STAFFORDSHIRE
POLICE

DATA PROTECTION POLICY (Public Facing)

Date: 30/07/2018
Version: 1.1
Review Date: 01/08/2019
Protective Marking: Official
Transparency: Full – proactively published

The Data Protection Act 2018 replaces the Data Protection Act 1998 and keeps the law up to date for the digital age in which ever increasing amounts of personal data, information relating to identifiable living individuals, are being processed. It sets new standards for protecting personal data, in accordance with recent EU data protection laws, giving people more control over the use of their data.

What the Data Protection Act 2018 covers

The four main areas provided for in the Act are general data processing, law enforcement data processing, data processing for national security purposes including processing by the intelligence services and regulatory oversight and enforcement.

Processing by the Police splits into General Processing (covered by DPA Part 2) and Law Enforcement Processing (covered by DPA Part 3). General Processing includes all processing directly within the scope of the General Data Protection Regulation (GDPR).

How is personal data defined?

The Act defines personal data as any information relating to an identified or identifiable **living** individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only potentially be linked to a living individual.

General Processing (GDPR -Part 2 of the Act)

Part 2 of the Act relates to general processing and covers police support functions such as Human Resources, Occupational Health, Finance and Payroll (including pensions), Estates, ICT and Procurement. This means that GDPR applies in its entirety to these functions.

The GDPR does **NOT** apply to the processing of personal data by a competent authority (broadly speaking the Police and other Criminal Justice Agencies) "**for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security".**

Principles

There are six principles which set out the main responsibilities for organisations to adhere to, these are:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further

processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
4. 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;
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.

Special Category Data

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. This data is broadly similar to the concept of sensitive personal data under the 1998 Act. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing under Article 9. There are ten conditions for processing this data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards. A condition for processing this data must be determined before you start processing and this must be documented.

Special category data could be; race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation'

The GDPR rules for sensitive (special category) do not apply to information about criminal allegations, proceedings or convictions. There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures and there must be a lawful basis for processing together with the need to comply with Article 10. These are captured in Part 3 of the Act – Law Enforcement Processing.

Article 10

"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept under the control of official authority"

Law Enforcement Processing (Part 3 of the Act)

Part 3 of the Act applies if you process personal data for **'law enforcement purposes'** and covers processing "**for 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".**

Principles

The principles are broadly the same as those in the GDPR, and are compatible so will assist in managing processing across the two regimes. Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation and a Controller must be able to demonstrate overall compliance with all of the law enforcement principles which are:

1. Processing of personal data for any of the law enforcement purposes must be lawful and fair;
2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;
   Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected;
3. Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed;
4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;
   Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay;
5. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need of the continued storage of personal data for any of the law enforcement purposes;

6. Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Policing Purpose

Staffordshire Police will hold information relating to a range of individuals including victims, witnesses, complainants, suspects and offenders, in connection with the policing purpose as well as details of others who work for or with the Force.

All personal information is held and processed in accordance with the Data Protection Act 2018. Anyone working within Staffordshire Police may only use information in accordance with their policing duties.

Information held by Staffordshire Police may be shared with other organisations where this is necessary for a policing purpose, for example information is shared:-

- With Criminal Justice systems as part of the pre-charge and post-charge processes e.g. prosecuting someone through the Court.
- When working with partner agencies to reduce crime and disorder, and anti-social behaviour as required by the Crime and Disorder Act.
- With the Disclosure and Barring Service which provides information to organisations in order to enable them to make safer recruitment decisions by identifying potential candidates who may be unsuitable to work with children or other vulnerable members of society.
- With other Professional and Regulatory Bodies.

Information is shared where specifically required to do so by statute or by order of the court.

Staffordshire Police will also share information with partner agencies when the information is required to enable them to carry out their statutory responsibilities or where it is necessary to prevent harm to an individual or others.

Any disclosure of personal information will be carefully considered in accordance with legislation, policy and/or information sharing agreements.

