POLICE & CRIME COMMISSIONER
for Leicester,
Leicestershire & Rutland
Your Communities - Your Commissioner

OPCC Policy for Data Protection

Version v.1 July 2023
Review Date: July 2025

Policy Owner:	Chief Executive
Role Responsible:	Policy and Compliance Officer
Senior Manager Review:	Director of Governance and Performance
Protective Marking:	Official
Date of next review:	July 2025

Review log

Version	Date	Minor / Major / No change	Section	Author
v.0.1	3/7/2023	First draft – based on GDPR/DPA legislation	All	8520 H Forman (Information Management)/ 7491 Nish Padhiar (OPCC)
V1	7/9/23	Approved	SMT	Interim CEO - Andrew Champness

Contents

1. Statement

1.1 The Police and Crime Commissioner (PCC) for Leicestershire is a statutory role which was established by the Police Reform and Social Responsibility Act 2011. The role was established as a corporation sole, meaning that the PCC is a separate and independent legal entity.

1.2 The Leicestershire PCC is a registered Data Controller (registration no. Z3594213) – as such, the PCC is committed to ensuring that all of its business is conducted in accordance with the laws governing data protection.

1.3 Dependent on the processing that is being undertaken, the PCC is both a Data Controller under the UK General Data Protection Regulation and the Data Protection Act 2018 (the data protection legislation) (GDPR), and also a Data Processor where it is processing information on behalf of other organisations.

1.4 Whilst the role, functions and powers of the PCC are set out in the 2011 Act, the Policing Protocol Order summarises the requirements and responsibilities placed upon the PCC.

1.5 The Leicestershire PCC has the legal power and duty to—

(a) Set the strategic direction and objectives of the Force ("Leicestershire Police") through the Police and Crime Plan ("the Plan"), which must have regard to the Strategic Policing Requirement set by the Home Secretary;

(b) Scrutinise, support and challenge the overall performance of the Force including against the priorities agreed within the Plan;

(c) Hold the Chief Constable to account for the performance of the Force's officers and staff;

(d) Decide the budget, allocating assets and funds to the Chief Constable; and set the precept for the Force area;

(e) Appoint the Chief Constable (except in London where the appointment is made by the Queen on the recommendation of the Home Secretary);

(f) Remove the Chief Constable subject to following the process set out in Part 2 of Schedule 8 to the 2011 Act and regulations made under section 50 of the Police Act 1996 (3);

(g) Maintain an efficient and effective police force for the police area;

(h) Enter into collaboration agreements with other PCCs, other policing bodies and partners that improve the efficiency or effectiveness of policing for one or more policing bodies or police forces in consultation with the Chief Constable (where this relates to the functions of the police force, then it must be with the agreement of the Chief Constable);

(i) Provide the local link between the police and communities, working to translate the legitimate desires and aspirations of the public into action;

(j) Hold the Chief Constable to account for the exercise of the functions of the office of Chief Constable and the functions of the persons under the direction and control of the Chief Constable;

(k) Publish information specified by the Secretary of State and information that the PCC considers necessary to enable the people who live in the Force area to assess the performance of the PCC and Chief Constable;

(l) Comply with all reasonable formal requests from the Panel to attend their meetings;

(m) Prepare and issue an annual report to the Panel on the PCC's delivery against the objectives set within the Plan; and

(n) Monitor all complaints made against officers and staff, whilst having responsibility for complaints against the Chief Constable.

1.6 In order to carry out their functions as described above, the PCC must process personal data – this means that they will collect, store, use and process personally identifiable information. In doing so, the PCC must comply with the provisions of the UK GDPR and the Data Protection Act 2028, and Article 8 of the Human Rights Act 1998, as well as any other relevant data protection legislation – this is essential to ensuring that public confidence in the organisation is maintained and will ensure successful business operations.

1.7 The PCC recognises that personal data must be processed in accordance with the principles governing data protection which are (in summary):

- Processing of personal data must be lawful, fair and transparent;
- Personal data must only be collected for a specified, explicit and legitimate purpose 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 ('purpose limitation');
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Personal data must be accurate and, where necessary, kept up-to-date 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 must only be kept in a form which permits identification of data subjects for the minimum time possible (no longer than is necessary) ('storage limitation'); and
- Personal data must only be processed in a manner that ensures appropriate security of the personal data.

