Police, Fire and Crime Commissioner for Essex

Data Protection Policy

Version Control	Version 2.0	January 2022
Reviewed By	S Humphreys (DPO)	January 2022
Policy owner	D Horsman (SIRO)	January 2022
First Published		December 2019
Next Review Date	S Humphreys	January 2024

Version history

Version Number	Date	Reason for review	Comments
1.0	December 2019		First publication
2.0	January 2022	Scheduled review	

Police, Fire and Crime Commissioner for Essex
Data Protection Policy
January 2022

Contents

1.0 Introduction

The Data Protection Act 2018 regulates the processing of information relating to individuals. This includes the obtaining, holding, using or disclosing of such information and covers computerised records as well as manual filing systems and card indexes.

The UK General Data Protection Regulation (UK GDPR) was applied from 01 January 2021 and replaced the General Data Protection Regulation which had been in force since 2018. The UK GDPR places significant emphasis on the documentation that data controllers must keep to demonstrate their accountability. This Regulation is inherent in the requirements of the Data Protection Act 2018.

The UK GDPR states that anyone who processes personal information must comply with principles of the Data Protection Act:

Principle 1: Lawfulness, Fairness and Transparency
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that the PFCC must tell the Data Subject what processing will occur (transparency); the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the PFCC must specify exactly what personal data is collected and for what it will be used.

Principle 3: Data Minimisation
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the PFCC must not store any personal data beyond what is strictly required.

Principle 4: Accuracy
Personal data shall be accurate and kept up to date. This means the PFCC must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation
Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the PFCC must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The PFCC must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability
The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means the PFCC must demonstrate that the six Data Protection

Principles (outlined above) are met for all personal data for which they are responsible.

The PFCC for Essex is a registered Data Controller (registration no. Z3451171). The PFCC, in providing a service as a public authority, collects, stores and processes personal information. The PFCC must comply with the provisions of the Data Protection Act, UK GDPR and other relevant legislation when processing personal information. This policy has also been informed by the results of an internal audit looking at UK GDPR regulation compliance within the PFCC's office, learning from the implementation of the first version of this policy developed in 2018 and expert training and development undertake by the Data Protection Officer and Senior Information Risk Owner.

Security

All data controllers have a responsibility to make sure they protect personal data and keep it secure. We will take action to make sure we do not process information unlawfully and to stop data being accidentally lost or destroyed. This policy outlines the general approach of the Police, Fire and Crime Commissioner (PFCC) for Essex in the processing of personal information for the purposes of carrying out his/her statutory role and seeks to:

- Ensure that the PFCC and all staff who process or use personal data abide by the principles set out above at all times, including by protecting the integrity, availability and confidentiality of data held by the PFCC, and
- Minimise the potential consequences of information security breaches by, wherever possible, preventing their occurrence in the first instance and, where necessary, containing and reducing their impact.

All PFCC employees and volunteers, as well as those contracted to provide services on the PFCC's behalf, are obliged to comply with this policy when processing personal data.

The UK GDPR and the DPA 2018 (together referred to as the data protection legislation) contain statutorily defined terms including:

- Personally identifiable information or personal data – personal data is any information that allows a natural living person to be identified
- Data Subjects – include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident.
- Data controller – the public authority which singularly or jointly sets the purpose and means for the processing of personal data. The PFCC should be considered the data controller for the personal data collected for the discharging of his/her statutory duties
- Data processor – those that process personal data on behalf of the data controller
- Processing – in relation to information or data can mean (by automation or manual activity) obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. This includes manipulation of data in some way, such as organising and retrieving of data; adaption, alteration or modification of the data; use of the information or data; transmitting the data and making the data available; and destroying,