A person has the right to see information held about them and can request access to their own information as detailed within the Right of Access procedure.

Registration / Notification

The Chief Constable acts as the Controller for Staffordshire Police and has delegated day-to-day data protection responsibility to the Data Protection Officer (DPO) who acts as the point of contact for the Information Commissioner's Office (ICO).

The Act places an obligation on Controllers to ensure that they process personal data in a fair and lawful manner for a specified purpose. Staffordshire Police have the following purposes registered with the Information Commissioner:-

- **Policing Purpose** – includes the prevention and detection of crime; apprehension and prosecution of offenders; protecting life and property; preserving order; maintaining of law and order; rendering 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.

- **The Provision to support the Policing Purpose**, which includes:
  - Staff administration, occupational health and welfare;
  - Management of public relations, journalism, advertising and media;
  - Management of finance
  - Internal review, accounting and auditing;
  - Training;
  - Property management;
  - Insurance management;
  - Vehicle and transport management;
  - Payroll and benefits management;
  - Management of complaints;
  - Vetting;
  - Management of information technology systems;
  - Legal services;
  - Information provision;
  - Licensing and registration;
  - Pensioner administration;
  - Research, including surveys[1];
  - Performance management
  - Sports and recreation;
  - Procurement;
  - Planning;
  - System testing;
  - Security;
  - Health and safety management

Privacy Notice

In order to comply with Principle 1 – fair and lawful processing, it is a requirement to produce and make publicly available a Privacy Notice. Staffordshire Police have produced a privacy notice which explains why we collect and use personal data, whose personal data we handle, what types of personal data we handle, where we obtain personal data from, which lawful basis do we use to process personal data, how we handle personal data and how we keep it secure and who we disclose personal data to. The privacy notice also explains data subject rights

including the right of access and provides advice on how to apply for their personal data which may be held by Staffordshire Police. A copy of our privacy notice is available via our website and intranet and displayed in public areas, for example custody sites and enquiry offices.

It is also a requirement to ensure signs are displayed where CCTV is in use.

Use of Police Information and Offences

Any use of police information which does not fall within the above categories is deemed unlawful. Section 170 of the Act states a person must not knowingly or recklessly:

(a) obtain or disclose personal data without the consent of the Controller;

(b) procure the disclosure of personal data to another person without the consent of the Controller;

(c) after obtaining personal data, to retain it without the consent of the person who was the Controller in relation to the personal data when it was obtained.

Staffordshire Police staff are aware that the Act creates personal liability and that obtaining; disclosing or procuring of police information for a non-work related purpose is strictly prohibited.

Right of Access

The General Data Protection Regulation (GDPR) Article 15 and the Data Protection Act 2018 (Part 3 Law Enforcement Processing) Section 45, provides individuals with the Right of Access to information that an organisation holds about them (previously known as Subject Access).

Requests can be made in any of the following ways:

1. Submit a request online
2. In writing to the Central Disclosure Unit (Right of Access), Staffordshire Police Headquarters, Weston Road, Stafford, ST18 0YY
3. Email the CDU @ iat@staffordshire.pnn.police.uk
4. Phone 101
5. Visit a police station in person
6. via social media

As with the 1998 Act the Right of Access remains and gives individuals a right to access their personal data. The right of access now allows individuals to be aware of and verify the lawfulness of processing.

The Central Disclosure Unit process ALL right of access requests received by Staffordshire Police. The timeframe for responding to a right of access request

is 1 calendar month and there is no charge for providing the information unless special conditions apply.

However, there are a number of changes to how a Controller should handle right of access requests from both the public and staff:

Requests can now be made verbally – A person doesn't need to complete a form, although this will always be the preferred option, they can telephone or attend a police station in person and make their request. They can even apply via social media. However, a request cannot be accepted until:

a) We have enough information to complete the request;
b) Identity has been confirmed, minimum requirement will be name, address and date of birth, for body worn video or photo / CCTV request we also need photographic proof, i.e. driving licence, passport etc.

