STAFFORDSHIRE POLICE

Appropriate Policy Document
Schedule 1, Part 4, Data Protection Act 2018

Processing special category and criminal offence data for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties including the safeguarding against and the prevention of threats to public security.

CONTENTS

1. INTRODUCTION

Staffordshire Police have a duty to obtain and use a wide variety of information including personal and special category information) in order to discharge its responsibilities and provide appropriate policing to the communities it serves.
When it collects and uses information about individuals and/or groups it should do so in compliance with current legislation and with respect to the rights and freedoms of individual subjects within the wider community. This policy seeks to ensure that we discharge those obligations in an informed, effective and legally compliant manner

2. DEFINITIONS

Biometric data - personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a human being, which allow or confirm the unique identification of that person, such as facial images or fingerprints;

Consent of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller - the person, company, public authority (i.e. the Chief Constable), agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Criminal Conviction and Offence Data – personal data relating to criminal allegations, criminal proceedings, criminal convictions, or related security measures;

Data Protection Act – the current UK legislation governing data protection. This is currently the Data Protection Act 2018;

Data Subject – an individual who is the subject of personal data;

Filing system - any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Genetic data - personal data relating to the inherited or acquired genetic characteristics of a human being which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the person in question;
Information Commissioner (ICO) – the UK's independent body responsible for monitoring the Data Protection Act, see www.ico.org.uk;

Personal data - any information relating to an identified or identifiable human being ('data subject'). An identifiable human being is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (user ID or cookie) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that human being.
Personal data includes, but is not limited to, an individual's:

- Name
- Address
- Telephone numbers
- Identification numbers, such as Payroll number, Service number or National Insurance number
- Recordings, photographs or reproductions of a person's voice, likeness or image
- Bank account numbers
- Medical records, attendance and sickness records
- Online identifiers (e.g. username).

A person's favourite football team, job title, etc. are not typically personal data.

Special categories of personal data – this includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Privacy – privacy can be defined in several ways, including 'the right to be left alone'. The term also covers freedom from unauthorised access to information deemed personal or confidential and freedom from being observed, monitored, or examined without consent or knowledge. Invasion of privacy can involve intrusion on a person's physical solitude or seclusion, public disclosure of private facts, publicly placing someone in a false light or appropriating a person's name or likeness for your own advantage (e.g. identity theft).

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor - a person, company, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a human being, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being;

Recipient - a person, company, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Restriction of processing - the marking of stored personal data with the aim of limiting their processing in the future;

Third party - a person, company, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. AIMS

This policy aims to:

- Ensure that processing of special category (sensitive) personal data by the Controller and his agents or by a processor on behalf of the controller is lawful.
- Ensure compliance with 'The first data protection principle' fair and lawful processing, as outlined in sections 35 of the DPA 2018 and the safeguards set out

in section 42 of that Act.
https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/

- Ensure that the conditions for sensitive processing under Schedule 8 of Part 3 of the DPA 2018 are appropriately applied and met.
- Ensure appropriate granularity when recording consent if relied upon for sensitive processing of data.
- Ensure that where consent is not given, that processing is necessary for the performance of a task carried out for law enforcement purposes.
- Ensure the organisation respects the data subjects' rights and freedoms by appropriate and careful consideration and application of the exemptions and caveats laid out in sections 15, 16, 24, 25, 44 through 50 and Schedules 2, 3, 4 and 8 of the DPA 2018.

4. SCOPE

This policy applies to all police officers, police staff and all other individuals working with or on behalf of the Staffordshire police, involved in the collection, recording, processing, using, retention, review and disposal of all personal information categorised as 'Special Category personal data' under EU Regulation 2016/679 – the General Data Protection Regulations (GDPR) or as 'sensitive personal data' for the purposes of processing under the DPA 2018.

This policy must be read in conjunction with the associated policies and procedures highlighted at the end of section 5 below. This should enable the reader to apply the six data protection Principles outlined in the DPA 2018 and our legal obligations regarding processing, retention and erasure of sensitive information
https://www.staffordshire.police.uk/SysSiteAssets/media/downloads/staffordshire/privacy/retention-schedule.pdf

For the purposes of this policy and processing by consent "sensitive processing" means:—
a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual's sex life or sexual orientation.

Where data is not processed by consent but under one of the conditions set out in Schedule 8 of the DPA 2018 then sensitive processing would be for one or more of the following purposes:
a) Statutory purposes (rule of law or substantial public interest).
b) Administration of Justice.
c) Protecting the Vital Interests of the data subject or another individual.
d) Safeguarding children and other individuals at risk.
e) Where personal data is already in the public domain.
f) Legal Claims (proceedings, advice etc.)
g) Courts or other judicial authorities acting in their judicial capacity.
h) Fraud Prevention
i) Archiving in the public interest, for scientific or historical research or statistical purposes.

In every case the reason for processing must be lawful and compliant with Part 2, section 8 of the DPA 2018 and / or Article 6 of the GDPR (Lawfulness of Processing).
The need for the processing and where appropriate the consent to process MUST be recorded in such a manner as to ensure that there is no question as to whether the consent is true or otherwise and should be a positive act such as a signed statement or audio recording where possible. If this is not the case then the full circumstances behind the necessity to process and the considered risks of not seeking consent must also be documented.
Please note that under the DPA 2018 a 'Law Enforcement Purpose' is defined as:-
"the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security"
This is subtly different from our policing purposes as outlined in the APP and Common Law but covers the same ground.

