here are risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.* | | | |
| Disposal of data: If personal data is not disposed of in an appropriate manner by the party with whom it was shared, it may be possible for third parties to obtain the data causing Medium High Medium/high Page \| 12 harm to the data subjects. Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Personal data shall not be kept for longer than necessary.Appropriate technical and organisational measures shall be taken.Corporate risk: Reputational risk. Loss of trust. Legal implications | High *if the retention periods set are not realistic * | High | High |
| Data Subject rights: That young people are not clear about their rights and understand their choices about taking part in and the potential to stop their personal data being shared or processed. | Medium | High | High |
| Further transfer of data: Risk to the safety of personal data if transferred elsewhere by the recipient . Harms could include embarrassment and distress, or being targeted for further attacks, reprisals and revenge. Compliance risk: Personal data shall be obtained for one or more specified and lawful purposes. | Medium | Medium | Medium |

| | | | |
|---|---|---|---|
| Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area. Corporate risk: Reputational risk. Loss of trust | | | |

## Step 7: Identify Measures to reduce risk

**Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6**

| Risk | Options to reduce or eliminate risk | Effect on risk | Residual risk | Measure approved |
|---|---|---|---|---|
| Retention and disposal | All partners must have a destruction of records policy in place.<br>Information must not be retained for longer than necessary for the purpose for which it was was obtained.<br>Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.<br>Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data<br>Retention periods will be stated in the DSA. | Low | Low | Yes |
| Data Subject Rights | The privacy notices from IFS explain why the project is running and how a young person's personal data will be used and shared. Personal data will be shared if the young person remains within the programme, but the young person can leave the programme at any time. If this happens, the young person can allow the data shared so far to be included in the evaluation, or for all their data to be deleted by IFS, prior to the start of the evaluation.<br>The Las and IFS will handle any data subject rights requests, including the right to object, as necessary. | Medium | Medium | Yes |

| | | | | |
|---|---|---|---|---|
| | Consideration of the lawful basis and application of data subject rights, and any requests or complaints from young people within the programme, will be assessed as part of the formal review at the end of the pilot phase, along with a review of this DPIA. | | | |
| Further transfer of data | The onward sharing of data by IFS as part of the programme has been identified and considered in separate DPIAs. The LAs and young people are aware of the onward sharing.<br><br>It is noted that where one party receives data from another, the receiving party is bound by the requirements of data protection legislation. All receiver must have full policies and processes in place to ensure data is handled securely. Systems are auditable and is in force. Employees are subject to robust employment checks. However it is noted that where a Data Controller handles data in a manner not expected this can lead to reputational damage for the supplying party, | Low | Low | Yes |

| **Step 8: Sign off and record outcomes** | | |
|---|---|---|
| **Item** | **Name/date** | **Notes** |
| Measures approved by: | IGfL Working Group | |
| Residual risks approved by: | IGfL Working Group | |
| DPO advice provided: | [redacted] | Pan-London Information Governance Lead |

| | | |
|---|---|---|
| Summary of DPO advice:<br>There has been considerable discussion on the lawful basis conditions to be used, the impact of informed consent for participation in the study, and the ethical way to engage young people for this programme. This DPIA reflects the outcome of those conversations.<br>Informal consultation has taken place with the ICO, who said that the chosen lawful basis conditions may be applicable based on the information provided, and recommended that only the most appropriate condition should be chosen. A copy of the final DPIA will be sent to the ICO for informal comment as part of the ongoing discussions with them about this project.<br>To assess the suitability of the lawful bases and approach agreed upon, the project team and the information governance working group have agreed that consideration of the lawful basis and application of data subject rights, and any requests or complaints from young people within the programme, will be assessed as part of the formal review at the end of the pilot phase, along with a review of this DPIA. Any concerns will be factored into the decision on whether to move to the efficacy phase of the programme. | | |
| DPO advice accepted or overruled by: | N/A | If overruled, you must explain your reasons |
| Comments:<br>N/A | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons |
| Comments:<br>N/A | | |
| This DPIA will kept under review by: | The IGfL working group and the project working group. In particular, when considering moving from pilot to efficacy stage. | |

**Glossary of terms**

1. Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. Special Categories of Personal Data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
3. Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
4. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
5. Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
6. *Data Subject* – an individual who is the subject of personal information.
7. *Direct Care* - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual).
8. Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.
9. Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
10. *Anonymised Data* - means data in a form where the identity of the individual cannot be recognised i.e. when:
    - Reference to any data item that could lead to an individual being identified has been removed;
    - The data cannot be combined with any data sources held by a Partner with access to it to produce personal identifiable data.