blocking or erasing data. The processing of data must comply with a number of rules which are captured within the data protection principles. Essentially:
    - Processing of personal data must be lawful and fair;
    - The security and confidentiality of personal data should be ensured;
    - The purposes of processing should be explicit and legitimate;
    - Personal data must be relevant, adequate and limited to what is necessary in relation to the purposes for which data is processed
    - Reasonable steps should be taken to ensure that data is accurate and up to date
    - Data should not be stored for any longer than is necessary
    - It should be clear and easy for people to understand that their personal data is being processed and what this entails and will be used for
    - Clarity should be provided to data subjects about what their data may be used for and any risks or relevant obligations in line with this.
- Special Category Data (also known as 'sensitive personal data') includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or Trade Union membership. The definition also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.
- Data Protection Impact Assessment – a process to help identify and minimise the data protection risks of a project or activity. A DPIA should be carried out for processing that is likely to result in a high risk to individuals' privacy. The DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any measures to mitigate those risks.

It is likely, across the delivery of his/her statutory functions, that there will be circumstances where the PFCC will be the data controller and data processor.

The contact details (postal address, telephone number and / or email address) of the Data Protection Officer will be provided on the PFCC's website for ease of reference for the public and other stakeholders. All initial enquiries should be directed to the Data Protection Officer via: pfcc@essex.police.uk

For completeness this policy should be read in conjunction with the following policies:

- Access to Information Policy
- Records Retention and Disposal Policy
- The PFCC's General Privacy Notice: https://www.essex.pfcc.police.uk/contact-us/privacy-notice/

2.0 Scope

This policy applies to the PFCC, the Deputy PFCC, and all staff including agency workers, secondees, volunteers and consultants engaged to work with the PFCC.

It covers all information held by the PFCC and / or by staff of the PFCC and others who are engaged to work for it. For the purposes of this policy, "information" is

defined as any information, data or records, irrespective of format, generated or used by the PFCC and its staff in the carrying out of its functions. Examples include electronic communication (including emails), video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.

3.0 Responsibilities and Individuals' rights under the UK General Data Protection Regulation (UK GDPR)

The PFCC is the Data Controller under UK GDPR and must implement appropriate technical and organisational measures (including this policy) to ensure, and be able to demonstrate, that the processing of personal data complies with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation. The PFCC, through their staff, is responsible for ensuring that any personal data supplied is accurate and up to date. To ensure adherence to the data protection principles set out above, the PFCC will, through this and other policies, correspondence with data subjects (where appropriate) and via their website, make the following information available to the public:

- The identity and contact details of the Controller;
- The contact details of the Data Protection Officer;
- The purposes for which the Controller processes personal data;
- The rights of data subjects to request access to, rectification or erasure of personal data or the restriction of its processing, and
- The existence of the right to lodge a complaint with the Information Commissioner and the contact details of the Commissioner.

The Chief Executive has delegated authority to carry out all functions and responsibilities of the Data Controller, although liability remains with the PFCC as a corporation sole.

The PFCC may use a Processor to carry out the processing of personal data on their behalf or may also be a Processor of information for other organisations. Further information regarding such arrangements is set out in section 5.

Data Protection Officer

The Data Protection Officer's (DPO's) duties include:

- Maintaining and communicating to the organisation current and comprehensive knowledge of data protection legislation;
- Being aware of the PFCC's current compliance status;
- Identifying and monitoring risk areas and recommending solutions to these to the PFCC and their Senior Management Team (SMT);
- Creating, maintaining, guiding and training staff relating to data protection policies, Information Sharing Agreements and Protocols to safeguard information and data that is shared with third parties;
- Providing advice, as required, on the carrying out of data protection impact assessments, and
- Co-operating and consulting with the Information Commissioner as required, including acting as the contact point for the Commissioner on issues relating to data processing.

Working with the Essex Police ICT service, the Data Protection Officer is also required to:

- Provide clear and effective procedures and guidance to staff on data protection and information security issues and ensure these are complied with, and
- Implement systems, both manual and electronic, to ensure that information and data are held as securely as possible.
- Overseeing all subject access requests

The PFCC and all staff are responsible for ensuring that the Data Protection Officer is involved properly and in a timely manner in all issues which relate to the protection of personal data. She / he should be included in any relevant working groups dealing with data processing activities within the organisation and will be invited to participate regularly in meetings of the PFCC's Senior Management Team (SMT) where decisions with data protection implications are to be taken. On such occasions, all relevant information is to be passed by the lead officer to the DPO in a timely manner in order to allow the DPO to provide adequate advice, and the advice of the DPO must be given due consideration by the decision maker.