5. LEGAL BASIS

The implementation of the Data Protection Act 2018 (DPA) has seen the requirement for a policy document to be put in place by police forces to cover sensitive processing for Law Enforcement Purposes. This is a requirement of sections 35(4) & (5) of the DPA when relying on the consent of the data subject or on a condition specified in Schedule 8 of the Act.
Examples of sensitive or special category personal data provided to the Force will include:
During the course of applying to join the Force as a police officer or police staff where we request:

- Racial or ethnic origin;
- Offences and alleged offences;
- Any criminal proceedings including outcomes and sentences;
- Cautions
- Personal identifier(s) e.g. tattoo.

During employment or service with the Force, it may be necessary to request provision of:

- Physical identifiers including DNA and fingerprints;
- Information relating to health and safety incidents, and accident details;
- Details to be recorded in occupational health records;
- Details for including in personal development records;
- Sound and visual images;

An individual's engagement with the Force may be as a result of falling into one or more of the following categories: i.e. as a witness, victim, relative, offender or suspect, or when passing information to the Force for law enforcement purposes.
As a result, it may be necessary to process an individual's:

- Political opinions;
- Religious or other beliefs of a similar nature;
- Details of a physical or mental health condition including medication, medical procedures etc.;

- Details of any offences and alleged offences, criminal proceedings, outcomes, sentences and cautions;
- Sex life or sexual orientation;
- Physical identifiers including DNA, fingerprints and other genetic samples;
- Photographs including footage from body worn video.

Where 'sensitive or special category' information provided consensually by an individual falling into any of the above categories or where such data has been obtained for the purposes of law enforcement; the category the provider falls into, must be clearly recorded. This will ensure the Force is able to differentiate between information collected consensually, in which case consent can be withdraw, putting an obligation on the Chief Constable as Data Controller, to cease processing and remove the data. Equally, where the 'sensitive or special category' information is collected as a result of a Schedule 8 condition, then the condition under which the data has been obtained must be recorded. This enables the identification and removal of the data after the 'relevant period' (six months from collection), or to ensure it is subject of review at the end of the 'relevant period' and further retention justified.
Where further retention is justified, the reason(s) must be recorded. In such cases reference may be made to the Force's Retention Schedule which is taken from the NPCC Retention and Disposal Schedule 2017
https://www.staffordshire.police.uk/SysSiteAssets/media/downloads/staffordshire/privacy/retention-schedule.pdf
The Force may only use the minimum amount of personal information necessary to fulfil or in connection with the particular purpose or purposes for which it has been collected, irrespective as to whether the data is recorded on a computer, in a pocket book or paper record such as a file or as an image including CCTV images.
The Force will ensure that information identified as 'sensitive' or defined as 'special category' data is handled securely, according to the requirements of Principle 6 GDPR and only accessed on a 'need to know' basis.

Other Acts/Policies considered in the drafting of this policy:

- Police Act 1996
- Human Rights Act 1998
- Freedom of Information Act 2000.
- Code of Practice (2005) for the Management of Police Information
- Force Data Protection Policy
  https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/

6. MONITORING

This policy will be monitored to ensure effective compliance. Monitoring will be the responsibility of the policy owner, who will be responsible for developing and reviewing this policy
Active monitoring will be undertaken by supervisors deployed into all relevant business areas.
This monitoring will:

- Ensure this policy has been put into practice
- Check that all the elements are operating properly

- Verify that any published procedures are being applied and complied with
- Ensure the aims of the policy are being achieved

Staff engaged within business areas will also be expected to undertake personal responsibility to ensure the policy is adhered to.
Monitoring is also a way of ensuring the policy does not discriminate against certain groups.
The Data Protection Officer/Deputy Data Protection Officer is accountable for the records management and auditing of these processes.

Other points of reference associated with this policy include:

- College of Policing Information Assurance Authorised Practice
- Force Retention Schedule taken from the NPCC Retention and Disposal Schedule 2017 https://www.staffordshire.police.uk/SysSiteAssets/media/downloads/staffordshire/privacy/retention-schedule.pdf
- Retention Guidelines for Nominal Records on the Police National Computer
- College of Policing guidance on the Management of Police Information
- Force Data Protection Policy
- Force Privacy Notice https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/

7. RETENTION AND ERASURE OF PERSONAL DATA

Personal data is held and disposed of in line with the Force's Retention Schedule which is taken from the National Police Chiefs Council (NPCC) Retention and Disposal Schedule. When disposing of information, the Force ensures this is carried out securely by using physical destruction methods as well as electronic data deletion.
The Force's Record of Processing Activities contains details of the retention periods for the Force's data processing activities together with information on the lawful basis for processing this data. If information is not retained or deleted in line with the policy then the reason is recorded in the Record of Processing Activities.

8. RESPONSIBILITY FOR PROCESSING SENSITIVE DATA

All authorised users are required to comply with the Force's Data Protection policies and mandatory training when processing personal data and to ensure that any processing of sensitive personal data is carried out legally, fairly and transparently. Information Asset Owners are responsible for ensuring that systems and processes under their control comply with current data protection legislation and that personal data is processed in accordance with the data protection principles.

9. REVIEW

The Data Protection Officer/Deputy Data Protection Officer will review this Appropriate Policy Document annually or sooner should there be a change in legislation or subject of case law to ensure that it remains current and relevant. Previous versions of this document will be retained for at least six months after any specified processing of sensitive personal data referred to in that document have ceased. The Data Protection Officer/Deputy Data Protection Officer is responsible for ensuring previous versions of this

document are made available on request and for ensuring this document is reviewed and updated when necessary.

Date for review: 01 APRIL 2021