## Appendix A: Full Scope of Data

| Tab on spreadsheet | Data Item | Type of data | Nature of data input | Defined options if applicable | Data description | Reason for collection | Shared with evaluators? | Can it be degraded? | Can it be obscured? |
|---|---|---|---|---|---|---|---|---|---|
| Front Page | LA Name | No personal data | defined option - selection from locked drop-down list | List of London LA names | Name of the LA to whom data relates | To be able to track roll-out of project, return of data, provide and link to information about constituent teams of control and treatment groups, to inform evaluation controlling for different types of team and service delivery | Yes | No | No |
| CYP participating in programme in control (CG) or treatment group (YC) | CYP ID | Personal data | Data copied from LA Database | n/a | unique client ID assigned to young person on service database | To be able to link data collected from worker on sessions delivered with the child or young person (CYP) | Yes | No, relies on an exact match | No |
| | UPN | Personal data | Data copied from LA Database | n/a | education unique pupil number if available | To be able to link administrative data on CYP outcomes to CYP in programme. To evaluate impact of programme and as a control measure *eg comparing outcomes of CYP with similar previous attainment in treatment & control groups* | Yes | No, relies on an exact match | In theory, we could get LAs to encrypt these and give the keys to MoJ and DfE but not to other parties. This would reduce re-identification risk but would be slow and expensive to a degree which I suggest it is disproportionate. |
| | ULN | Personal data | Data copied from LA Database | n/a | further education unique learner number if available | To be able to link administrative data on CYP outcomes to CYP in programme. To evaluate impact of programme and as a control measure *eg comparing outcomes of CYP with similar previous attainment in treatment & control groups* | Yes | No, relies on an exact match | In theory, we could get LAs to encrypt these and give the keys to MoJ and DfE but not to other parties. This would reduce re-identification risk but would be slow and expensive to a degree which I suggest it is disproportionate. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | CYP Forenames | Personal data | Data copied from LA Database | n/a | legal first names of young person | To link to survey data collected directly from young people for qualitative evaluation of impact of programme. Where unique identifier not available, in combination with other CYP name fields and DoB, to be able to link administrative data on CYP outcomes to CYP in programme. To evaluate success of programme and as a control measure *eg comparing outcomes of CYP with similar previous attainment in treatment & control groups* | Yes | No, relies on an exact match | In theory, we could get LAs to encrypt these and give the keys to MoJ and DfE but not to other parties. This would reduce re-identification risk but would be slow and expensive to a degree which I suggest it is disproportionate. |
| | CYP last name | Personal data | Data copied from LA Database | n/a | legal surname of young person | To link to survey data collected directly from young people for qualitative evaluation of impact of programme. Where unique identifier not available, in combination with other CYP name fields and DoB, to be able to link administrative data on CYP outcomes to CYP in programme. To evaluate success of programme and as a control measure *eg comparing outcomes of CYP with similar previous attainment in treatment & control groups* | Yes | No, relies on an exact match | In theory, we could get LAs to encrypt these and give the keys to MoJ and DfE but not to other parties. This would reduce re-identification risk but would be slow and expensive to a degree which I suggest it is disproportionate. |
| | DoB | Personal data | Data copied from LA Database | n/a | (dd/ mm/ yy) | To link to survey data collected directly from young people for qualitative evaluation of impact of programme. Where unique identifier not available, in combination with other CYP name fields and DoB, to be able to link administrative data on CYP outcomes to CYP in programme. To evaluate success of programme and as a control measure *eg comparing outcomes of CYP with similar previous attainment in treatment & control groups* | Yes | No, relies on an exact match | In theory, we could get LAs to encrypt these and give the keys to MoJ and DfE but not to other parties. This would reduce re-identification risk but would be slow and expensive to a degree which I suggest it is disproportionate. |
| | Age | Personal data | Calculation from DoB - measures between DoB and 'today' | Calculated field | Age based on DoB | For teams to be able to quickly see age of CYP, to ensure CYP is age eligible, to inform LA monitoring of age of CPY participants to monitor for bias in age groups and/ or disapplication by CYP of specific ages | No | No | n/a |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Gender | Personal sensitive data | defined option - selection from locked drop-down list | Gender table | select most appropriate option | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| | Ethnicity | Personal sensitive data | defined option - selection from locked drop-down list | Ethnicity table | select most appropriate option | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | Not without undermining the benefits of the study, specifically the ability to understand differences in how children of different characteristics experience and benefit from the intervention. | No |