Senior Information Risk Owner

The PFCC has appointed a Senior Information Risk Owner (SIRO) who is responsible for ensuring data assets and risks are managed as a process within the organisation and that the Senior management Team and PFCC recognises the importance of data protection in delivering corporate objectives. The SIRO is also the focal point for information risk management including resolution of any escalated risk issues raised by the DPO. On occasion the SIRO will also seek input from others (internally and externally) to highlight contemporary information risks and threats which may prevent corporate objectives from being achieved.

Importantly the SIRO also owns the organisation's overall information management policy and risks and ensure they are implemented / mitigated consistently.

The SIRO's key responsibilities include:

- ensuring that the data protection legislation and policy is applied and maintained consistently throughout the organisation
- owning and reviewing information-based risks
- ensuring that Data Protection Impact Assessments are carried out on all new projects when required
- understanding the information risks faced by the organisation, its partners and commissioned services ensuring that they are addressed, and that they inform strategic priorities ensuring that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny.

All staff

Compliance with data protection legislation is the responsibility of everybody who processes personal information in the PFCC. As such, all staff are required to familiarise themselves and comply with this policy, for example by ensuring that the records they keep are up to date and accurate; that any personal data they hold, whether in electronic or paper format, and the devices on which they are stored (e.g.

laptops, mobile telephones) are kept securely, and that personal data is not disclosed deliberately or accidentally, either orally or in writing, to any unauthorised third party.

All PFCC staff must also notify the Data Protection Officer of any filing system or computer database in their use that contains (or will contain) personal data (e.g., name and address) in order to ensure its inclusion on the PFCC's data asset register.

The PFCC uses the Government Security Classifications in order to ensure that data and information assets are adequately protected. The classifications apply to all information that PFCC collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners. Responsibility is placed upon the individual to handle the data contained within a document according to its sensitivity and any protective marking.

Line managers

Line managers must ensure that, as part of the induction process, new starters familiarise themselves with this Data Protection Policy, the Government Security Classifications and with associated policies and procedures and complete any data protection and information security training relevant to their role. On termination or suspension of employment or contracts, managers are responsible for making arrangements to ensure that access to computer systems and buildings is ceased in order to ensure the protection of data and information.

Any breach of this Data Protection Policy, whether deliberately or through negligence, may lead to disciplinary action being taken and, in certain circumstances, even criminal prosecution.

Subject's rights

Individuals have a number of rights under UK GDPR, including the right to:

- ask the PFCC if it holds personal information about them;
- ask what it is used for;
- be given a copy of the information (subject to certain exemptions);
- be given details about the purposes for which the PFCC uses the information and of other organisations or persons to whom it is disclosed;
- ask for incorrect data to be corrected;
- be given a copy of the information with any unintelligible terms explained;
- be given an explanation as to how any automated decisions taken about them have been made;
- ask that information about them is erased ("right to be forgotten");
- ask the PFCC not to use personal information:
    - for direct marketing, or
    - to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

The manner in which the PFCC will respond to the exercise of these rights is set out in its Access to Information Policy. These rights are not absolute. If the PFCC is unable to respond to a request, it will outline the legal reasons for its decision clearly.

Note the Freedom of Information Act is independent legislation, it is not under Data Protection law and is covered separately in the PFCC Access to Information policy.

4.0 Data Security

Information and data are vital assets to the organisation. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss or destruction of, or damage to, personal data. We will put in place procedures and technologies (though the provision of Essex Police ICT systems and support) to maintain the security of all personal data from the point of collection to the point of destruction.

Personal data will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the data protection legislation and ensure that data subjects' rights are protected and that these requirements are governed by a contract or other legally binding agreement (please see section 5).

