Privacy Notice – Corporate Fraud Team

Introduction	The Corporate Fraud Team has provided this privacy notice to help you understand how we collect, use and protect your information whilst we provide you with a corporate fraud service. The document below will describe how we may collect and process your personal information. The purpose of this document is to clearly acknowledge the Council's responsibilities in relation to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
Definitions	**Personal Data** means any information related to an identified or identifiable natural (living) person ('**data subject**') i.e. a person that can be directly or indirectly identified by reference to a name, ID reference number, email address, location data, or physical, physiological, genetic, mental, economic, cultural or societal identifier **Special Personal Data** previously known as 'sensitive personal data', relates to race, ethnic origin, politics, religion, trade union membership, genetic data, biometric data, health, sex life or sexual orientation. Records of criminal personal data must also be treated in a similar way. **Data Controller** determines the purposes and means of processing personal data. **Data Processor** is responsible for any operation which is performed on personal data on behalf of the controller e.g. collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction. **Third Party** is someone / somebody who is not the Data Controller, the Data Processor or the Data Subject.
Who we are	East Suffolk 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.

The Corporate Fraud Team assists the Council's corporate framework to help counter any fraudulent activity. The Team investigate fraud both internally and externally for the organisation and its partners.

The Council is the 'data controller' for the information which is collated and processed. This means we are responsible for deciding how we can use your information. If you want more information regarding the services delivered, please go to our website.

The Council regards lawful and correct treatment of personal information as critical to their successful operations, maintaining confidence between the Council and those with whom they carry out business. The Council will ensure that they treat personal information correctly in accordance with the law.

These corporate fraud services are statutory and the laws allowing us to collect this information are:

- 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 and Criminal Evidence Act 1984;
- Public Interest Disclosure Act 1998;
- Proceeds of Crime Act 2002
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017).

The legislation that allows us to prosecute are:

- 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 & 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;
- Money Laundering Regulations 2017.

The Data Protection Officer for ESC is Siobhan Martin, Head of Internal Audit, and can be contacted at dataprotection@eastsuffolk.gov.uk

How the law protects you

GDPR says that we are allowed to use personal information only if we have a proper reason to do so. More information on how the law protects you can be found on the East Suffolk website.

Our Responsibilities

GDPR provides us with main responsibilities for processing personal data.

All personal information provided by you is held securely and in confidence by us in our computerised and other records. When we process your personal information, we do so in compliance with GDPR.

For further information on our responsibilities, please see the East Suffolk website.

Your Rights

The GDPR provides you with the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making
9. The right to withdraw consent
10. The right to complain

Requests in relation to your rights with regards to the personal data we hold should be made verbally or in writing to the Data Protection Officer.

For further information on your rights, please see the East Suffolk website.

Your responsibilities

You are responsible for making sure you give us accurate and up to date information, and to let us know if any personal information we hold is incorrect.

When do we collect information about you?

We collect information about you from different places, including:

- Most of the personal information we hold is provided by you in applications and 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 or via a third party;
- Corporate Fraud have access to any and all information supplied to any department within the Council by individuals including customers, staff, suppliers and any other third parties.

What information do we maintain?

The information about you which we will maintain will include:

- Name; and
- Contact Details (addressees, 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 licences, birth certificates);
- Vehicle information;
- Photographs and Video footage, Social Media data;
- Health information (to assist investigations into Blue Badge fraud).

How do we use your information?

We will be using your information to:

- Prevent , detect and prosecute fraud and other crime;
- To protect the Public Purse;
- To verify the information that you have supplied is correct and accurate. Where necessary, we will do this by verifying your information with other Local Authorities and Government Departments.

We will not use your personal data for other purposes other than for what it was collated unless we have obtained your consent or for other lawful purposes (e.g. detection and prevention of fraud).

We use a risk based assessment system to make automated decisions about information in respect of undertaking any fraud referral case. This helps us to make sure our decisions are quick, fair, efficient and correct based on what we know. They are based on personal information that we have or that we are allowed to collect from others.

How long do we keep your information?

The Corporate Fraud Team delivers a fraud service and we have to keep information as a business record of what was delivered. The type of service will determine how long we have to keep it in line with our legal obligations and in line with the statutory retention periods:

- Fraud referrals and investigations (proven), evidence information and intelligence gathered – closure date + 6 years
- Fraud referrals and investigations (not proven), evidence information and intelligence gathered – closure date + 1 year
- Fraud Investigators Pocket Notebooks – date surrendered + 6 years
- Fraud interview Records (CD's) and Tapes – closure + 6 years
- Regulation of Investigatory Powers Act forms and Non RIPA forms (copies) – response date + 6 years
- Single point of Contact Department for Work and Pensions requests – Response date + 1 year
- Requests for Information – Current Financial year + 1 year
- National Fraud Initiative – Current and previous exercise kept only – in line with Cabinet Office retention guidance.

We will hold your personal information for statutory legal guidelines for an Investigations fraud case. Subject to our statutory legal obligations you may request that your personal information is deleted at any time.

Data Sharing	We will share your personal information with: • The Police; • Other responsible Authorities; • Other Local Government Departments Any information shared will be in line with the GDPR regulations and usually in connection with the prevention, detection and prosecution of crime and safeguarding. This will be via a secure messaging service.
Transferring your information overseas	Currently, we do not transfer any personal information outside of the European Economic Area (EEA).
National Fraud Initiative (NFI)	We may share information provided to us with other bodies responsible for auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud. For further information, see the East Suffolk website.