| | Disability | Personal sensitive data | defined option - selection from locked drop-down list | Disability table | choose as many options as apply or if no disability leave blank | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | Is already degraded to only physical/ mental/ learning difficulties /other. Further degradation (to yes/no) would undermine the benefits of the study. | No |
| | LGBTQ+ | Personal sensitive data | defined option - selection from locked drop-down list | LGBTQ+ table | If young person considers themselves to be in any of the groups associated with LGBTQ+ please choose yes | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | Not without undermining the benefits of the study, specifically the ability to understand differences in how children with different characteristics experience and benefit from the intervention. | No |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Looked after | Personal data | defined option - selection from locked drop-down list | Yes/ No | If young person is looked after please choose yes | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| SEND | Personal data | defined option - selection from locked drop-down list | Yes/ No | If young person has special educational needs please choose yes | To inform LA monitoring of age of CYP participants to monitor for bias and/ or disapplication by CYP of specific characteristics. As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| In Education/ Training/ Employment? When starting in programme | Personal data | defined option - selection from locked drop-down list | Yes/ No | select most appropriate option to indicate if young person is in EET at the start of work with them in the Your Choice treatment group or Your Choice control group | To be able to monitor change in EET outcomes during the course of the programme delivery with CYP. Informs evaluation of Impact | Yes | No | No |
| In Education/ Training/ Employment? When ending with programme | Personal data | defined option - selection from locked drop-down list | Yes/ No | select most appropriate option to indicate if young person is in EET at the end of work with them in the Your Choice treatment group or Your Choice control group | To be able to monitor change in EET outcomes during the course of the programme delivery with CYP. Informs evaluation of Impact | Yes | No | No |
| Previously received Your Choice treatment? | Personal data | defined option - selection from locked drop-down list | Yes/ No | if young person has previously received a complete Your Choice treatment or ended their involvement prematurely during an earlier episode please choose the 'yes' option | To be able to control for CYP who effectively receive more treatment than the programme typically delivers. To allow LAs to monitor young people who are coming through their system with similar risk levels or who are changing their minds about taking part in the programme | Yes | No | No |
| Worker name | Personal data | Feed from field on Worker tab | Populated field | Forename & surname of worker | For LA use, to enable easy monitoring of who to contact for missing data, as a means of reducing data input on spreadsheets. | No | No | No |
| Worker ID | Personal data | Feed from field on Worker tab | Populated field | unique worker ID assigned to worker on service database | Used to link worker details between tabs and to link with session information completed by worker and submitted directly to evaluators. | Yes | No | No |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Start date of current 'episode' | Personal data | Data copied from LA Database | n/a | Date on which young person first came to the attention of your service in this current episode (dd/ month/ yyyy) | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| Most relevant primary need | Personal data | defined option - selection from locked drop-down list | Most relevant primary need table | choose the primary 'need' from the drop-down list that is closest to the young person's needs - uses children in need definitions | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | Potentially - the standard categorisation has 23 non-exclusive options - but this would significantly degrade the benefits of the study and would not significantly reduce re-identification risk. | No |
| Involved with other council service? | Personal data | defined option - selection from locked drop-down list | Yes/ No | answer 'yes' if young person is currently receiving a service from another part of the council (Y/N) | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| Start date of 'episode' with other service | Personal data | Data copied from LA Database | n/a | date on which young person first came to the attention of other service in their current episode (dd/ month/ yyyy) | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| Name of other service | No personal data | Data copied from LA Database | n/a | name of other council service being received simultaneously by young person | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| Reason for involvement with other service | Personal sensitive data | inputter free text entry | n/a | function/ service being fulfilled/ delivered by other council service - this could be due to statutory requirements or for other reasons | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups* | Yes | No | No |
