# Privacy Notice – Internal Audit

| | |
|---|---|
| **Introduction** | Internal Audit have provided this privacy notice to help you understand how we collect, use and protect your information whilst we provide assurance to the Council on its risk management, control, fraud and governance processes, and the administration of data protection requests.<br><br>The document below will describe how we may collect and process your personal information.<br><br>The purpose of this document is to clearly acknowledge the Council's responsibilities in relation to the UK General Data Protection Regulation (UK 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<br><br>**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.<br><br>**Data Controller** determines the purposes and means of processing personal data.<br><br>**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.<br><br>**Third Party** is someone / somebody who is not the Data Controller, the Data Processor or the Data Subject. |
| **Who we are** | Internal Audit is an independent function whose primary objective is to provide assurance to the Council on risk management, control, fraud and governance processes. Internal Audit is also responsible for monitoring and ensuring compliance with Data Protection.<br><br>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.

The requirement for the Council to have an internal audit function is set out in legislation: Section 151 of the Local Government Act 1972. The requirement for an Annual Governance Statement is defined in the Accounts and Audit Regulations 2015.

We administer data protection requests in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018.

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**

UK 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**

UK 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 UK GDPR.

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

**Your Rights**

The UK 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:

- During the course of internal audit and governance reviews of council provided services and of services provided to the council
- In conducting an investigation, personal information is gathered from numerous sources such as council records, external organisations, third parties, witnesses and the investigation subject.
- Directly from you when submitting a request under data protection legislation.
- From other service areas within the Council to enable us to respond to data protection requests, FOI requests, complaints and whistleblowing concerns.
- From other external parties.
- Internal Audit 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?**

Internal Audit will have access to information held by any services area within the Council in order to be able to undertake their work; this may include the following types of data:

- Personal, for example name, date of birth, address, sex and marital status
- Employment information, for example national insurance number, details of employer, salary details, employment dates, next of kin, sickness records
- Financial details, for example bank and/or building society account information including transactions and balances, mortgage accounts, insurance policies, pension information, credit history
- Health information gathered to assess eligibility for benefits
- Financial information regarding appraisal of financial standing of potential contractors
- Written statements and recordings of interviews conducted
- Other information gathered during the course of an investigation or proactive exercises.

**How do we use your information?**

Internal Audit are required to hold, or have access to, information from systems and processes across the Council so that we can:

- Fulfil legal requirements to provide an internal audit function
- Investigate referrals made under the corporate whistleblowing policy
- Maintain the central register of applications for RIPA (Regulation of Investigatory Powers Act 2000)
- Ensure the effectiveness of governance processes
- Facilitate the prevention, deterrence and detection of fraud committed against the Council

- Facilitate effective risk management within the Council
- Investigate potential irregularities
- Respond to requests and complaints made under data protection legislation
- Administer and investigate data matching under the National Fraud Initiative
- Respond to requests and complaints made under the Freedom of Information Act 2000.

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 do not use automated decision making.

**How long do we keep your information?**

We will hold your personal information for 6 years plus current year (7 years) in accordance with the Accounts and Audit Regulations 2015.

We will hold your personal information in relation to data protection requests (i.e. subject access requests and other data protection requests) for 6 years plus current year (7 years). You can request that your personal information is deleted at any time.

**Data Sharing**

We will only share your personal information where permitted by law. We will share your personal information with:

- Other internal Council services to enable the establishment of the effectiveness of corporate systems and processes.
- During the course of an investigation or audit, data may be shared with other Council departments such as Human Resources and the Corporate Fraud Team.
- Legal practitioners, tribunals and courts where criminal action is taken against an individual.
- Our partners, Norse, if you submit a data protection request which relates to the services they administer on our behalf, e.g. car parking.
- The Council's external auditors (Ernst & Young)
- Local Government Ombudsmen as requested as part of any ongoing complaint investigations
- Cabinet Office: we participate in the National Fraud Initiative, a data matching exercise, to assist in the prevention and detection of fraud. We are required to provide certain data sets. For further information, please see the section below.
- Ipswich Borough Council (IBC): Internal Audit works in partnership with IBC, and IBC Internal Audit staff have access to information relevant to the work they are undertaking.
- The police, other councils or other third parties as permitted by the UK General Data Protection Regulation and the Data Protection Act 2018.

| | |
|---|---|
| **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. |