Privacy Notice

Introduction

East Suffolk Council (ESC) considers your personal data to be of the utmost importance, and have provided this Privacy Notice to help you understand how we collect, use and protect your information whilst we provide you with a service.

The purpose of this document is to clearly acknowledge the Council's responsibilities in relation to the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

The Information Commissioner's Office (ICO) maintains a public register of data controllers. Each register entry gives details of the data controller and a general description of what the personal data held is used for.

ESC is a Data Controller and we are registered with the Information Commissioner's Office.

Elected members are also data controllers in their own right, and they are responsible for ensuring any personal information they hold or use in their office as elected members is processed in accordance with GDPR and DPA 2018. All elected members are registered with the ICO as data controllers.

Our services are diverse, statutory and discretionary and due to their wide ranging role, we have to collate and process a vast amount of personal data.

What is personal information and 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.

The legal basis for processing your personal information

GDPR and DPA 2018 say that we are allowed to use personal information only if we have a proper reason to do so. This includes sharing it with other parties. The GDPR and DPA 2018 state that we must have one or more of these reasons:

- Statutory obligation or legal duty;
- To fulfil a contract we have with you;
- We have a legitimate interest;
- We have your consent;
- It is necessary to protect public health;
- It is necessary for employment purposes.

We will only collect and process information that we need.

More information on how the law protects you can be found on the ICO website.

Our Responsibilities

GDPR Article 5 provides us with the main responsibilities to abide by, to ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purposes;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary; and
6. Processed securely.

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

The Council regards the 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 Council fully endorses and adheres to the principles of data protection as set out in the GDPR and DPA 2018.

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 and DPA 2018. We maintain strict security standards and procedures with a view to preventing unauthorised access to your data. We undertake regular testing of our IT systems. We use leading technologies, such as data encryption, fire walls and service authentication to protect the security of your data. All our staff and all third parties we may hire are required to observe our privacy standards and must complete privacy training.

One of the main responsibilities we have is that we process and hold your personal data securely. The GDPR and DPA 2018 state that special personal data requires more protection and additional conditions for processing. We will process any special personal information only for the purposes for which you provide it, unless permitted by law.

The Council will always treat any data breach as a serious issue, and all potential breaches will be thoroughly investigated.

Your Rights

The GDPR and DPA 2018 provide you with the following rights:

- The right to be informed: You have the right to be informed about the collection and use of your personal data, and this is outlined in this privacy notice.
- The right of access: You have the right to request access to the personal data we may hold about you. This is undertaken using a Subject Access Request.
- The right to rectification: You have the right to request that inaccurate personal data we hold is rectified.
- The right to erasure: In certain circumstances, you have 'the right to be forgotten' and have your personal data erased.
- The right to restrict processing: In certain circumstances, you have the right to request the restriction or suppression of your personal data.
- The right to data portability: In certain circumstances, you have the right to request to obtain your own personal data for your own use or to give to other organisations.
- The right to object: In certain circumstances, you have the right to object to your personal data being collated, stored and processed.
- Rights in relation to automated decision making and profiling: You have the right to request that we do not make our decisions based on solely an automated process, and you can object to an automated decision and ask that a person reviews it in certain circumstances.
- The right to withdraw consent: In our discretionary service provisions, you have the right to withdraw your consent at any time.
- The right to complain: You have the right to complain through our complaints procedure, and then to the Information Commissioner.

Any requests in relation to your rights with regard 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 ICO 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:

- Directly from you;
- From a third party;
- From publicly available sources;
- From other organisations or agencies.

We will only collect your personal information in line with the relevant regulations and the law, and this may relate to any of our statutory or discretionary services you apply for, currently hold or have held in the past.

We will obtain personal information through a number of different mediums such as telephone, email, in person, post, or online. At the point of data collection, the lawful basis for processing will be determined and explained.

Due to the diverse statutory and discretionary services we provide, further privacy notices are available at the point of data collection.

