|  |
| --- |
| **Data Protection Impact Assessment *(DPIA)*** |
| **A - Does the proposed activity involve ECC processing, collecting, handling, storing or sharing personal data?** |
| Yes – continue to question B |
| No – this form does not need to be completed for your proposed activity |
|  |
| **B - Will any of this personal data be anonymised?** *(please see the attached standard for the anonymisation of data* <https://ico.org.uk/media/1061/anonymisation-code.pdf>*)* |
| Yes – this form does not need to be completed for your proposed activity, however, should you need any Advice and Guidance from IG then please contact the team ([informationgovernanceteam@essex.gov.uk](mailto:informationgovernanceteam@essex.gov.uk)) |
| No – continue with the completion of this DPIA form |

**\*Customer is only required to complete Sections 1 - 8\***

|  |  |
| --- | --- |
| **1 - About the activity:** | |
| **Title of activity:** |  |
| Person completing this form: |  |
| Information Asset Owner: |  |
| Business Owner Details: |  |
| System Owner Details: |  |
| Other people IG may need to liaise with and their role in the activity:  *(e.g. if you are on leave, a commercial colleague, activity lead or owner etc).* |  |
| Previous DPIA Completed*: If a DPIA has been completed previously for a similar piece of work, please provide the title of this activity* |  |
| Online portal reference: | *IG will complete this once the form is received* |
| IG Filing Number & IG Officer completing: | *IG will complete this once the form is received* |

|  |
| --- |
| **2 - Describe the activity:** |
| Briefly describe what the activity is and what is the purpose of the activity, why it needs to happen, how it is intended to work. *This is to ensure IG and TS understand the activity and can provide you with the required support.*  Please attach any relevant documents you think we may need to see. |
| *Please ensure that you include the benefits to the Data Subject, ECC/3rd parties and identify any potential risks/disadvantages to the Data Subjects use of their personal data* |

|  |  |  |  |
| --- | --- | --- | --- |
| **3 - Describe the information and Data Subjects involved:** | | | |
| **Please tell us about the information that will be collected or processed, will this be by:** | | | |
| **ECC collecting/processing the information  Third Party collecting/processing** | | | |
| **3 (a) - Personal Information** | | | |
| [**Personal data:**](#_Personal_information:)  *Please list the fields of data that will be processed:* | | | **Special categories of personal data:**  *Please mark if any of the below are involved:* |
|  | | | Religious or Philosophical Beliefs  Racial or Ethnic Origin  Political Opinions  Trade Union Membership  Genetic Data  Biometric Data  Health  Sex Life/Sexual Orientation |
| **Other detail on the personal data:** | | | **Other detail on the special categories of data:** |
|  | | |  |
| **Categories of Data Subject**  *Mark a box next to the categories of data subject whose personal data will be processed* | | | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Customers |  | Complainants (& Reps) |  | Suspected Offenders |  | | Suppliers |  | Advisors/ Consultants |  | License/ Permit Holders |  | | Offenders |  | Benefits Recipients |  | Inspected Persons |  | | Claimants |  | Carers (& Reps) |  | Captured on CCTV |  | | Students/ Pupils |  | Incident witnesses |  | Employees of other Orgs |  | | Landlords |  | Employees/ Contractors |  | Holders of Public Office |  | | | | |
| **Number of Data Subjects this involves:** | | **Comments on categories of Data Subject:** | |
|  | |  | |
| **3 (b) – Is personal identifiable information being used for statistical/analytical/research purposes in relation to Adult Social Care?** | | | |
| Yes  No  N/A  **If Yes, have you considered the National Data Opt Out guidance and are using a ‘cleaned’ data set, as laid out in the guidance?**  Yes  No | | | |
| **3 (c) - Does the dataactivity include the use of data relating to criminal convictions and offences?** | | | |
| Yes  No | *If yes, please describe the data collected:* | | |
|  |  | | |

|  |  |  |
| --- | --- | --- |
| **4 - Privacy Notices and Transparency** | | |
| *Please provide any information provided to Data Subjects that explains how their data will be processed, such as a Privacy Notice or wording on a consent form.* | | |
| Does a Privacy Notice exist for this processing? | Yes  No | *Insert hyperlink or embed notice here:* |
| If relying on consent, is a consent form in place? | Yes  No | *Insert hyperlink or embed consent form here:* |