| Your choice or control group? | Personal data | defined option - selection from locked drop-down list | YC/ CG | if young person will be receiving 'Your Choice' treatment use 'YC', if in control group use 'CG' | Critical to identifying if young person is receiving treatment or business as usual service. Without this it would not be possible to evaluate impact of randomised controlled trial (RCT) | Yes | No | No |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Data referred to programme | No personal data | inputter date entry | n/a | date young person meeting criteria is assigned to the Your Choice treatment or control group | To enable measurement of length of involvement with young person as part of Your choice programme. To monitor and control for delays to start of programme delivery | Yes | No | No |
| | Date commenced on programme | No personal data | inputter date entry | n/a | date that Your Choice treatment begins | To enable measurement of length of involvement with young person as part of Your choice programme | Yes | No | No |
| | Date Ceased on programme | No personal data | inputter date entry | n/a | date Your Choice treatment or work with control group ends, young person opts out of programme or treatment/ work ends for another reason | To enable measurement of length of involvement with young person as part of Your choice programme | Yes | No | No |
| | Summary of work with young person | Personal sensitive data | inputter free text entry | n/a | brief description of the interventions being received by young people from this service and any other council services during the period in the Your Choice treatment programme or control group. If the worker changes, please mention that here (whilst showing the new worker against the child on this page and entering the workers details on the worker tab (if the worker is not already on that tab) and give a brief description of why. If the young person leaves the programme prematurely - because they opt out or move to another LA, please state this and a brief description of the reasons for this here. applies to YC treatment group and the control group | As a control measure *eg comparing outcomes of CYP with same/similar characteristics in treatment & control groups, with similar experiences of involvement with the system.* Also to capture information about why a young person ends involvement prematurely - relevant to evaluation of impact, do certain groups not make it to the end etc. | Yes | No | No |
| Workers involved in programme in control (CGT) or Treatment (YCT) or Wider (WT) or Other (OTH) Teams | Worker name | Personal data | Data copied from LA Database | n/a | Forename & surname of worker | For LA use, to enable easy monitoring of who to contact for missing data, as a means of reducing data input on spreadsheets. | No | No | No |
| | Worker ID | Personal data | Data copied from LA Database | n/a | unique worker ID assigned to worker on service database | Used to link worker details between tabs and to link with session information completed by worker and submitted directly to evaluators. | Yes | No | No |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Worker role | Personal data | Data copied from LA Database | n/a | service or organisation name for the workers role eg Social Worker, Youth Offending Team Worker, Speech & Language Therapist (SALT), substance misuse worker | As a control measure *eg comparing CYP with workers in the same/ similar roles and controlling for interventions by other workers that impact on outcomes so impact that is **only** from Your Choice can be more clearly evaluated and impact of programme accurately assessed* | Yes | No | No |
| | Service or organisation type | No personal data | Data copied from LA Database | n/a | Service name or if part of 'wider team' type of organisation eg VCS, School, Speech & Language service | As a control measure *eg comparing CYP involved with services delivering the same/ similar interventions within the same systemic framework so impact that is **only** from Your Choice can be more clearly evaluated and impact of programme accurately assessed* | Yes | No | No |
| | Team or organisation name | No personal data | Data copied from LA Database | n/a | Team name (& number if relevant) or if other organisation name/ school name/ unit name | As a control measure *eg comparing CYP involved with teams delivering the same/ similar interventions within the same systemic framework so impact that is **only** from Your Choice can be more clearly evaluated and impact of programme accurately assessed* | Yes | No | No |