In order to operate efficiently, ESC have to collect and use information about people with whom it works, including: members of the public, service users, current, past and prospective employees, clients, customers, contractors, suppliers, and partner organisations. In addition, the Council may be required by law to collect and use information in order to comply with the requirements of central government. Personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means.

To fulfil our statutory obligations, we will have to collate and process your personal data. Where we are providing discretionary services, or we are entering into a contract with you, if you choose not to give us your personal data it may delay or prevent us from fulfilling this role.

Cookies

Cookies are small computer files sent to your PC, tablet, or mobile phone by websites when you use them. They stay on your device and get sent back to the website they came from, when you go there again. Cookies store information about your visit to that website.

CCTV

Overt CCTV monitoring must be carried out in accordance with the ICO's code of practice on CCTV. Any covert surveillance activities of the law enforcement community are governed by the Regulation of Investigatory Powers Act (RIPA) 2000.

What information do we maintain?

The Council may need to use some information about you, for example:

- to maintain our accounts and records
- to manage our property and housing
- to provide leisure and cultural services
- to carry out surveys
- to collect taxes and pay benefits
- licensing and other regulatory activities
- protecting public money by taking part in local, regional and national fraud initiatives
- crime prevention including the use of CCTV
- to provide services to our residents and visitors
- to support and manage our employees
- to manage archived records for historical and research purposes.

Due to the diverse statutory and discretionary services we provide, further privacy notices are available at the point of data collection which explain the information we hold.

How do we use your information?

We require your personal information for a number of statutory and discretionary obligations and we will not use your personal data for purposes other than for what it was collated unless we have obtained your consent, or for other lawful purposes (e.g. the detection and prevention of fraud).

Automated Decision Making

We sometimes use systems to make automated decisions about you. 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.

Marketing

We may use marketing to let you know about products, services and offers that you may want from us. You will be given the option to opt in to marketing at the point of data collection.

How long do we keep your information?

We will hold your personal information in accordance with statutory responsibilities and contractual requirements. If you have supplied personal information for a discretionary service the period of time the data will be held will be detailed within the privacy notice at the point of data collection. Once your information is no longer needed, it will be securely and confidentially destroyed.

Why we share data and who we share it with

We use a number of commercial companies and partners to either store personal information or to manage it on our behalf. Where we have these arrangements there is always a contract, memorandum of understanding or information sharing protocol in place to ensure that the organisations comply with data protection law.

Organisations that we may share your information with include: Councillors, MPs, The Cabinet Office, the Department for Work and Pensions, other local councils, Her Majesty's Revenues and Customs, the Police, the Fire Service, the Ambulance Service, Health and Social Care providers and agencies, the Housing Ombudsman, credit reference agencies, service providers and contractors and partner agencies/bodies.

We may also share your personal information when we feel there is a good reason that is more important than protecting your confidentiality. This does not happen often, but we may share your information:

- for the detection and prevention of crime/fraudulent activity; or
- if there are serious risks to the public, our staff or to other professionals; or
- to protect a child; or
- to protect vulnerable adults who are thought to be at risk.

When using personal data for research purposes, the data will be anonymised to avoid the identification of an individual, unless consent has been given for the use of the personal data in this way.

We do not sell personal information to any other organisations for the purposes of direct marketing.

Transferring your information overseas

The Council may transfer your personal information outside of the European Economic Area (EEA) only where there are adequate safeguards in place. Please refer to individual team privacy notices which detail if your personal information will be transferred.

National Fraud Initiative (NFI)

We are required by law to protect the public funds we administer. 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. The Cabinet Office is responsible for carrying out data matching exercises. 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. We participate in the Cabinet Office's National Fraud Initiative, a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise, as detailed here. 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 GDPR and DPA 2018. Data matching by the Cabinet Office is subject to a Code of Practice. Further information on the Cabinet Office's legal powers and the reasons why it matches particular information.
Data Protection Officer	The Data Protection Officer for ESC is Siobhan Martin, Head of Internal Audit, and can be contacted at dataprotection@eastsuffolk.gov.uk or 01394 444488.