|  |  |
| --- | --- |
| **4 (a) - Compliance with accuracy and retention policy:** (*link with Retention Schedule*) | |
| **Please answer the following** | |
| Accuracy | Data accuracy will be maintained by [ *provide the relevant detail*] |
| Retention Schedule | This data will be deleted after Choose an item. years |

|  |  |
| --- | --- |
| **4 (b) Has there been any consultation with Data Subjects?** | |
| Yes  No | If No, why not? |
| **4 (c) Does your activity involve engaging with Service Users or Members of the Public?** | |
| Yes  No | If Yes, please contact the Research and Citizen Insight Team to discuss your requirements, as you may need to complete the research governance process: [citizeninsight@essex.gov.uk](mailto:citizeninsight@essex.gov.uk) |

|  |  |  |
| --- | --- | --- |
| **5 - Data Controller/Processor** | | |
| **Is ECC the** [**Data Controller**](#_Data_controller:)**?**  *(If you are unsure please describe below and the IG Team will assess).* | | Yes  No |
|  | | |
| **Is ECC a Joint Controller?**  *(If Yes, please provide the details of the other controller involved)* | | Yes  No |
|  | | |
| **Does the processing involve** [**Data Processor(s)**](#_Data_Processor(s):_(See)**?**  *If so, who are the* [*third parties*](#_Third_party:) *involved in this activity?* | | |
|  | | |
| **Do we have a statutory duty to provide this service and process the personal data?** | **If yes, please name the relevant legislation/statutory instrument:** | |
| Yes  No |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6 – Transfer/storage outside the UK and outside the** [**EEA.**](#_The_EEA:)  *Where will information be transferred or stored?*  *This includes systems and support services for those systems. Consider all parties involved.* | | | | |
| 6 a) | Will all information remain in the UK? | Yes  No | *Yes – Go to section 7 or;*  *No – go to 6 b)* | |
| 6 b) | Will all information remain in the EEA? | Yes  No | Please detail country: | *Yes – Go to 6 d)*  *No – Go to 6 c)* |
|  |
| 6 c) | If outside of the EEA, where will information be stored/transferred? | Please detail: |  | *Then go to 6 d)* |
|  | | |
| 6 d) Describe why it is necessary to transfer information outside of the UK: | |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **6 e) - Transfer outside the** [**EEA.**](#_The_EEA:)  *If the answer to 6b was yes, please complete:* | | | |
| **Select safeguards:** | | **Appropriate conditions – derogation for situation:** | |
| Adequacy Decision |  | Where it is in the public interest established in UK law |  |
| To defend legal claims |  |
| Standard Contract Clauses |  | In the vital interests of the data subject or others |  |
| Public registers |  |
| Binding Corporate Rules |  | NON-STATUTORY ONLY - Explicit consent of the Data Subject |  |
| NON-STATUTORY ONLY - Where necessary for the performance of a contract |  |

|  |
| --- |
| **7 – What security measures will be implemented to protect the data?** |
| *This should include whether the information will be sent/received by secure email, what access controls will be implemented as an example* |

|  |  |
| --- | --- |
| **8 – Contracts/Agreements/Protocols**  *Where a third party is processing information on behalf of ECC or we are sharing information, we need to ensure we have the right written instructions in place.* | |
| Has a Data Processing agreement been completed? | Yes  No |
| What Contract/Agreement is in place? |  |
| What Procurement Process is being implemented for this activity? |  |
| Is there an Information Sharing Protocol (ISP) in place? (please provide the title of this document) |  |
| Is this activity without formal agreements or terms in place such as an internal process or ad hoc sharing | Yes  No |