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
(a) Confidentiality - means that only people who are authorised to use the personal data should access it;
(b) Integrity - means that personal data should be accurate and suitable for the purpose for which it is processed;
(c) Availability - means that authorised users should be able to access the personal data if they need it for authorised purposes.

Security procedures include:
(a) Entry controls. The office of the PFCC is PAC entry controlled, with only authorised persons allowed entry. Visitors will be accompanied at all times. Any stranger seen in close proximity to entry-controlled areas will be challenged, their reasons for presence checked and if necessary, reported to a senior manager;
(b) Secure, lockable desk drawers and cupboards. Desk drawers and cupboards will be kept locked if they hold confidential information of any kind. Personal information is always considered confidential;
(c) Methods of disposal. Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required;
(d) Equipment. PFCC employees will ensure that individual monitors are not visible from outside their workstation and that they log off from their PC when it is left unattended;
(e) IT security. IT provision is provided for the PFCC by the Essex Police/Kent Police Joint ICT Department. A condition of use is compliance with the security policies of Essex Police.

Training for staff includes:
(a) Mandatory training for all staff on Data Protection, including e-learning in conjunction with Essex Police and through regular team updates and sessions;
(b) Training for specialist Data Protection staff, including those who handle Subject Access Requests;
(c) Training for new starters as part of the corporate induction process.

Governance and assurance procedures include:
(a) Internal and external audits of the PFCC's data protection processes and procedures;
(b) For complex and sensitive data collection processes where the type of processing is likely to result in a high risk to the rights and freedoms of individuals, the PFCC will ensure that a Data Protection Impact Assessment is conducted. This should be carried out in conjunction with the Data Protection Officer.
The DPIA must include the following:

- A general description of the envisaged processing operations;
- An assessment of the risks to the rights and freedoms of data subjects;
- The measures to be put in place to address those risks, and
- Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act 2018, taking into account the rights and legitimate interest of data subjects and other stakeholders.

5.0 Use of Data Processors

The PFCC, as the Data Controller, may use a Data Processor to carry out the processing of personal data on its behalf. However, the PFCC may only use a processor who provides guarantees to implement appropriate technical and organisational measures to ensure that the processing meets the requirements of the Data Protection Act 2018 and ensures the protection of the rights of data subjects.

Any processor used by the PFCC may not engage another processor ("a sub-processor") without the prior written authorisation of the PFCC. Where the PFCC provides a general written authorisation to a processor, the processor must inform the PFCC if they propose to add further or replace any sub-processors and give the PFCC the opportunity to object to the proposal.

Processing on behalf of the PFCC by a processor must be governed by a contract in writing between the two parties setting out:

- The subject matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subjects involved, and
- The obligations and rights of the controller and processor.

The contract must require the processor to:

- Act only on instructions from the controller (including that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to do so);
- Ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality;
- Assist the controller to ensure compliance with the rights of data subjects;
- At the end of the provision of services by the processor to the controller, either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and to delete copies of the personal data unless subject to a legal obligation to store them;
- Make available to the controller all information necessary to demonstrate compliance with the above, and
- Comply with the requirements of this section for engaging sub-processors.

6.0 The PFCC and Essex Police

The Police Reform and Social Responsibility Act 2011 created the role of Police and Crime Commissioner (PCC) for each of the police forces in England and Wales and set out the functions that the PCC must discharge. In order for the PFCC to discharge those functions there is a requirement for some information in the possession of Essex Police to be shared with the PFCC. A reciprocal sharing of some information from the PFCC to Essex Police may also be required to assist in the discharge of the PFCC's functions

Whilst the PFCC and the Chief Constable for Essex Police are separate entities / sole corporations, there is a close daily working relationship that is mutually beneficial to the delivery of effective and efficient policing in Essex. In a number of areas the PFCC and Chief Constable will share back office support, for example, in areas such as vetting, HR, IT and associated systems and payroll. In this instance the personal data under the control of the PFCC will be processed by the Chief Constable. There will also be circumstances, for example in the handling of police complaints, where the PFCC will receive personal data from the Chief Constable where the Chief Constable is the controller, in order for both parties to discharge their statutory duties. There is a current Information Sharing Agreement between the PFCC and the Chief Constable of Essex Police which details the regulation of this agreement: (pfcc.police.uk)https://www.essex.pfcc.police.uk/finance-reporting/publications/

