Restricted – None

London Counter Fraud Hub Privacy Impact Assessment Live Service

File Name: CIPFA-LCFH-DPIAv1.1

Date Published: 29th January 2019

Version: 1.1

Status: Final

Author: LCFH Project Team

Approved by	
London Borough of Ealing	**Date:**
Lorraine Cox (Corporate Information Governance Manager)	03/07/2018
Kevin Griffin (Chief Technical Architect)	03/07/2018
David Arrowsmith (ICT Technical Expert - Compliance and Change)	03/07/2018

DOCUMENT INFORMATION

Master Location:	Document1
File Name:	Document1

CHANGE HISTORY

Version No.	Date	Details of Changes included in Update	Author(s)
1.0	13/6/18		LCFH Team
1.1	29/01/19	Updated to reflect Secure network and PSN gateway	LCFH Team

RELATED DOCUMENTS

Document Name	Issue Status & Date	Owner

STATEMENT OF COPYRIGHT

Contents

1. Introduction

This privacy impact assessment (PIA) is undertaken to identify and minimise privacy risks related to the implementation of the London Counter Fraud Hub a service which is being delivered by the Chartered Institute of Public Finance and Accountancy (CIPFA).

2. Identifying the need for a privacy impact assessment

2.1 Aims and Objectives

The London Counter Fraud Hub (LCFH) project objective is to combine data from London boroughs and third party data sources to provide a fraud and error analytics framework which will assist councils in their ongoing work to detect and deter fraud. The findings will be presented back to councils for further investigation. The LCFH will also provide additional investigatory capacity which can be used at the discretion of councils.

The LCFH will also provide the ability to introduce an automated recovery service for simple high volume/low value cases that would not require further investigation.

In addition the LCFH will prevent fraud and error by providing an enquiries portal to end users that accesses the analytical database, and provides a summary of any risk score associated with an individual in LCFH.

The LCFH will deploy advance data analytics across all the data to enable the detection and prevention of fraud across local authority boundaries.

The LCFH will use proven technology known as a data integration and analytics engine called NetReveal, this enterprise risk management platform is developed by BAE Systems who are a subcontractor of CIPFA

The findings from the analytics engine will be presented through a case management system called Enterprise Investigation Manager which will also be provided BAE Systems enabling end users to triage, investigate and manage workflows.

This technology is used in HMRC; the National Crime Agency; the Insurance Fraud Bureau and across commercial sectors to integrate and analyse discrete data sources and create flags for review by experienced counter fraud professionals.

2.2 The benefits

The LCFH will act as an identification and prevention tool providing councils an important new resource to identify and prevent individuals from committing fraud against London local authorities and taxpayers

The LCFH project will:

- Minimise fraud losses for councils in London
- Detect fraud across boundaries, detect fraud and maximise recovery opportunities by taking advantage of advanced technology and automation
- Allow councils to undertake investigations they do not currently have capacity to undertake

- Prevent fraud by disseminating alerts, intelligence, analysis and good practice, allowing councils to act to eliminate fraud opportunities before they are widely exploited
- Deter potential fraudsters through maintaining a robust profile and by publicising successes in partnership with councils
- Provide councils with high quality fraud leads enabling them to better target fraud investigation resources
- Maximise recoveries by collaborating with councils on investigation and recovery

2.3 Why the need for a PIA was identified

The LCFH will involve the collection of new personal data which has not previously been held by CIPFA however through this operation this data will have already have been aggregated by local authorities and third party organisations.

CIPFA will collect the data with the consent of the local authorities and third parties. CIPFA will advise local authorities what is happening with their information and that their data is being shared for the prevention and detection of fraud; the apprehension or prosecution of offenders; to identify data irregularities that maybe indicative of fraud; and to enable the assessment or collection of any tax or duty or any imposition of a similar nature.