**\*End of Customer Section\***

**\*For Information Governance to complete\***

|  |  |
| --- | --- |
| **9 – Technical Services (TS) Engagement** | |
| **Has TS provided any input regarding technical controls relating to this proposed activity?** | |
| Yes  No  N/A | *If No, then the customer needs to be directed to the Security Architect for them to review this process* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **10 - Conditions for Processing** | | | | | | | | |
| Tick all relevant conditions which provide a legal basis for the processing of Personal and Special Category data. | | | | | | | | |
| **Personal Data** | | | **Special Categories** | | | | | |
| 6(1)(a) | Consent |  | 9(2)(a) | Explicit Consent |  | 9(2)(g) | Public Interest |  |
| 6(1)(b) | Contracts |  | 9(2)(b) | Employment, Social Security, Social Protection Law |  | 9(2)(h) | Medicine, Employee Capacity, Medical Diagnosis, Health or Social Care |  |
| 6(1)(c) | Legal Obligation |  | 9(2)(c) | Vital Interests |  | 9(2)(i) | Public Health |  |
| 6(1)(d) | Vital Interests |  | 9(2)(d) | Not-for-Profit Body |  | 9(2)(j) | Archiving, Scientific and Historical Research or Statistical Purposes |  |
| 6(1)(e) | Public Interest/ Official Authority |  | 9(2)(e) | Made Public |  |  | | |
| 6(1)(f) | Legitimate Interests |  | 9(2)(f) | Legal Claims / Judicial |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **11 - High Risk Processing** | | | |
| Does the processing meet the criteria of High Risk processing as defined by the Information Commissioner’s Office? | | | |
| * Systematic and extensive profiling with significant effects |  | Profiling children or targeting marketing or online services at them |  |
| * Processing of special category, for law enforcement purposes or criminal offence data on a large scale |  | Processing data that might endanger the individual’s physical health or safety in the event of a security breach. |  |
| * Systematically monitoring publicly accessible places on a large scale, e.g. CCTV |  | Profiling or special category data to decide on access to services; |  |
| * New technologies, or changes to how we use technologies |  | Profiling individuals on a large scale |  |
| * Where we intend to match data or combine datasets from different sources |  | Where processing genetic or biometric data |  |
| * Where we collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’) |  | Where international transfers will be necessary |  |
| * Processing to track individuals’ location or behaviour |  | **High Risk?**   Yes  No | |

|  |  |  |  |
| --- | --- | --- | --- |
| **12 - Compliance with Data Protection Principles (the principles of Accuracy and Storage are addressed by the customer in section 4a):** | | | |
| **Have the following principles been addressed? (If the answer is ‘No’ to any of the below then please provide an explanation for the risk that has been assessed)** | | | |
|  | **Yes** | **No** | **Comments** |
| Lawfulness, Fairness and Transparency |  |  |  |
| Purpose limitation |  |  |  |
| Data Minimisation |  |  |  |
| Integrity, Availability and Confidentiality |  |  |  |

**Data Protection Act 2018 (DPA 2018) (Law Enforcement Processing) ONLY**

|  |
| --- |
| **13 - Is the above data processed for** [**Law Enforcement purposes**](#_Sensitive_personal_information:)**?**  *This must be the primary purpose for processing the data and we must have enforcement powers to*  *do so.* |
| Yes  Yes (continue completing this section)  No (continue to section 16) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **14 - Conditions for Sensitive Processing** | | | | | |
| Tick all relevant conditions which provide a legal basis for sensitive processing under part 3.  [Schedule 8 conditions.](http://www.legislation.gov.uk/ukpga/2018/12/schedule/8/enacted) | | | | | |
| 1 | Judicial and Statutory Purposes |  | 6 | Legal Claims |  |
| 2 | Administration of Justice |  | 7 | Judicial Acts |  |
| 3 | Protecting Individual’s Vital Interests |  | 8 | Preventing Fraud |  |
| 4 | Safeguarding of Children and of Individuals at risk |  | 9 | Archiving etc. |  |
| 5 | Personal data already in the public domain (by the Data Subject) |  |  | | |

|  |  |  |
| --- | --- | --- |
| **15 - Transfer outside the** [**EEA.**](#_The_EEA:) | | |
| **The transfer is only permitted if the following three conditions are met:** | | |
| **Condition 1** | Necessary for Law Enforcement Purposes |  |
| **Condition 2** | Based on an Adequacy Decision (section 74) or; |  |
| Appropriate Safeguards (section 75) or; |  |
| One of the Special Circumstances below: |  |
| (a) | To protect the vital interests of the Data Subject or another person |  |
| (b) | To safeguard the legitimate interests of the Data Subject |  |
| (c) | For the prevention of an immediate and serious threat to the public security of a member state or third country |  |
| (d) | In individual cases for any of the law enforcement purposes |  |
| (e) | In individual cases for a legal purpose. |  |
| **Condition 3** | Recipient is a relevant authority in a third country or a relevant international organisation.  *(If neither, further sections may apply, see* [*chapter 5*](http://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/5/enacted)*)* |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **16 – Risk Description** | | | | |
| **Risk Number** | **Risk Description** | **Score and Risk Probability Indicator before mitigations** | **Mitigating Factors** | **Score and Risk Probability Indicator after mitigations** |