2. Aims

2.1 This policy aims to:

- Set out the basis on which the PCC will process any personal data collected from data subjects, or that is provided to us by data subjects or other sources, in accordance with the data protection legislation;

- Set out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data; and

- Address the relationship between the PCC and Leicestershire Police ('the Force').

3. Scope

3.1 This Policy is applicable to all employees of the PCC for Leicestershire as well as the Police and Crime Commissioner, Deputy and Assistant Police and Crime Commissioners, volunteers, consultants, contractors and partner organisations. This policy is designed to set out clearly how the PCC will protect personal data – it is a set of principles, rules and guidelines that informs how the PCC will ensure ongoing compliance with the data protection laws.

4. Policy

4.1 The relationship with Leicestershire Police

4.1.1 Whilst separate legal entities, the PCC and Chief Constable of Leicestershire Police have a close working relationship on a day-to-day basis. As for the PCC, the Chief Constable is a corporation sole, which means that they are an individual person who represents an official position which has a single separate legal entity – this is an official position that can only be created by statute, for the PCC this is the Police Reform and Social Responsibility Act 2011 and the Policing Protocol Order 2011

4.1.2 The PCC and Chief Constable have agreed to work collaboratively and co-operatively where necessary in order to ensure the effective and efficient delivery of policing services.

4.1.3 Whilst the PCC and Chief Constable have clear, distinct legal identities, it is acknowledged and accepted that there is a clear rationale and justification for the sharing of certain areas of business support in order to achieve mutually beneficial efficiencies. Accordingly, the Chief Constable provides certain functions to the OPCC through a Service Level Agreement (SLA).

4.1.4 As a result of these arrangements (the delivery of certain services to the PCC by the Chief Constable) personal data under the control of the PCC is processed by the Chief Constable. This will be regulated by an agreement between the two corporation sole – between the Data Controller and Data Processor.

4.1.5 There are instances in which the PCC will receive personal data from the Chief Constable in order for the Chief Constable and PCC to carry out their statutory obligations – one such example is in relation to Complaint Reviews.

4.1.6 The relationship between the PCC and Chief Constable is such that, in absence of a PCC specific policy document and as appropriate, the policies of the Chief Constable are taken to apply within the OPCC.

4.2 Data collected and held by the PCC

4.2.1 The PCC will ensure that all personal data is processed in a manner that is fair, lawful and transparent. The PCC takes seriously its obligations relating to the custodianship of the personal data processed for the purposes of carrying out his statutory role, and its responsibilities for compliance with the The UK GDPR and the Data Protection Act 2018, and Article 8 of the Human Rights Act 1998, and other relevant data protection legislation.

4.2.2 The PCC, compared to other public authorities, collects a relatively small amount of personal data – this data is processed to enable the PCC to perform its statutory functions. No data should be collected or processed by the PCC outside of this function. The personal data that is routinely collected and processed by the PCC is as follows:

- Name, address and any other contact details such as email addresses and telephone numbers;
- Age, date of birth and biographical details;
- Employment documentation including previous employment history, references and educational history;
- Gender, ethnicity, religion and nationality data;
- Passport/Visa details;
- Health and disability Information;
- Criminal antecedent history (where the information is necessary to carry out a legislative function);
- Complaint, incident and accident information;
- Offences including alleged offences;
- Criminal proceedings, outcomes and sentences;
- Family details;
- Lifestyle and social circumstances;
- Photos and videos;
- Finance data to provide payments – e.g. to employees, contractors etc.;
- Additional information you provide;
- Education and training details; and/or
- Certain manual files linked to the previous police authority.

4.2.3 In relation to this personal data, the PCC is a Data Controller – this is because the PCC determines the means and purposes for the collection of the data. The data listed above is usually collected directly from the data subject themselves (for job applications, lodging of complaints/queries, OPCC staff HR, etc.), however some of the data may be collated from third-party sources including Leicestershire Police.

4.3 Data minimisation

4.3.1 In accordance with Article 5(c) of the UK GDPR and the Data Protection Act 2018, and Article 8 of the Human Rights Act 1998, the PCC will ensure it only processes data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" – this is the principle of data minimisation.

4.3.2 Prior to collecting the data, the PCC as Data Controller must consider the following questions for each point of data they plan to collect:

- Does the data subject know the PCC is collecting the data?
- How are the PCC planning to use this data?
- Does the data subject know why the PCC is collecting the data?
- Is there a way of achieving the same purpose without having to collect the data?
- How long will the PCC need the data for in order to achieve the purpose?