7.0 PFCC and Essex County Fire and Rescue Service (ECFRS)

The Policing and Crime Act 2017 obligated 'Blue Light Services' to collaborate more effectively. Following public consultation, the submission of a business case and approval by the Home Office, the PCC for Essex took on joint governance of the Essex County Fire & Rescue Service in October 2017, becoming the Essex Police, Fire & Crime Commissioner, Fire & Rescue Authority (PFCCFRA).

Details of the PFCCFRA, ECFRS privacy policy and details of how to contact their DPO can be found here https://join.essex-fire.gov.uk/privacy-policy/

There is a current Information Management Protocol between the PFCC and the fire and rescue service which details the regulation of information sharing between them. This is appended as Schedule 5 to the PFCCFRA Constitution, available here:

https://www.essex.pfcc.police.uk/wp-content/uploads/2021/07/FINAL-PFCCFRA-Constitution-March-2020.pdf

8.0 PFCC and The Police, Fire and Crime Panel

The Essex Police, Fire and Crime Panel (PFCP) scrutinises the decisions of the PFCC in their capacity as both the Police and Crime Commissioner and the Police, Fire and Crime Commissioner Fire and Rescue Authority.

For the PFCP to discharge this function there is a requirement for some information in the possession of the PFCC to be shared with the PFCP. A reciprocal sharing of some information from the PFCP to the PFCC may also be required to assist in the discharge of the PFCC's functions.

There are current Information Sharing Agreements between the PFCC and the PFCCFRA and the Essex Police, Fire and Crime Panel which details the regulation of this agreement:

https://www.essex.pfcc.police.uk/wp-content/uploads/2021/07/FINAL-PFCCFRA-Constitution-March-2020.pdf

9.0 Data

The data that the PFCC collects and holds is, compared with other public bodies, relatively small and is used to discharge the statutory functions of the Commissioner. There are a number of examples of this including:

- Appointments to paid roles
- Appointments to volunteer roles (Restorative Justice, Police Dog Welfare, Independent Custody Visiting)
- Applications for appointments
- Correspondence with the PFCC
- Complaints against the Chief Constable, PFCC, DPFCC, paid employees or volunteers including Rights to Review and Appeals
- Contacts that work with the PFCC to deliver governance, information, public meetings, business meetings or board meetings, surveys and consultations
- Police Appeals Tribunals
- Information provided by the Chief Constable and / or Chief Fire Officer relevant to the discharge of the PFCC's statutory duties
- Information that may be shared between the relevant Media departments

This information is stored on a secured IT platform and email service provided by Essex Police. Hard copies, where relevant, are stored in a lockable location and the entry to the office of the Police, Fire and Crime Commissioner is limited to those who have adequate security clearance, with all visitors being accompanied during their visit.

10.0 Documenting the Personal Data we hold and the Processing Activities we undertake

Data owners and the type of data owned by the PFCC are recorded on a dedicated data asset register. This register allows the PFCC to identify the type and purpose of data in both a controller and processor capacity. Information on where the data has come from, our legitimacy / purpose for requesting or processing it, the basis and consent for collection, whom it may be shared with, security of data, identification of storage and length of retention are documented.

It is the responsibility of each data owner to update this information regularly – this is essential should we need to access the data for any purpose. The Data Asset Register is frequently audited and monitored by the Data Protection Officer (DPO)

This is linked and regulated in conjunction with our Records Retention and Disposal Policy.

The links provided below illustrate the determination of what data is and what personal and sensitive data is:

https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf

11.0 Privacy information

When collecting personal data, to meet our UKGDPR and DPA responsibilities, we are required to give people certain information such as our identity and how we intend to use their information – this is done through a privacy notice. UK GDPR requires us to explain our lawful basis for processing this data, how long we are going to hold it for and that individuals have the right to complain to the ICO, or a Court of Law, if they feel we are not handling their data correctly.