1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R1 |  | Choose an item.  Overall Grading  Choose an item. |  | Choose an item.  Overall Grading  Choose an item. |
|  |  | Choose an item.  Overall Grading  Choose an item. |  | Choose an item.  Overall Grading  Choose an item. |
|  |  | Choose an item.  Overall Grading  Choose an item. |  | Choose an item.  Overall Grading  Choose an item. |

[Corporate Risk Assessment](https://cms-intranet.essex.gov.uk/Documents/POLICY_Information_Risk_Toolkit.docx)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **17 – Has this processing been fully updated on the Information Asset Register (RoPA)?** | | | | |
| Yes  N/A | **Asset (or sub-asset) ID:** |  | **Flow ID:** |  |

|  |  |
| --- | --- |
| **18 - Customer agreement** | |
| Please sign to confirm that IG advice given has been followed as documented above and that any new changes to this activity will be notified to the IG Team so that a review can be undertaken prior to the activities annual review date as denoted below.  **Please Note:** A further review will take place on the 3rd Month of this activity being approved | |
| **Name:** | |
| **Date:** | |
| **Annual DPIA Review will be completed on the following date:** Select Date | |
|  | |
| **19 - Information Governance approval** | |
| **Name** | **Date** |
|  | Select Date |
| **Annual DPIA Review will be completed on the following date:** | Select Date |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **20 – Additional Approvals** | | | | |
|  | | **Name** | **Date** | **Comments** |
| **Information Governance** | **Scope/Design:** |  | Select Date |  |
| **Implementation:** |  | Select Date |  |
| Further sign offs if required: | | | | |
| **Data Protection Officer (DPO)** | **Sign off residual risks if IG have been unable to mitigate fully:** |  | Select Date |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| If prior consultation with the ICO was sought: | | | | | | |
| **Date of request for consultation** | **Date of acknowledgement** | | **Date response due** (Generally 8 weeks, but can extend for a further 6 weeks) | **Date of response** | **ICO opinion** | |
| Select Date | Select Date | | Select Date | Select Date |  | |
| **Senior Information Risk Officer (SIRO)** | | **Name** | | | **Date** | **Comments** |
|  | | | Select Date |  |
| **Supporting Documentation**  **[Hyperlink or embed here]** | |  | | | | |

**Guidance:**

# Personal Data:

Information about a living individual that identifies them either on its own or with other data. Such as:

|  |  |  |
| --- | --- | --- |
| Name | Address | Date of Birth |
| IP Address | Location Data | Online Identifier |

# Law Enforcement Purposes: The prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Only Competent Authorities can process personal data for law enforcement purposes. If we have enforcement powers, e.g. Trading Standards, School Penalty Notices, Coroners this may apply, but it would not apply to processing where law enforcement is not the primary purpose, e.g. Child and Adult protection services.

# Data Controller: (See the ‘key terms’ link below to the ICO website for further details).

*‘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’*

In most cases if ECC need to conduct work or commission a service to do this work on our behalf, we will be the Data Controller for the information which is processed in order to do that work.

# Data Processor(s): (See the ‘key terms’ link below to the ICO website for further details).

*‘means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’*

This will usually be the third party we contract to do work on our behalf or provide us with systems.

# Business Information:

Information not relating to individuals such as finance information, project documentation or any other information we would not want to be out in the public domain.

# Third Party:

A party who will be processing information on our behalf. Such as a partner, a commissioned provider, another party involved in the activity. This could also be a volunteer, person on work experience, a consultant, or anyone who is not employed by ECC but is handling our information.

# The EEA:

The EEA includes EU countries and also Iceland, Liechtenstein and Norway.

[**https://www.gov.uk/eu-eea**](https://www.gov.uk/eu-eea)

Consider where the information is transferred or stored. For instance, some companies have their servers hosted outside the EEA and this would not meet Data Protection requirements.

# For more information:

Please see the guidance document here: [IGIA Guidance](https://cms-intranet.essex.gov.uk/Documents/IG%20Impact%20Assessment%20Guidance.docx)

Please see some [**key terms**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/) on the ICO website

Here are the ECC [information policies](https://cms-intranet.essex.gov.uk/Pages/Information_policies.aspx)

You can contact the information governance team on:

[informationgovernanceteam@essex.gov.uk](mailto:informationgovernanceteam@essex.gov.uk) - 03330 139824