The data in scope is non-sensitive personal data (names, dates of birth, addresses etc.) however once the data is processed within the LCFH, for the purposes of identifying potentially fraudulent applications, this may result in the generation of sensitive personal data in connection with the alleged commission of an offence and/or the disposal of proceedings or the sentence of any court in relation to the commission of an offence therefore this would represent additional intrusion to individuals.

3. Information Processing

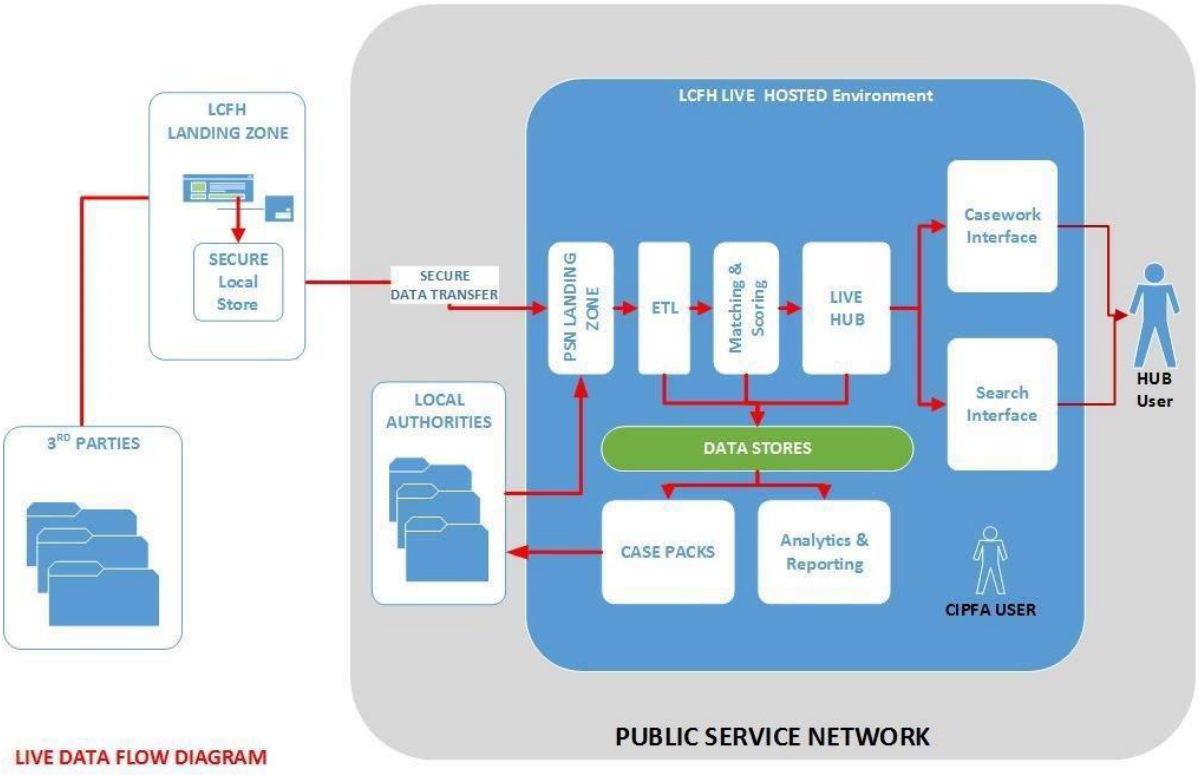
The LCFH will be processing 3 initial data sets from local authorities which are Council Tax, Business Rates and Housing, in order to identify fraud types which are Single Person Discount, National Non Domestic Rates and Housing Tenancy.

In addition, the LFCH will use data from third parties which are Equifax credit reference agency data; Halo Death related data; Ordnance Survey map and point of interest data.

The LCFH live service will collect new data from the local authorities and third parties. CIPFA will house the LCFH in a new secure hosted digital environment. This environment is a cloud based secure hosted facility that has a number of government accreditations and relevant industry standard accreditations.

The environment is connected to the Public Secure Network and has a Secure Internet Gateway that requires certified user access using encrypted certificates and authenticated users.