| | Your choice, control group or wider team | No personal data | defined option - selection from locked drop-down list | Your Choice team/ Control group team/ Wider Team/ Other table | if worker will be delivering 'Your Choice' treatment use 'YCT', if worker is in control team use 'CGT', if in wider team 'WT'.<br>If worker is someone outside the wider team please use 'OTH'. | Critical to identifying if young person is receiving treatment or business as usual service. Without this it would not be possible to evaluate impact of randomised controlled trial (RCT) | Yes | No | No |
| | Date worker commenced 5-day training | No personal data | please enter date | n/a | date worker started Your Choice training (if in YCT group) | To measure that time taken for worker to complete the first four days of Your Choice training, delays may have an impact on training efficacy | Yes | No | No |
| | Date worker completed first 4 days of training | No personal data | please enter date | n/a | date worker completes the fourth day of Your Choice training (if in YCT group) | To measure that time taken for worker to complete the first four days of Your Choice training, delays may have an impact on training efficacy | Yes | No | No |
| Worker Clinical Supervision | Worker name | Personal data | Feed from field on Worker tab | Populated field | Forename & surname of worker | For LA use, to enable easy monitoring of who to contact for missing data, as a means of reducing data input on spreadsheets. | No | No | No |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Worker ID | Personal data | Feed from field on Worker tab | Populated field | unique worker ID assigned to worker on service database | Used to link worker details between tabs and to link with session information completed by worker and submitted directly to evaluators. | Yes | No | No |
| | Service | No personal data | Feed from field on Worker tab | Populated field | Service name | As a control measure *eg comparing CYP with workers in the same/ similar roles and controlling for interventions by other workers that impact on outcomes so impact that is **only** from Your Choice can be more clearly evaluated and impact of programme accurately assessed* | Yes | No | No |
| | Team name | No personal data | Feed from field on Worker tab | Populated field | Team name (& number if relevant) | As a control measure *eg comparing CYP involved with services delivering the same/ similar interventions within the same systemic framework so impact that is **only** from Your Choice can be more clearly evaluated and impact of programme accurately assessed* | Yes | No | No |
| | Date of clinical supervision | No personal data | inputter date entry | n/a | Date when supervision was delivered<br><br>(dd/ month/ yyyy) | Relates to potential impact of clinical supervision - a key element of Your Choice - on efficacy of programme. A control measure to allow for differences in frequency, availability, types of supervision and potential impact on treatment delivery & efficacy | Yes | No | No |
| | Type of supervision | No personal data | defined option - selection from locked drop-down list | Individual/ Peer | Was this Individual or Peer supervision? | Relates to potential impact of clinical supervision - a key element of Your Choice - on efficacy of programme. A control measure to allow for differences in frequency, availability, types of supervision and potential impact on treatment delivery & efficacy | Yes | No | No |
| Eligible but not participating | CYP ID | Personal | Data copied from LA Database | n/a | unique client ID assigned to young person on service database<br><br>only here to prevent duplicates being recorded - will not be shared with evaluators | For LA use, to enable easy monitoring of duplicates and for error checking | No | No | No |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Age | Personal | defined option - selection from locked drop-down list | Age table | select age of CYP | To monitor characteristics of CYP not engaging in programme, to check there is no system bias or discrimination preventing young people taking part or other reasons that may indicate certain cohorts do not see Your Choice as relevant for them | Yes | No | No |
| | Gender | Personal sensitive data | defined option - selection from locked drop-down list | Gender table | select most appropriate option | To monitor characteristics of CYP not engaging in programme, to check there is no system bias or discrimination preventing young people taking part or other reasons that may indicate certain cohorts do not see Your Choice as relevant for them | Yes | No | No |
| | Ethnicity | Personal sensitive data | defined option - selection from locked drop-down list | Ethnicity table | select most appropriate option | To monitor characteristics of CYP not engaging in programme, to check there is no system bias or discrimination preventing young people taking part or other reasons that may indicate certain cohorts do not see Your Choice as relevant for them | Yes | No | No |
| | Reason why CYP didn't want to be part of study | Personal sensitive data | inputter free text entry | n/a | brief description of why the eligible young person didn't want to take part in the study/ evaluation despite being eligible to take part. | To monitor characteristics of CYP not engaging in programme, to check there is no system bias or discrimination preventing young people taking part or other reasons that may indicate certain cohorts do not see Your Choice as relevant for them | Yes | No | No |

