Information Charter

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 provide individuals with numerous rights including the Right to be Informed. This Information Charter[1] sets out the standards you can expect from Essex Police when we obtain, hold, retain, process and disclose information, including but not limited to personal data[2] about you or your enquiries with the Force. The Force holds both personal and non-personal information in a variety of databases and information stores which are critical to its lawful functions, together with systems relating to Force support functions.

This Charter also describes your statutory rights in regard to information under the provisions of the General Data Protection Regulation (GDPR) and Data Protection Act 2018, Freedom of Information Act 2000 and Environmental Information Regulations 2004.

The Freedom of Information Act 2000 (FOIA 2000) was introduced to give the public greater access to information in relation to the workings of government and public bodies, in order to ensure transparency and greater accountability. The FOIA 2000 provides access to information held by public authorities and entitles individuals to request information from public authorities. Essex Police is a "public authority" under the FOIA 2000 and the Freedom of Information (Scotland) Act 2002. For further information on how the Force manages information under the FOIA 2000, please visit the Freedom of Information pages on our website.

The use and disclosure of personal data is governed in the United Kingdom by the GDPR and Data Protection Act 2018. The Chief Constable of Essex Police is the Controller and he has an obligation to ensure that Essex Police handles all personal data in accordance with the legislation.

Essex Police takes that responsibility very seriously and takes great care to ensure that personal data is handled appropriately in order to secure and maintain individuals' trust and confidence in the force.

Standards

- Information is handled in accordance with the GDPR and the Data Protection Act 2018 which set out the Data Protection principles of good information handling practice governing the fair and lawful processing, maintenance and security of the data.

[1] This document is designed to help satisfy the 'Fair Processing' requirements of the General Data Protection Regulation and Data Protection Act 2018. Additional Fair Processing Notices may be included on other such items including but not limited to forms, force policies, email footers and CCTV signage.

[2] 'Personal Data' is defined under Article 4(1) of the General Data Protection Regulation and Part 1 Section 3(2) of the Data Protection Act 2018. In practical terms it means information handled by Sufolk Force that relates to identifiable living individuals. It can include intentions and expressions of opinion about an individual. The information can be held electronically or as part of a paper record and can include CCTV images and photographs. The legislation uses the term 'processing' to effectively cover any usage of personal data.

- We will take care to ensure information is:

- Only collected and used by the Force to carry out its legal and legitimate functions as defined by legislation, common law and best practice; in accordance with the Policing and Supported Policing Purposes which include:

  Policing Functions:

  - Preventing / Detecting Crime
  - Apprehending/ Prosecuting Offenders
  - Protecting Life and Property
  - Preserving Order
  - Maintaining Law and Order
  - Providing Assistance to the Public in accordance with force policies and procedures; and
  - Any duty or responsibility of the police arising from common or statute law

  Support Functions:

  - Staff/ Pensioner Administration, Occupational Health and Welfare
  - Public Relations/ Media
  - Finance/ Payroll/ Benefits/ Accounts/ Audits/ Internal Review
  - Training/ Health & Safety Management
  - Property/ Insurance/ Vehicle/ Systems and Transport Management
  - Complaints
  - Vetting
  - Legal Services/ Information Provision
  - Management of information technology systems
  - Licensing/ Registration
  - Research[3] (including surveys and analytics)/ Performance Management
  - Sports/ Recreation
  - Procurement
  - Planning/ Testing/ Security
  - Health and Safety Management
  - Strategy and Policy development
  - Social Media Correspondence and analysis

- Accurate, kept up-to-date and destroyed when no longer required

- Adequate, relevant and not excessive – we will only ask for what we need

- Adequately protected through a variety of physical, technological and procedural measures to maintain and safeguard the confidentiality, integrity and availability of the information by preventing unauthorised access and unauthorised/ accidental disclosure, loss or corruption.

[3] Essex Police is required to conduct Customer Satisfaction Surveys to evaluate our performance and effectiveness. We may contact individuals, such as victims of crime of those reporting incidents, and ask them to give us their opinion of the service we are providing to the public. We use the information given to improve our service wherever we can. Essex Police like many police forces uses a private company to undertake such surveys on our behalf with strict controls to protect the personal data of those involved.