The Information Commissioners Office (ICO) provides further guidance:

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

The PFCCs privacy notice can be found here, on the home page of our website: http://www.essex.pfcc.police.uk/contact-us/privacy-notice/

Where consent is required from an individual in order to process their information the PFCC will explain to the individual what is being asked of them and why. Consent is likely to be required when a correspondent is raising an issue with the PFCC that requires information or a response from Essex Police, the Essex County Fire and Rescue Service or a third party. In instances such as this, refusal to give consent may impact on the response that the PFCC is able to facilitate or provide.

The Restorative Justice Team also works from within the PFCC's office and as such has an established suite of privacy notice detail and UK GDPR compliant processes across the team and the dedicated ICT system that is utilised in this practice. The Restorative Justice Privacy Notice can be found here: https://restorativeessex.co.uk/privacy-policy/

12.0 Lawful basis for processing personal data

We will identify the lawful basis for processing activity of data, document it and update our privacy notice to explain it. This lawful basis should be documented on the PFCC's Data Asset Register.

It should be emphasised that the lawful basis needs to be carefully considered as this has an impact with regard to the rights of individuals. For example, in some cases individuals may have a stronger right to have their data being deleted where consent is used as the lawful basis for processing.

13.0 Data and Information Security Breaches

Any breach of security relating to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed constitutes an information security breach. Such breaches can take the form of personal data breaches, IT security incidents or the compromising of physical security assets.

Examples of personal data breaches include:

- Access to personal data by an unauthorised third party;
- Sending personal data to an incorrect recipient (for example in emails);
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission, or
- Loss of availability of personal data.

Examples of IT security incidents include:

- Attempts by unauthorised sources to access systems or data;
- Unauthorised processing or storage of data, or
- Unauthorised changes to system hardware or software.

Examples of physical security asset breaches include:

- Shared passwords;
- Loss of organisation owned assets such as mobile telephones and laptops;
- Loss of PAC tags, or
- Inappropriate or unauthorised access rights.

Any suspected data breach (whether by the Data Controller or any Data Processor acting on behalf of the Data Controller) shall be notified to the Data Protection Officer without delay for consideration of action. The DPO will undertake to identify whether a data breach or “near miss” has occurred.

In case of a personal data breach, as data controller we shall – unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual(s) - without undue delay, and not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner’s Office.

The Data Protection Officer must record the following information in relation to any personal data breach:

- The facts relating to the breach;
- Its effects, and
- Any remedial action taken

When the personal data breach is likely to result in a high risk to the rights and freedoms of a natural living person(s), the data controller shall communicate the personal data breach to the data subject without undue delay and will include:

- The nature of the breach;
- The name and contact details of the Data Protection Officer or other contact point from whom more information can be obtained;
- The likely consequences of the personal data breach, and
- The measures taken or proposed to be taken by the Data Controller to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

The Data Controller may choose not to give some or all of the information above to the data subject if and for as long as this may be a necessary and proportionate measure to avoid obstructing an official or legal inquiry, investigation, or procedure; to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, or in order to protect public or national security, or the rights and freedoms of others.

APPENDIX A: Special Category and Criminal Offence Personal Data

Introduction

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) this document outlines where processing of special category and criminal offence personal data is needed for:
a) Performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment
b) Reasons of substantial public interest

This policy document should be read in conjunction with the Police, Fire and Crime Commissioner (PFCC) for Essex's Data Protection Policy.

Definitions

Special Category Data (Article 9 UK GDPR) includes information revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data or biometric data
- Health data
- Data on a person's sex life or sexual orientation

Criminal Offence Data:
Article 10 of the UK GDPR applies to personal data relating to criminal convictions and offences, or related security measures (Criminal Offence Data). The Information Commissioner's Office guidance says the concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the previous1998 Data Protection Act. However, it is potentially broader than this as Article 10 specifically extends to personal data linked to related security measures.