## Drop Down Boxes

| Gender | Ethnicity | Disability | LGBTQ+ | Most relevant primary need | Age |
|---|---|---|---|---|---|
| Male | Asian or Asian British - Indian | Physical disability | Yes | N1 Abuse or neglect | 11 |
| Female | Asian or Asian British - Pakistani | Mental health need | No | N2 Child's disability | 12 |
| Trans | Asian or Asian British - Bangladeshi | Learning difficulties | Prefer not to say | N3 Parental disability or illness | 13 |
| Non-binary | Asian or Asian British - Chinese | Other | not known | N4 Family in acute stress | 14 |
| Other | Asian or Asian British - any other Asian Background | | | N5 Family dysfunction | 15 |
| Prefer not to say | Black or Black British - African | | | N6 Socially unacceptable behaviour | 16 |
| | Black or Black British - Caribbean | | | N7 Low income | 17 |
| | Black or Black British any other Black Background | | | N8 Absent parenting | |
| | Mixed Heritage - White & Black African | | | N9 Cases other than children in need | |
| | Mixed Heritage - White & Black Caribbean | | | N0 Not stated | |
| | Mixed Heritage - White & Asian | | | | |
| | Mixed Heritage - any other ethnic Background | | | | |
| | White: British | | | | |
| | White: Irish | | | | |
| | White: Gypsy, Traveller | | | | |
| | White: any other white background | | | | |
| | Other Ethnic Group: Arab | | | | |
| | Other Ethnic Group: any other ethnic background | | | | |
| | Prefer not to say | | | | |
| | Not Recorded/ Not Given | | | | |

## Appendix C: Cloud security questionnaire

**Cloud Security Principles Assessment** This assessment is based on guidance from the National Cyber Security Centre and can be found at https://www.ncsc.gov.uk/collection/cloud-security
Supplier: Institute for Fiscal Studies

| Security Principle | Security Question | Recommendation | Describe how | Supplier (describe how - not just yes or no) |
|---|---|---|---|---|
| **1. Data in transit protection** | How is data protected between the user's device and the service? | Encrypted community WAN service / Community WAN service / CAPS-encrypted / IPSec VPN Gateway - CPA / Bonded fiber optic connections / Legacy SSL or TLS / encryptedTLS, version 1.2 or later / N/A | Service Provider Assertion / Contractual Commitment / Independent Validation of Assertion / Independent Testing of Implementation / Assurance in the Service Design / Assured Components / N/A | There is no user or service. Data will be transmitted from the LA to the IFS via encrypted email using the egress switch service, which uses identity-based AES 256-bit encryption with FIPS 140-2 approved cryptographic libraries as default on its endpoints. For more information on technical, physical and organizational measure in place at the egress service see https://www.egress.com/security/measures-and-controls.<br><br>If Egress is not available to a LA or a LA uses a different system for secure transmission of information, we are happy to use that provided it reaches similar security standards as Egress. If no secure email service is available, the fall back option would be to use IFS's secure portal. |

| | | |
|---|---|---|
| How is data protected within the service? | As above | Data will be stored on an encrypted (XTS-AES 256) network of the Institute for Fiscal Studies (IFS) in a secure folder with access restricted to named researchers who need to work on the data for the purpose of the evaluation. Access to folders is controlled by ICT with approval from the Head of Data Services.<br>All IFS ICT systems are managed by staff directly contracted by ISFIFS. IFS use Azure cloud storage for back up. Azure complies with ISO27001 as well as a number of other compliance standards.<br>The IFS information security management system is ISO27001 compliant, and the IFS has an Information Classification and Handling Policy which sets out a comprehensive set of guidelines for handling all types of data and information (including highly confidential information).<br>IFS also is Cyber Essentials Certified (certificate number IASME-CE-042755 exp 27/05/2022) . All project team members will follow strict procedures in this policy and adhere to the IFS Information Security Policy when using or collecting data. All project team members will have received appropriate GDPR and data security training. All researchers on this project are ONS accredited researchers. |
| How is data protected between services? | As above | n/a |

| | | | |
|---|---|---|---|
| **2. Asset protection and resilience** | Where are the service provider's datacenters located? | UK / EEA / USA with EU-U.S Privacy Shield / Other countries with data protection treaties (Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Please seek guidance from IG team if transferring to or from Japan, Canada and the USA) / Other countries | UK only except back up which is EEA |
| | Where are the services managed from? | As above | UK only |
| | Where is the service provider's legal jurisdiction? | As above | UK only |
| | Do the datacentres where your consumer data is located, have suitable physical security? | Yes / No | Yes - access to IFS areas of the building are controlled by a key card entry system that is linked to the alarm system. Entry and exit is logged with logs kept for 3 months. The building security perimeter is controlled by the landlord. Access to the building during working hours is via manned reception desks, in the main foyer to the building and at the IFS reception. |
| | How is storage media containing consumer data protected from unauthorised access? | CAPS-assured components / Foundation grade-assured components / FIPS-assured encryption / Other encryption / Secure containers or cages / No protection | Data will be stored on an encrypted (XTS-AES 256) network of the Institute for Fiscal Studies (IFS) |
| | How do you erase consumer data when resources are moved or re-provisioned, or when the consumer leaves the service or when they request it to be erased? | CPA Foundation Assured Product / CESG or CPNI-approved erasure / Other secure erasure / Other erasure process | Heidi eraser |