- Essex Police will only use appropriate personal data necessary to fulfil a particular purpose or purposes. Personal data could be information which is held on a computer, in a paper record i.e. a file, as images, but it can also include other types of electronically held information i.e. CCTV images.

  We process the following types/classes of information:

  - personal details
  - physical identifiers including facial images, voice recordings
  - family details
  - lifestyle and social circumstances
  - goods and services provided
  - financial details
  - employment and education details
  - intelligence material
  - sound and visual images
  - licenses or permits held
  - complaints
  - references to manual records or files
  - information relating to health and safety

  We also Special Category information that may include:

  - physical or mental health details
  - racial or ethnic origin
  - trade union membership
  - political opinions
  - religious or other beliefs
  - sexual life and sexual orientation
  - DNA, fingerprints and other genetic or biometric samples

  We also process information relating to criminal conviction and offence data including:

  - offences and alleged offences
  - criminal proceedings, outcomes and sentences
  - criminal intelligence

- Where possible and/or appropriate you will be informed of the reason for collecting, holding and using your personal information. Although, in view of the statutory functions of the Force, this may not always be possible as doing so may prejudice the Policing functions (as detailed above).

  We process personal information about:

  - offenders and suspected offenders
  - victims
  - witnesses
  - persons given a caution or a warning
  - consultants and other professional experts

- persons subject to judicial and other disposals including convictions, bind-overs, discharges, acquittals, orders made under legislation
- suspect offenders under the age of 10
- staff, former staff and potential staff including volunteers, agent, temporary and casual workers
- complainants and enquirers
- relatives, guardians and associates of the people we are processing personal
- information about
- advisers, consultants and other professional experts
- pensioners and beneficiaries
- other individuals necessarily identified in the course of police enquiries or activities
- suppliers
- patients
- individuals coming to the attention of the data controller as a result of any criminal
- activity considered to be a risk to national security

- We sometimes need to share information with the individuals we process information about and other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection legislation. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

  Where necessary or required we share information with:

  - other police forces
  - family and associates of the individuals we process information about
  - regulatory bodies
  - courts
  - prisons
  - non home office police forces
  - customs and excise
  - local and central government
  - security companies
  - partner agencies, approved organisations and individuals working with the police
  - licensing authorities
  - service providers
  - press and the media
  - healthcare professionals
  - current, past and prospective employers
  - examining bodies
  - law enforcement and prosecuting authorities
  - legal representatives
  - defence solicitors
  - independent police complaints authority
  - the disclosure and barring service
  - partner agencies involved in crime and disorder strategies, and public protection

- private sector organisations working with police in anti-crime strategies
- voluntary sector organisations
- approved organisations working with the police
- offices of the Police and Crime Commissioner
- emergency services
- business associates and professional advisers
- persons making an enquiry or complaint
- ombudsman and regulatory authorities
- data processors
- educators and examining bodies
- financial organisations
- credit reference agencies
- survey and research organisations
- trade and employer associations and professional bodies
- Crown Prosecution Service
- HM Courts Service
- international agencies concerned with the safeguarding of international and domestic
- national security anywhere in the world
- third parties involved in investigations relating to the safeguarding of national security

- Where possible, you will be informed if we intend to use or share your information for a non-obvious purpose, either directly, via the Force website or other means of communication.

- We will work with partner agencies and may share your information with them. All attempts to anonymise the personal information will be considered in the first instance and only personal information will be shared if there is a legal basis in which to do so and after having fully considered your rights to privacy.

- We will actively manage our Information Assets in conjunction with Information Asset Owners who will manage and monitor the information through its lifecycle.

- Essex Police keeps personal data for as long as is necessary for the purpose for which it was collected and recorded. Records containing personal data relating to matters of intelligence, public protection, violent and sexual offenders, missing persons, case and custody, crime and incident, firearms, child abuse investigations and domestic abuse will be retained in accordance with the College of Policing Authorised Professional Practice (APP) on the Management of Police Information. Other records are held in accordance with our Review, Retention and Disposal Schedules.

- We may use your personal information to analyse our performance and effectiveness. In some cases it may be necessary to contact you and ask you to assist us in the analysis in order to gather information about the services we provide.