The Data Protection Principles

Article 5 of the UK GDPR sets out six principles relating to processing of personal data. These provide that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The PFCC will process data covered by this policy in accordance with the six data protection principles.

Processing necessary to carry out obligations under employment law

HR and HR related services are provided to the PFCC by Essex Police.

The special category personal data that it is necessary to process to carry out obligations under employment law is health data relating to employees.

The processing of health data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or data subject in connection with employment (paragraph 1 (1) (a) of Schedule 1 to DPA 2018).

The PFCC requires health data on an employee to carry out its duty to make reasonable adjustments under the Equality Act 2010. The PFCC will not request health data before a conditional job offer is made.

Employees will be provided with a privacy notice explaining the lawful basis for processing the data and the sharing of their data with Essex Police for employment and HR purposes.

The data will not be used for any other purpose than the original purpose or as permitted by law.

The PFCC will only collect the minimum personal data that we need for the purpose it is collected.

The PFCC will ensure the data is accurate and kept up to date where necessary.

Processing necessary for reasons of substantial public interest

The special category and criminal offence personal data it is necessary to process for reasons of substantial public interest is:

- Health data relating to volunteers
- Criminal records relating to volunteers
- Race, ethnicity, religious beliefs, sexual orientation and health of volunteers and employees (i.e. equal opportunities data)

Health data relating to volunteers

The processing is necessary for the exercise of a function conferred on the PFCC by law and for reasons of substantial public interest (paragraph 6 (1) and (2) (a) of Schedule 2 to DPA 2018).

This policy and process also applies to the Independent Custody Visiting (ICV) Scheme as part of its functions under sections 1 and 5 of the Police Reform and Social Responsibility Act 2011 (the 2011 Act) and section 51 of the Police Reform

Act 2002; restorative justice volunteers in the delivery of the Restorative Justice Scheme provided through the PFCC's office and to those Legally Qualified Chairs (LQCs) who are retained through this office. Independent custody visitors and many of the Restorative Justice practitioners are volunteers. The PFCC recruits the volunteers to carry out the ICV visits and Restorative Justice visits. The PFCC may retain health data on volunteers to comply with its duty to make reasonable adjustments and to protect their welfare in a custody environment.

The processing is necessary for the exercise of a function conferred on the PFCC by law and for reasons of substantial public interest (paragraph 6 (1) and (2) (a) of Schedule 2 to DPA 2018). The PFCC needs to carry out a vetting procedure on prospective volunteers to assess their suitability.

Volunteers will be provided with a privacy notice explaining the lawful basis for processing the data. The data will not be used for any other purpose than the original purpose or as permitted by law. The PFCC will only collect the minimum personal data that is needed for the purpose it is collected. The PFCC will ensure the data is accurate and kept up to date where necessary.

Criminal Offence data is treated securely and indicated on the vetting application – many volunteers will send this directly to the Vetting Department, but where it is held by this team, this is stored securely electronically and is limited to access by the management of that volunteer scheme.

Equal opportunities data relating to employees and volunteers

The processing of data relating to race, ethnicity, religious beliefs, sexual orientation and health of volunteers and employees is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between specified groups of people with a view to enabling such equality to be promoted or maintained (paragraph 8 (1) of Schedule 1 to DPA 2018).

The PFCC carries out equal opportunities monitoring as a part of its public sector equality duty (PSED) under the Equality Act 2010. Employees and volunteers will be provided with a privacy notice explaining the lawful basis for processing the data.

The data will not be used for any other purpose than the original purpose or as permitted by law. The PFCC will only collect the minimum personal data that is needed for the purpose it is collected. The PFCC will ensure the data is accurate and kept up to date where necessary. The PFCC will not carry out processing for the purposes of measures or decisions in relation to a particular individual. The PFCC will not carry out processing if it is likely to cause substantial damage or substantial distress to an individual. The PFCC will not carry out processing where an individual has given written notice requiring that we do not process the data, provided the notice gave us a reasonable period in which to stop the processing the data.

The PFCC will retain the data and dispose of the data in accordance with the Records Retention and Disposal Policy. A record of this processing will be kept by the PFCC.