The right of access also extends to the following:

Right to Rectification
Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. It must be done within one month, or three months in complex cases. Where no action is taken individuals have the right to be informed of how to seek a judicial remedy.

Right to Erasure
Individuals have a right to have personal data erased in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected / processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing with the processing;
- When the personal data was unlawfully processed
- When the personal data has to be erased in order to comply with a legal obligation;
- When the personal data is processed in relation to the offer of information society services to a child.

Right to restrict processing
Where it is claimed that data is inaccurate or the right to erasure has been exercised individuals can require the Controller to restrict processing until verification checks have been completed. Individuals may also require Controllers to restrict processing where there is no legal basis

Right to data portability – not applicable for Law Enforcement Processing
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a

safe and secure way without hindrance to usability. The personal data must be provided in a structured, commonly used and machine readable form. The information must be provided free of charge.

Right to object – not applicable for Law Enforcement Processing
Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), and processing for purposes of scientific research and statistics.

Rights related to automated decision making including profiling
This gives individuals the right to object to decisions made about them on the basis of automated processing where those decisions have legal or other significant effects. This includes processing where there is no human intervention, for example where automated processes are used to sift recruitment applications.

Requests received in relation to any of the above should be directed to the Data Protection Officer or Central Disclosure Unit Manager at Staffordshire Police Headquarters, Information Assurance Team, Block 8, Weston Road, Stafford, ST18 0YY.

Exemptions

Crime and Taxation – The GDPR regulations relate to the processing of personal data where it is done so for non-Law Enforcement purposes. The Data Protection Act 2018 sets out exemptions from the GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within GDPR **DO NOT** apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within Schedule 2 Part 1 Paragraph 2 (Crime & Taxation: general). This applies where personal data is disclosed by an organisation subject to GDPR to the police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

It restricts the application of GDPR data protection principles and subject rights to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection or the apprehension or prosecution of offenders without fear of breaching GDPR or Data Protection Act 2018.

Vital Interests – GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure is necessary in order to protect the vital interests of the data subject or of another natural person.

Data Protection Impact Assessments

Data Protection Impact Assessments replace Privacy Impact Assessments and are mandatory under the DPA 2018 in cases where processing is likely to result in a high risk. It is a valuable tool to identify the most effective way to comply with data protection obligations and meet data subjects' expectations of privacy. A DPIA must be completed before carrying out types of processing likely to result in high risk to individual's interests. Where a DPIA is carried out that identifies a high risk that cannot be mitigated, Staffordshire Police are obliged to consult with the Information Commissioner's Office.

Personal Data Breach

Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual definitely must be notified to the Information Commissioner in accordance with force procedure.

Where a breach has been identified Staffordshire Police are required to inform the Commissioner without undue delay and within 72 hours of becoming aware of a personal data breach, unless it is unlikely to result in a **risk** to the rights and freedoms of an individual or individuals.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. The consequence of such a breach is that the Controller (Chief Constable) will be unable to ensure compliance with the six principles relating to the processing of personal data. Examples of a personal data breach are provided below:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data misuse of personal data
- cyber attacks

- lost or stolen paperwork

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. A personal data breach will occur whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Staffordshire Police have a process in place for dealing with such breaches and, where appropriate, reporting breaches to the Information Commissioner's Office.

Data Protection Officer

Under the new Act the appointment of a Data Protection Officer is mandatory for a Police Force as it is considered to be a public authority who carry out processing of personal data.

Staffordshire Police are going through significant transformation and a review of the DCC Directorate is currently well underway. As an interim measure the force has adopted the Model Force Structure which is recommended by the National Police Chief's Council (NPCC) with the Head of Information Assurance taking on the designated role of the DPO and the Review Supervisor acting as the Deputy DPO, this will continue until the outcome of the review is known and the new structure is in place.