- Information Management policies and procedures are implemented and continually reviewed to ensure continual improvements in the way in which information is handled by reflecting any changes in legislation and developments in case law as necessary.

- All staff and contractors are suitably vetted and trained in the appropriate policies and procedures for ensuring the correct handling of personal information. Staff receive training at the start of employment and refresher training as deemed necessary.

- We will proactively monitor the legitimate use and quality of information through audits and transaction monitoring. Any breaches are taken seriously and disciplinary/ criminal investigations are undertaken as necessary. The Force will not tolerate any misuse of information.

- Essex Police takes the security of all personal data under our control very seriously. We will comply with the relevant parts of the GDPR and Data Protection Act 2018 relating to security and seek to comply with the National Police Chief's Council (NPCC) Community Security Policy. We use a variety of physical, technical and procedural measures to protect personal information from unauthorised or accidental disclosure, loss or corruption.

- Essex Police may monitor or record and retain telephone calls, texts, emails and other electronic communications to and from the force in order to deter, prevent and detect inappropriate or criminal activity, to ensure security, and to assist the purposes the purposes described above. The Force does not place a pre-recorded 'Fair Processing Notice' on telephone lines that may receive emergency call (including misdirected ones) because of the associated risk of harm that may be caused through the delay in response to the call.

- We will ensure statutory rights to information under the provisions of the GDPR and Data Protection Act 2018; Freedom of Information Act 2000 and Environmental Information Regulations 2004 are addressed. Should you find any of the information we hold about you is incorrect or misleading, we will ensure it is thoroughly assessed and corrected where appropriate.

- Individuals have a number of rights enshrined in the Data Protection legislation:

    - **Right to be Informed**
      This is provided for in Articles 13 and 14 of GDPR and Section 44 of the Data Protection Act 2018 which sets out the general duties of a Controller. This Information Charter addresses that requirement.

    - **Right of Access**
      Individuals have the right to apply for a copy of their personal data held by Essex Police. This right, commonly referred to as Subject Access is created by Article 15 of GDPR and Section 45 of the Data Protection Act 2018 and is used by individuals who want to see a copy of the information an organisation holds about them (subject to exemptions).

      Details of the application process can be found here.

    - **Right to Rectification**
      Article 16 of GDPR and Section 46 of the Data Protection Act 2018 provides individuals with the right to have inaccurate personal data rectified or completed if

it is incomplete. This may involve the Force providing a supplementary statement to the incomplete data.

- **Right to Erasure**
  Article 17 of GDPR and Section 47 of the Data Protection Act 2018 provides individuals with the right to have personal data erased. This is known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- **Right to Restrict Processing**
  Article 18 of GDPR and Section 47 of the Data Protection Act 2018 provides individuals with the right to restrict processing of their personal data in certain circumstances. This means that an individual can limit the way an organisation uses their data.

- **Right to Data Portability**
  Article 20 of GDPR provides individuals with the right to receive personal data they have provided to a Controller in a structured, commonly used and machine readable format. It also gives them the right to ask a Controller to transmit this data directly to another Controller.

- **Right to Object**
  Article 21 of GDPR provides individuals with the right to object to:
  - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority;
  - direct marketing; and
  - processing for purposes for scientific/historical research and statistics.

- **Rights related to automated decision making including profiling**
  Article 22 of GDPR and Sections 49/50 of the Data Protection Act 2018 makes provision to protect individuals from processing carried out solely by automated decision making that has legal or similarly significant effects on them.

- Generally, if individuals have any concerns regarding the way their personal data is handled by Essex Police or the quality (accuracy, relevance, non-excessiveness etc.) of their personal data, they are encouraged to raise them with the Force's Data Protection Officer, Adam Hunt, using the contact details provided below:

  Data Protection Officer
  Information Management Team
  Essex Police Headquarters
  PO Box 2
  Chelmsford
  CM2 6DA

  Email: dpo@essex.pnn.police.uk

  Telephone: 101

- The Information Commissioner is the independent regulator responsible for enforcing the legislation and provides advice and guidance about the requirements. The Information Commissioner's Office (ICO) can be contacted via the following:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) / 01625 545 745 (national rate)

Website: www.ico.org.uk