PFCC
POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX

APPROPRIATE POLICY DOCUMENT

September 2021
Review date: September 2022

Contents

Introduction

As part of the statutory and corporate functions of the Police, Fire and Crime Commissioner for Essex (Essex PFFC), we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information in this policy supplements our privacy notice available here: https://www.essex.pfcc.police.uk/contact-us/privacy-notice/ and our employee privacy notice here: https://www.essex.pfcc.police.uk/finance-reporting/publication

Our processing of special category and criminal offence data specifically for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018.

Definitions

Special Category Data

The UK GDPR defines special category data as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Offence Data

In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Conditions for processing special category and criminal offence data

Essex PFCC processes special categories of personal data under the following GDPR Articles:

- Article 9(2)(a) – explicit consent. In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.
- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on Essex PFFC or the data subject in connection with employment, social security or social protection.
- Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.
- Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
- Article 9(2)(g) - reasons of substantial public interest.
- Article 9(2)(j) – for archiving purposes in the public interest.

We process criminal offence data under Article 10 of the GDPR.

Processing which requires an Appropriate Policy Document
Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD.

The following section of this policy is the APD for Essex PFCC. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed
We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs, and their membership of any trade union. Further information about this processing can be found in our employee privacy notice available here: https://www.essex.pfcc.police.uk/finance-reporting/publication.

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our statutory functions to provide an efficient and effective police, fire and rescue service. This may be evidence provided to us as part of a complaint or intelligence information we gather for our investigations. Further information about this processing can be found in our privacy notice available here: https://www.essex.pfcc.police.uk/contact-us/privacy-notice/

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing special category data
Essex PFCC processes special category data for the following purposes under schedule 1 of the DPA 2018:

- Part 1 paragraph 1: employment, social security and social protection.
- Part 2 paragraph 6: Statutory purposes
- Part 2 paragraph 7: Administration of justice and parliamentary purposes
- Part 2 paragraph 8: Equality of opportunity or treatment
- Part 2 paragraph 10: Preventing or detecting unlawful acts
- Part 2 paragraph 11: Protecting the public against dishonesty
- Part 2 paragraph 12: Regulatory requirements relating to unlawful acts and dishonesty
- Part 2 paragraph 14: Preventing fraud
- Part 2 paragraph 15: Suspicion of terrorist financing or money laundering
- Part 2 paragraph 25: Informing elected representatives about our work

Essex PFCC processes criminal offence data for the following purposes under schedule 1 of the DPA 2018:

- Part 1 paragraph 1: employment, social security and social protection when recruiting.
- Part 2 paragraph 6: Statutory purposes i.e. our management of Restorative Justice processes
- Part 2 paragraph 7: Administration of justice and parliamentary purposes
- Part 2 paragraph 10: Preventing or detecting unlawful acts
- Part 2 paragraph 11: Protecting the public against dishonesty
- Part 2 paragraph 14: Preventing fraud
- Part 2 paragraph 15: Suspicion of terrorist financing or money laundering
- Part 2 paragraph 25: Informing elected representatives about our work
- Part 2 paragraph 26: Publication of legal judgments

Procedures for ensuring compliance with the data protection principles

Article 5 of the UK GDPR requires Data Controllers to demonstrate how they comply with the data protection principles. This section describes the measures that Essex PFCC have taken to demonstrate accountability for the personal data that we process and contains details about how we ensure compliance with the data protection principles.

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, employee privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for Essex PFCC to provide an efficient and effective police, fire and rescue service.

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the Essex PFCC in its capacity as a 'public authority' e.g. the Equality Act.

Principle (b): purpose limitation

We process special category and criminal offence data for the purposes listed above, in accordance with the conditions set out in Articles 9-10 of the UK GDPR and Schedule 1 of the DPA.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule available here:

https://www.essex.pfcc.police.uk/finance-reporting/publication. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)
Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies
Our retention and erasure practices are set out in our retention schedule available here: https://www.essex.pfcc.police.uk/finance-reporting/publication