The diagram below details the flow of data that the LCFH will receive from the local authorities and third parties during the live service:



The LCFH system collects data over the PSN via a secure file transfer server,that requires accredited and encrypted certification methods. The data is placed into a secure directory ready for processing by the analytics engine.

The analytics engine parses the data and analyses it across the datasets to identify any potential fraud that may be highlighted. This analysis is displayed within an application that is a role based system that segregates data between the participating authorities, ensuring that there is no cross-access of data within the application. Users of the system will have the

ability to export data relating to any cases identified but this will be fed back using secure file transfer back to the local authority over the PSN.

Data will not be shared by anyone who has not signed up for the system and anyone who is not part of an agreed user list maintained by CIPFA and the local authorities

In addition to complement the live service CIPFA will undertake the following actions:

- ensure all staff involved with the hub have been vetted
- ensure all staff involved with handling LCFH data are suitably trained
- ensure all staff undertake mandatory information security e-learning
- continue its program to maintain ISO27001 accreditation
- ensure its PSN accreditation is maintained and accurate
- implement necessary access controls
- include terms in applicable MOUs, agreements and contracts that address safeguards to be implemented to ensure appropriate use of information
- implement audit procedures to ensure compliance with security standards
- appoint a security officer
- provide details of its security policy
- provide details of information governance
- maintain a data security plan
- maintain a security architecture
- sign a data sharing agreement with each party providing data
- sign a data transfer agreement with each party providing data
- sign a data processing agreement with each party providing data

4. Consultation Requirements

A key component of fairness is that individuals should know who is processing data about them and the purpose of the processing. Processing activity should generally be within the reasonable expectations of an individual, should be explained in a fair processing or privacy notice and people should not be misled about how their data is used.

CIPFA will meet this by consulting internally with:

- CIPFA LCFH Information Assurance
- LCFH Enterprise Architecture
- LCFH Project Team
- Legal Counsel

CIPFA will meet this by consulting externally with:

- BAE Systems
- Local Authorities
- 3rd Party Data Providers
- Lead Authority
- Other people and organisations as appropriate

5. Identifying the privacy and related risks

Potential privacy risks, the associated compliance and corporate risks have been considered and are in the table below:

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Information provided by local authorities and third parties to CIPFA is held insecurely BAE Systems	Information could become compromised	Large volume of personal data is identified	May lead to sanction by ICO Reputational damage Possible claims for compensation
Inaccurate, insufficient or out of date information	Inaccurate data is held about individuals	Non-compliance with DPA	May lead to sanction by ICO Reputational damage
Excessive or irrelevant personal information being processed	Data is not properly managed	Non-compliance with DPA	Distrust by data providers about how information is used Reputational damage and loss of business
Retention of data for excessive time periods	Information might be used for longer than is necessary	Non-compliance with DPA	Distrust by data providers about how information is used Reputational damage and loss of business
Unwanted disclosure of information to recipients by CIPFA	Inadequate disclosure controls increase the likelihood of information being shared inappropriately	Non-compliance with DPA	Distrust by data providers about how information is used Reputational damage and loss of business Possible claims for compensation
Use of information in a way unacceptable to the individual	Incorrect usage of the information could cause unjustified intrusion	Non-compliance with common law duty of confidentiality Non-compliance with DPA	Distrust by data providers about how information is used Reputational damage and loss of business Possible claims for compensation
Fair processing	Transparency -	Non-compliance	May lead to

notice issued does not explicitly reference CIPFA and/or the LCFH	information is used for different purposes without knowledge of people	with DPA	sanction by ICO Reputational damage and loss of business
Linking or merging of data incorrectly identifies individuals	Identification or disclosure of information about individuals incorrectly implying fraud Vulnerable individuals are identified causing undue distress	Non-compliance with DPA	Distrust by data providers about how information is used Reputational damage and loss of business Possible claims for compensation

6. Identifying privacy solutions

The following solutions have been identified to reduce the risks:

