

Privacy Notice: Durham County Council Internal Audit, Risk and Fraud: Corporate Fraud Team

This Privacy Notice tells you about what information we collect about you, how we use that information and who we share it with.

1. Who we are and what we do

Durham County Council has a responsibility to protect the public purse and recognises the potentially significant risk that fraud and corruption pose to the achievement of the Council's aims and objectives. The public also expects the Council to safeguard public funds and ensure they are available and used for their intended purpose that of providing services for the residents and service users of the Council.

As part of this responsibility the Council actively participates in the National Fraud Initiative (NFI), a national data matching exercise currently run by the Cabinet Office under its statutory powers.

As well as the NFI, under the Council's Counter Fraud and Corruption Strategy and within the Counter Fraud Operational Plan, a programme of local data matching/analytical exercises is also included to proactively seek out fraud and error in areas identified as being at risk of fraud.

The Corporate Fraud Team has data warehousing software which allows for this programmed work to be carried out, by collecting data from various sources both internally and from external organisations i.e. other Local Authorities.

For further information about the services available please contact the Corporate Fraud Team on:

Telephone: 03000 266745
Email: corporatefraudteam@durham.gov.uk
Website: www.durham.gov.uk/fraud
In person: County Hall, Durham, DH1 5UL

For the purposes of Data Protection, Durham County Council is the Data Controller.

2. What type of personal information do we collect and how do we collect it?

The majority of personal information we collect is electronic but we can receive paper documents to collect personal information to deliver the service.

We may collect the following types of Personal Data:

- Name;
- Contact details (addresses, telephone numbers, email addresses etc);
- Date of birth;
- National insurance number;
- Details of family and household members;
- Financial information;
- Current employment and employment history;

- Identity information (passports, driving licenses, birth certificates);
- Vehicle information;
- Photographs and video footage.

Special category data:

We may also collect Health information, such as evidence of injuries for an insurance claim or evidence to assist investigations into potential blue badge fraud or direct payment fraud.

For the data warehousing software, we receive monthly data extracts of current personal information from the following areas:

- Blue Badges
- Business Rates
- Council Tax
- Council Tax Reduction Claims
- Direct Payments
- Durham County Council Payroll
- Durham County Council Pension
- Electoral Role
- Housing Waiting List
- Insurance Claims
- Leisure Memberships
- Licensing (Taxi, Market Traders, Personal Alcohol and Scrap Metal)
- Livin Social Housing Tenants

We are currently reviewing further data extracts and this list will continue to grow.

The NFI and local data matching allows the comparison of various data sets against other data sources to help detect and prevent potential fraud and error in areas such as blue badges, concessionary travel, council tax, creditors, electoral role, housing benefit, housing waiting list, licensing, payroll, pensions and social care. The main NFI data matching exercise currently occurs over a two year cycle but is moving to real-time and 'near' real-time fraud prevention activity. A supplementary NFI exercise takes place annually in relation to the Electoral Register and Council Tax Single Person Discounts. Local data matching can be done in real time and there will be a programmed activity within the Counter Fraud Operational Plan.

We may collect information about you in the following ways:

- Most of the personal information we hold is provided by you in applications and the supporting information you include with it;
- Paper forms;
- Online information;
- Communication with yourself (telephone, in person, written);
- Information received from a third party / external organisation;
- Allegations of fraud reported direct to the Corporate Fraud Team.

The legislation that allows us to collect this information is:

- Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013;
- Prevention of Social Housing Fraud Act (Power to Require Information) (England) Regulations 2014;
- Local Government Finance Act 1992;
- Regulation of Investigatory Powers Act 2000;
- Criminal Procedures and Investigations Act 1996;
- Police & Criminal Evidence Act 1984;
- Freedom of Information Act 2000;
- Data Protection Act & General Data Protection Act 2018;
- Human Rights Act 2008;
- Local Government Act 2000;
- Public Interest Disclosure Act 1998;
- Part 6 of the Local Audit and Accountability Act 2014;
- Digital Economy Act 2017.

The legislation that allows us to prosecute is:

- Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013;
- Prevention of Social Housing Fraud Act (Power to Require Information) (England) Regulations 2014;
- The Fraud Act 2006;
- Forgery and Counterfeiting Act 1987;
- Computer Misuse Act 1990;
- Identity Card Act 2006;
- The Bribery Act 2010;
- Welfare Reform Act 2012;
- Housing Act 1996;
- Road Traffic Regulation Act 1984;
- Proceeds of Crime Act 2002.

3. What is our lawful basis to obtain and use your personal information?

Lawful Basis (Article 6)

- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Conditions from Article 9

Conditions for processing special category data are known under Article 9.

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest.

