Privacy Notice – Counter Fraud

Who we are

London Borough of Havering (LBH) is registered with the Information Commissioner's Office (ICO) as a 'Data Controller' This privacy notice applies to you ('the service user') and LBH ('the Council'). The Council takes the privacy of your information very seriously.

This privacy notice relates to our functions relating to Counter Fraud. It provides additional information that specifically relates to this particular service, and should be read together with our general privacy notice, which provides more detail, including what data we process about you and from you.

Why Counter Fraud processes your data

The Council uses your personal information in order to carry out activities and obligations associated with counter fraud investigations.

The Council has a statutory duty under Section 151 of the Local Government Act 1972 to establish a clear framework for the proper administration of the authority's financial affairs.

To perform that duty the Section 151 Officer relies, amongst other things, upon the work of Counter Fraud in the prevention and detection of fraud and error in the following areas, including but not limited to:

- Council Tax
- Non-Domestic Rates (Business Rates)
- Direct payments from Social Care
- Electoral Register
- Employee/Internal
- Housing/Tenancy
- Insurance Claimants
- Licences, e.g. market trader/ operator, and (new) personal licences to supply alcohol
- School admissions
- Transport passes, including residents' parking permits and blue badges

The lawful basis for processing your data

We process and share the information provided to us from council services to help to prevent and/or detect potential fraud and crime, by both conducting our own Data Matching and sharing this information with other public bodies, such as the Department for Work and Pensions, other Local Authorities, HM Revenues and Customs, and the Police where required to be disclosed or under the relevant exemptions concerning 'crime and taxation' and 'Information required to be disclosed by law etc or in connections with legal proceedings' set out in Part 1 of Schedule 2 of the Data Protection Act 2018.

Our lawful basis under UK GDPR is Article 6(1)(c) legal obligation, Article 6(1)(e) public task (with a basis in law) and Article 9 (g) Substantial Public Interest.

Our lawful basis under UK GDPR Article 10 are:

Data Protection Act 2018 Schedule 1, Part 1:

- Para 2(1) the processing is necessary for health or social care purposes and (e) the provision of social care

Data Protection Act 2018 Schedule 1 Part 2:

- Para 6 statutory and government purposes, processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest
- Para 7 processing necessary for the administration of justice
- Para 10(1) Preventing or detecting unlawful acts, the processing is necessary for the purposes of the prevention or detection of an unlawful act

Data Protection Act 2018 schedule 1 Part 3:

- Para 33 necessary for legal claims, in connection with legal proceedings or in connection with legal rights

The basis in law for Counter Fraud investigations are set out below:

- Section 151, Local Government Act 1972
- Local Audit and Accountability Act 2014 (Part 6)
- Schedule 2, Data Protection Act 2018
- The Police & Criminal Evidence Act 1984 (PACE)
- Criminal Procedures and Investigations Act 1996
- The Criminal Justice Act 1967
- Section 68 of the Serious Crime Act 2007
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- Fraud Act 2006
- Bribery Act 2010
- Prevention of Social Housing Fraud Act 2013
- The Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000

How we use your data and who we may share with

Havering Council is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and crime including fraud and money laundering.

We will only share your personal data with the following organisations where it is appropriate and legal to do so:

- The Cabinet Office
- Government agencies
- Specified anti-fraud organisations (SAFOs) and CIFAS
- The Police
- Judicial agencies e.g. Courts
- Department of Work and Pensions
- HMRC
- Other local authorities for similar purposes

- Credit reference agencies
- In certain circumstances employers

We will not share your personal data with any other third party unless there is a risk of serious harm or threat to life.

National Fraud Initiative

The Cabinet Office currently requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Cabinet Office for matching for each exercise, and these are set out in the Cabinet Office's guidance.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information.

Computerised data matching allows potentially fraudulent claims and payments to be identified.

Where a match is found it may indicate that there is an inconsistency which requires further investigation.

No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

How long we will keep your data

We will keep your data safe and secure for a period of 6 years in line with our retention Schedule. After this time, it will be securely destroyed.

Records will only be retained beyond the default retention period if their retention can be justified for statutory, regulatory, legal or security reasons.

How we protect your data

We comply with all laws concerning the protection of personal information and have security measures in place to reduce the risk of theft, loss, destruction, misuse or inappropriate disclosure of information. Staff access to information is provided on a need-to-know basis and we have access controls in place to help with this.

Know your rights

We process your data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Find out about your individual rights at or at www.havering.gov.uk/privacy or https://ico.org.uk/your-data-matters/ If you have any queries or concerns relating to data protection matters, please email: **dpo@havering.gov.uk**