| | | | |
|---|---|---|---|
| | How is storage media containing consumer data sanitised or securely destroyed at the end of its usable lifetime? | CESG-assured destruction service (CAS) / CPA Foundation Assured Product / CPNI-approved destruction service / BS EN 151713:2009-compliant destruction / CESG or CPNI-approved erasure / Other secure erasure / Other destruction/erasure process | We wipe equipment using Heidi Eraser. Anything that cannot be wiped is sent to a specialist company to be physically destroyed |
| | Is all equipment potentially containing consumer data, credentials or configuration information identified at the end of its life or prior to being recycled? | Yes / No | Yes |
| | How are any components containing sensitive data sanitised, removed or destroyed? | CESG-assured destruction service (CAS) / CPA Foundation Assured Product / CPNI-approved destruction service / BS EN 151713:2009-compliant destruction / CESG or CPNI-approved erasure / Other secure erasure / Other destruction/erasure process | We wipe equipment using Heidi Eraser. Anything that cannot be wiped is sent to a specialist company to be physically destroyed |
| | Are accounts or credentials specific to redundant equipment revoked to reduce their value to an attacker? | Yes / No | yes |
| | What is the availability of the service? | (Open text) | n/a |
| **3. Separation between consumers** | Is the service a public, private, community or hybrid cloud service? | Public cloud / Community cloud / Private cloud / Hybrid cloud | n/a |

| | | | |
|---|---|---|---|
| | What types of other consumer, do your consumers share the service or platform with? | No other Consumer / Only Government / a specific interest group (eg. Charities) / Anyone-Public | n/a |
| | Do you provide separation of consumer data and service from other consumers of the service? | Yes / No | n/a |
| | Is the management of a consumer's service, kept separate from other consumers (consumers covered separately as part of Principle 9)? | Yes / No | n/a |
| **4. Governance** | Do you have a governance framework and processes in place for the service? | Yes / No | We are Cyber Essentials certified and we are GSAD accredited |
| **5. Operational security** | Are the status, location and configuration of service components tracked throughout their lifetime? | Yes / No / N/A | n/a |
| | Are changes to the service assessed for potential security impact? And are changes managed and tracked through to completion? | Yes / No | n/a |
| | Are potential new threats, vulnerabilities or exploitation techniques which could affect the service assessed, and are corrective actions taken? | Yes / No | The IFS systems are both internally and externally penetration tested annually. Vulnerabilties are tracked and fixed. |
| | Do you monitor relevant sources of information relating to threat, | Yes / No | yes |

| | | |
|---|---|---|
| vulnerability and exploitation techniques? | | |
| Are the severity of threats and vulnerabilities considered within the context of the service and do you use this information to prioritise implementation of mitigations? | Yes / No | yes |
| Are known vulnerabilities within the service tracked until suitable mitigations have been deployed through a suitable change-management process? | Yes / No | n/a |
| Do you make available to Buyers, timescales for implementing mitigations to vulnerabilities? | Yes / No | n/a |
| Do you conduct protective monitoring and analysis to identify suspicious activity? | Yes / No | Yes |
| Do you have incident-management processes in place and are they enacted in response to security incidents? | Yes / No | yes - we have a security incident management policy |
| Do you have a defined process and contact route for reporting security incidents by consumers and external entities? | Yes / No | yes - we have a security incident management policy and a personal data breach policy |
| Do you publish to consumers, a definition of a security incident, along with the triggers and timescales | Yes / No | Yes. Although we don't routinely make our policies publically available, we are happy to share them with interested parties. |