4. What is your personal information used for?

We use your personal information:

- To prevent, detect and investigate fraud and other crime;
- To prosecute, sanction and redress fraudsters;
- To protect the public purse;
- To verify that the information you have supplied is correct and accurate.
Where necessary, we will do this by verifying your information with other Local Authorities and Government Departments for example.

It is the Council's intention to continue with the existing arrangements and further explore opportunities for data matching both internally between services and externally with neighbouring authorities, and develop links with other external agencies, to enhance opportunities for information sharing.

Data matching is carried out by the Corporate Fraud Team to assist the corporate framework to help counter any fraudulent activity. The team proactively use council data to assist the prevention and detection of crime.

The sharing of fraud intelligence between authorities via restricted internet forums and groups is critical in alerting to rising fraud trends and is a mechanism the Council actively engages in. The Council receives regular data analysis and fraud information alerts from its memberships.

5. Will your personal information be shared?

Your personal information can be shared if the law allows this. We do investigate and share information with other local authorities, other law enforcement agencies and any partners that we have service level agreements in place.

We may also enter into specific information sharing arrangements with partners such as local authorities where it would support our statutory functions.

The Corporate Fraud Team also shares personal information with (and receives information) from a number of other organisations as part of our prevention and detection of fraud. Such organisations may include the Police, Home Office, Cabinet Office, DWP, Registered Social Landlords and Local Authorities. Any information sharing is managed in accordance with relevant privacy and data protection legislation.

We have data sharing agreements with:

- Believe Housing - we investigate Tenancy Fraud and do Right to Buy verification checks on their behalf and therefore could share your personal data to prevent and detect fraud;

- Livin Housing - we investigate Tenancy Fraud and do Right to Buy verification checks on their behalf and therefore could share your personal data to prevent and detect fraud;
- Karbon Homes - we do Right to Buy verification checks on their behalf and therefore could share your personal data to prevent and detect fraud;
- Bernicia Housing - we do Right to Buy verification checks on their behalf and therefore could share your personal data to prevent and detect fraud;
- Gentoo Group - we do Right to Buy verification checks on their behalf and therefore could share your personal data to prevent and detect fraud.
- Gateshead Metropolitan Borough Council
- Newcastle City Council
- Durham Constabulary

If you would like confirmation of who we do share information with please contact us.

6. How do we keep your information secure?

The security of your personal information is important to us. The records we keep about you are secure and are confidential within the Council. The Council have a range of procedures, policies and systems to ensure that access to your records are controlled appropriately.

Anyone who receives information from us is also under a legal duty to only use the information for the purposes agreed and keep the information secure and confidential.

7. How long will we keep your personal information?

After we deliver a service to you, we have to keep your information as a business record of what was delivered. The type of service will determine how long we have to keep it. Our corporate and service retention guidelines show how long we keep it for different purposes. This ranges from months for some records to decades for more sensitive records.

The retention periods for the Corporate Fraud Team are as follows:

➤ <u>Type of personal information</u>	➤ <u>Retention period</u>
<ul style="list-style-type: none"> • Data Warehousing Extracts held in Corporate Fraud System (internal and external). 	<ul style="list-style-type: none"> - 1 month <p>Note: Each month a new data extract is loaded and replaces the previous month.</p>
<ul style="list-style-type: none"> • Data Warehousing Extracts received from Service Areas (stored in secure server). 	<ul style="list-style-type: none"> - Date loaded into Warehouse + 1 year
<ul style="list-style-type: none"> • Data Warehousing Extracts received from external Organisations (stored in secure server). 	<ul style="list-style-type: none"> - 1 month <p>Note: Each month a new data extract is loaded and replaces the previous month.</p>

- National Fraud Initiative
- Current and previous exercises kept only.

Note: will follow Cabinet Office retention guidance.

8. Personal information processed outside of the European Union (EU)

We do not process your personal data outside of the EU

9. Marketing

At no time will your information be used or passed to others for marketing or sales purposes, or for any commercial use without your express consent.

10. What are your information rights?

Your Information Rights are set out in the law. Subject to some legal exceptions, you have the right to:

- request a copy of the personal information the council holds about you
- have any inaccuracies corrected;
- have your personal data erased;
- place a restriction on our processing of your data;
- object to processing;

To exercise your rights, you can apply on line or download an application form from the [DCC website](#) or you can contact the data protection team at inforights@durham.gov.uk

To learn more about these rights please see the [ICO website](#).

11. Further Information

Our Data Protection Officer (DPO) provides help and guidance to make sure we apply the best standards to protecting your personal information. If something goes wrong with your personal information, or you have questions about how we process your data, please contact our Data Protection Officer at DPO@durham.gov.uk or write to:

DPO
Floor 4 Room 143-148,
Durham County Council
County Hall,
Durham County Council
DH1 5UF

If we have not been able to deal with your query, you can also contact the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745