Risk	Solution(s)	Result (Is the risk eliminated, reduced, or accepted?)	Evaluation (Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?)
Information provided by local authorities and third parties to CIPFA is held insecurely.	CIPFA have a secure landing zone and data is held in a secure segregated environment. All data will be processed within this sealed digital environment	Risk is eliminated	Recommended solution is proportionate and compliant to the project and minimises any impact on individuals and/or data providers
Inaccurate, insufficient or out of date information	Arrangement is in place to conduct a data quality assessment to test out data and ensure it is generated correctly before being ingested into the analytics solution	Risk is reduced	Recommended solution is justified however risk needs to be managed
Excessive or irrelevant personal information being processed	Fraud indicators and fraud risk scores have been pre-determined for the data sets and fraud types during a workshop with relevant data providers therefore information processing is limited	Risk reduced	Recommended solution is proportionate and compliant to the project and minimises any impact on individuals and/or data providers
Retention of data for excessive time periods	CIPFA will issue destruction notices to confirm that information has been permanently	Risk eliminated	Recommended solution is proportionate and compliant to the project and minimises any impact on individuals and/or data providers

	deleted		
Unwanted disclosure of information to recipients by CIPFA	Data is held in a secure segregated digital environment. No data will be made available in a form to anyone outside the service subscribers. CIPFA will appoint a representative responsible for security. CIPFA will develop, implement, maintain, review and update its security measures, policies, procedures and systems in conjunction with the data providers	Risk eliminated	Recommended solution is proportionate to the project and minimises any impact on individuals and/or data providers
Use of information in a way unacceptable to the individual	CIPFA will retain a record (for a specified period) of any processing of personal data it carries out on behalf of the local authority. The local authority has right of audit to inspect all facilities, equipment, records, documents and electronic data relating to the processing of personal data	Risk is eliminated	Recommended solution is justified, compliant and proportionate and minimises any impact on individuals and/or data providers
Fair processing notice issued does not explicitly reference CIPFA and/or the LCFH	CIPFA will update its fair processing notice when it is applicable to do so and will publish it to relevant parties	Risk is managed	Recommended solution is compliant and proportionate and minimises any impact on individuals and/or data providers
Linking or merging of data incorrectly identifies	CIPFA to ensure fraud matching indicators and	Risk is reduced	Recommended solution is compliant and proportionate and minimises any impact on

individuals	analytics algorithms are correctly set to reduce false positives		individuals and/or data providers

7. Signing off and recording the PIA outcomes

The following solutions to reduce the risks have been approved for implementation:

Risk	Approved solution	Approved by
Information provided by local authorities and third parties to CIPFA is held insecurely BAE Systems	Confirm arrangements in place prior to ingesting data that BAE Systems has a secure landing zone and data is held in a secure walled gardened digital environment	Project Manager
Inaccurate, insufficient or out of date information	Confirm arrangements are in place to conduct data quality assessment	Project Manager Enterprise Architect
Excessive or irrelevant personal information being processed	Arrangements in place to undertake workshops on the data sets and fraud types to pre-determined fraud indicators and risk scores	Project Manager LCFH Manager
Retention of data for excessive time periods	Arrangements in place to issue destruction notices to confirm that information has been permanently deleted	Project Manager LCFH Manager
Unwanted disclosure of information to recipients by CIPFA	Confirm arrangements in place to appoint a representative responsible for security and that no output will be generated by the LCFH during the pilot phases	Project Manager LCFH Manager
Use of information in a way unacceptable to the individual	Confirm arrangements in place to retain a record of any processing of personal data carried out on behalf of the local authority and/or third party data provider	Project Manager LCFH Manager
Fair processing notice issued does not explicitly reference CIPFA and/or the LCFH	Update the fair processing notice prior to rollout of the LCFH live service and publicise to relevant parties	Project Manager LCFH Manager
Linking or merging of data incorrectly identifies individuals	Confirm arrangements are in place to correctly set fraud matching indicators and analytics algorithms to reduce false positives	Project Manager Enterprise Architect