| | | | |
|---|---|---|---|
| | for sharing such incidents with service consumers? | | |
| | Do you publish the content and format of security incident notifications? | Yes / No | no |
| | What are your maximum timescales by which an incident will be investigated? | 1 week / 2 weeks / 1 month / 3 months | incidents must be reported immediately and investigation will start straight away. Response time will depend on the severity of the incident. |
| **6. Personnel security** | Do your staff, who have access to the service (physically or logically), have adequate personnel security screening for their role? | Developed vetting / Security clearance vetting / Baseline personnel/security standard (BPSS) / Background checks in accordance with /Employment checks | Some staff are BPSS checked already. If required all staff with a need to use the data can be BPSS checked.A BPSS check in involves a basic disclosure check https://www.gov.uk/request-copy-criminal-record |
| **7. Secure development** | Are new and evolving threats regularly reviewed and are development tasks initiated to improve and reinforce the security of the service in line with these changing threats? | Yes / No | Yes - this is done as part of our ISO27001 and our business continuity planning. |
| | Is software development carried out in line with industry good practice regarding secure design, coding, testing and deployment? | Yes / No / N/A | yes - we have a secure development policy but this is not relevant here. |
| | Are software configuration management processes in place to ensure the integrity of the solution through development, testing and deployment? | Yes / No / N/A | n/a |
| **8. Supply-chain security** | Do you inform consumers how much of their information is shared with, | Yes / No | n/a |

| | | | |
|---|---|---|---|
| | or accessible by, third-party suppliers and their supply chains? | | |
| | Do your procurement processes ensure that relevant security requirements, such as the Cloud Security Principles, placed on third-party suppliers and delivery partners are explicitly documented? | Yes / No | n/a |
| | Are the risks to your service from third-party suppliers and delivery partners regularly assessed and appropriate security controls implemented? | Yes / No | n/a |
| | Do you monitor how your suppliers comply with security requirements and initiate remedial action where necessary? | Yes / No | n/a |
| | Do you have the necessary information and processes to verify that hardware and software used in the service is genuine and has not been obviously tampered with? | Yes / No | n/a |
| **9. Secure consumer management** | Can only authorised individuals from the consumer organisation authenticate and access management interfaces for the service? | Yes / No | Yes |

| | | | |
|---|---|---|---|
| | Can only authorised individuals from the consumer organisation perform actions affecting the consumer's service through support channels? | Yes / No | Yes |
| | Can consumers only manage their own service, and not access, modify or otherwise affect the service of other consumers via management tools and interfaces? | Yes / No | Yes |
| | Does your service support consumers in implementing the 'principle of least privilege' by providing the ability to constrain permissions given to consumer administrators? | Yes / No | Yes |
| | Do you inform consumers which networks, management interfaces are exposed to and what functionality is available via those interfaces? | Yes / No | n/a |
| **10. Identity and authentication** | Do your identity and authentication controls provide an appropriate level of confidence that a user has authorisation to access a specific interface? | Username and two factor authentication / Username and TLS client certificate / Authentication federation / Limited access over dedicated link, enterprise or community network' / Username and password / Username and strong password / passphrase | Access to the data will be given only to those individuals working on the project. Permissions are set by IT in consultation with the Head of Data Services. Access to the network is via strong individual passwords that are changed every 3 months. |

| | | | |
|---|---|---|---|
| | | enforcement / GPG43 / Other mechanism / No controls | |
| **11. External interface protection** | Do you provide on-boarding guidance, covering safe and secure connection? | Yes / No | na |
| | What method of interconnection do you provide? | Internet / PSN WAN / Private WAN / Internet and Private WAN | n/a |
| | Do you provide access control of the data, to the service for consumers? | Yes / No | n/a |
| | Do you provide authentication and authorisation to the service for all functions? | Yes / No | n/a |
| **12. Secure service administration** | Which service management model do you use? | Dedicated devices on a segregated network / Dedicated devices for community service management / Dedicated devices for multiple community service management / Service management via bastion hosts / Direct service management | IFS is ISO27001 compliant. |
| **13. Audit information provision to consumers** | Do you provide audit information to consumers? | Data made available / Data made available by negotiation / None | n/a |
| **14. Secure use of the service by the customer** | Which end-device population is the cloud service accessible from? | Corporate / Enterprise devices / Partner devices / Unknown devices | n/a |
| | Do you provide on-boarding guidance, including impacts on the consumer's security? | Yes / No | n/a |

| | | |
|---|---|---|
| Do you provide user or administrator training on use of the service and its security? | Yes / No | n/a |