STANDARD OPERATING PROCEDURES:
OFFICE OF THE BEDFORDSHIRE POLICE AND CRIME COMMISSIONER

Title	Data Protection / Information Management Policy
Area of Compliance	Compliance
Version No.	1.0
Senior Lead	Chief Executive
Author	Compliance

Revision History

Date	Revision	Change	Section	Review Date
21.05.2018	1.0			21.05.2019
21.05.2019	1.0	No Change		21.05.2020
20/09/2019	2.0	Info regarding BCH Force policy added		20/09/2019
20/09/2019	2.0	No Change		20/09/2020
20/09/2020	2.0	No Change		20/09/2021

Introduction

The Police and Crime Commissioner (PCC) is a registered Data Controller (registration no. Z3369495). The PCC is committed to conducting its business in accordance with the data protection laws. During the course of our activities we will collect, store and process personal data about our service users, employees, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

PCC employees are obliged to comply with this policy when processing personal data.

The types of personal data that the PCC may be required to handle include information about service users, employees and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (together referred to as the Data Protection Legislation).

Bedfordshire OPCC link with BCH (Beds,Cambs,Herts) Information Management Unit when dealing with Information management - BCH14/001 Joint - Information Management Policy (IMP) – Available on the Intranet.

Definition of Data Protection terms

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data Controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR. The PCC is the data controller of all personal data it collects or uses in its day to day business and in providing services.

Data Processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it includes suppliers, providers and contractors which handle personal data on the PCC's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, viewing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

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.

Third Party - Any individual/organisation other than the data subject, the data controller (the PCC's) or its agents.

Data Protection Impact Assessment is a process to help identify and minimise the data protection risks of a project. A DPIA should be carried out for processing that is likely to result in a high risk to individuals. 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 additional measures to mitigate those risks.

Responsibilities under the General Data Protection Regulation (GDPR)

The PCC is a Data Controller under GDPR; it is also a Processor of information for other organisations.

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

The Data Protection Officer is responsible for ensuring compliance with GDPR and with this policy and may assign officers to support this process.

Compliance with Data Protection legislation is the responsibility of everybody who processes personal information.

The PCC, through its staff, is responsible for ensuring that any personal data supplied is accurate and up-to-date.

Data Protection Principles

Anyone processing personal data must comply with the six principles relating to processing of personal data in the GDPR. 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'). For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in GDPR. These include, among other things, processing is necessary:
  - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the PCC;
  - for the performance of a contract to which the data subject is party;
  - for compliance with a legal duty;
  - the data subject has given consent for the data to be processed for a specific purpose(s).

When special category data (sensitive personal data) is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only process personal data for specific purposes. We will notify those purposes to the data subject when we first collect the personal data or as soon as possible thereafter.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). Personal data, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
- 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'). Personal Data, which is kept for a long time, must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that personal data held by the PCC is accurate and up-to-date. Individuals should notify the PCC of any changes in circumstance to enable personal records to be updated accordingly. It is

the responsibility of the PCC to ensure that any notification regarding change of circumstances is noted and acted upon.

- 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. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. On occasion, 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 in accordance with Article 89(1) of the GDPR.
- 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').

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them through our Privacy Notices about:
(a) The purpose or purposes for which we intend to process that personal data.
(b) The legal basis for processing.
(c) The types of third parties, if any, with which we will share or to which we will disclose that personal data.
(d) The length of time that we will retain the data.
(e) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information within the required timescales.

We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of our Data Protection Officer.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies 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.

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. Any stranger seen in entry-controlled areas will be reported;
(b) Secure lockable desks and cupboards. Desks 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. PCC employees will ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended;
(e) IT Security. IT provision is provided for the PCC by the Bedfordshire Police Force ICT Department. A condition of use is compliance with the security policies of Bedfordshire Police.

Training for staff includes:

(a) Mandatory training (E-Learning) for all staff on Data Protection, with refresher training;
(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. (E-Learning)

Governance and assurance procedures include:
(a) Internal and external audits of the PCC's Information Management processes and procedures;

(b) For new data collection processes the PCC will ensure that a Data Protection Impact Assessment is conducted in conjunction with the Data Protection Officer for all new and/or revised systems or processes.

Disclosure and sharing of Personal Information

We will only disclose or share a data subject's personal data where we are legally permitted to do so, in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, service users or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Individual's rights under GDPR

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

- ask the PCC 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 PCC 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 PCC not to use personal information:
- for direct marketing; which is likely to cause unwarranted substantial damage or distress;
- to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

These rights are not absolute, if the PCC is unable to respond to a request, it will outline the legal reasons for its decision clearly.

Dealing with Subject Access Requests

The PCC has provided application forms on its website to assist data subjects to make a request to access information we hold about them. Data subjects do not have to use our forms or use any particular wording. A subject access request is valid if it is submitted by any means, *i.e*. in a letter, an email or verbally. Employees who receive a request should pass it without delay to the Compliance Officer.

Any individual who wishes to exercise this right should provide satisfactory proof of identity and sufficient information to enable the data to be located.

Subject to satisfactory completion of above, the PCC should respond within one month.

There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include repeat access requests, confidential references, and third party information.

Further information can be found in the GDPR Privacy Policy.

Dealing with a Data Security Breach
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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A data security breach must be reported to the Data Protection Officer without delay to be recorded and reported as appropriate.

Further information can be found in the PCC's Data Breach Policy.

Retention and disposal of data

The PCC discourages the retention of personal data for longer than they are required.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (*e.g*. shredding, disposal as confidential waste, secure electronic deletion).

The PCC maintains a Retention Policy and a Retention Schedule that is specific and relevant to specific types of information and the services they relate to. These outline the appropriate periods for retention.

Where the PCC deviates from its Retention Schedule it will record the reasons why and will indicate how long the information will be retained.

Further information can be found in the PCC's Retention and Disposal Policy.