4.3.3 Practical steps taken by the OPCC to ensure that data minimisation requirements are met include:

- Use of anonymised/pseudonymised data where at all possible and appropriate;
- Only collecting and processing data that is relevant to the purpose;
- Not collecting any data "just in case";
- Continually reviewing data that is held by the PCC to assess if it is still required or whether it can be destroyed; and
- When sharing data, ensuring that this is only on a "need to know" basis, and that only the minimum data necessary to achieve the purpose is disclosed.

4.4 Data Review, Retention and Disposal (RRD)

4.4.1 The PCC has a policy for Records Management – this sets out how RRD will be managed by the OPCC and details the specific retention periods for the various types of data processed by the OPCC. For any data not covered by these documents, the retention periods for the Chief Constable will be applied.

4.4.2 As referenced above (4.3.3), data retained by the PCC will be regularly reviewed for consideration of accuracy, relevancy, GDPR compliance and disposal. Any inaccurate personal data will be rectified or disposed of. For purposes of disposal, personal data will not generally be retained beyond the time where the purpose for the data processing (including its retention) has ended. Retention should not be for longer than is necessary and consideration as to retention should be given against the time limits in the policy for Records Management. If data is retained beyond the period specified in this documentation the justification must be recorded, and where necessary or appropriate, the DPO consulted.

4.4.3 Data will be stored in manual records, long-term storage or the Leicestershire Police's ICT systems whose use is provided to the OPCC by the Chief Constable. In each of these locations, the necessary levels of security are afforded to the personal data, using appropriate technical or organisational measures, in order to ensure there is no unauthorised or unlawful processing, accidental loss, destruction or damage.

4.4.4 Data subjects must be informed of the retention of their data by the PCC and their rights in relation to it (see Section 4.5).

4.5 Rights of data subjects

4.5.1 *Rights of access*

A data subject who makes a request to the PCC (whether in writing, by phone or email) is entitled to be told whether or not any of their personal data is being processed. If this is the case, then the data subject is entitled to be advised of the description of the personal data, the purposes for which it is being processed, the details of any recipients, the retention periods and their rights of rectification, erasure, restriction and objection. A data subject has a right to be given a copy of the information that is held, and given details of the source of the data – this is a Subject Access Request (SAR).
Where access is requested, all reasonable measures to verify the identity of the data subject should be adopted before access is given.

The first copy of information provided in response to a SAR will be provided free of charge. Thereafter a reasonable fee reflecting the cost of administration may be charged.

Where the request is excessive or repetitive, either a fee may be charged in respect of administration costs, or the request can be refused. In the case of the latter, the reasons will be provided to the data subject. Information about their right to make a complaint to the Information Commissioner's Office (ICO) will also be provided with this communication.

SARs will be responded to, where at all possible, without delay and no later than a month after receipt of the request. If the request is complex or there are a number of requests from an individual this may be extended by a further two months – in this circumstance we will contact the data subject to advise them of this.

4.5.2 *Right to rectification*

The data subject has the right to require a Data Controller to rectify any errors in their personal data. The response to the exercise of this right must be within a month of being notified of it. If no action is being taken in response to the request, the data subject must be informed of this as well as their right to lodge a complaint with the ICO.

Third parties to whom the personal data has been disclosed should also be informed of the exercise of this right.

4.5.3 *Right to erasure*

The data subject has the right to require a Data Controller to delete their personal data if the continued processing of those data is not justified. This will involve consideration of whether the organisation has a lawful basis for processing the personal data.

4.5.4 *Right to restrict processing*

Data subjects may not be entitled to require the Data Controller to erase their personal data, but may be entitled to limit the purposes for which the controller can process those data. This may occur where the accuracy of the data is contested, the processing is unlawful but the data subject requests restriction instead of deletion, or where the data is no longer required by the data controller but the data subject requires it for the establishment, exercise or defence of legal claims.

4.5.5 *Right to data portability*

The data subject has the right to transfer their personal data between controllers. This right may only be exercised where the legal foundation is consent or contract. It does not apply where the controller is acting under official authority or in the public interest.

Data subjects have the right to receive personal data relating to them in a structured, commonly used, machine-readable format to enable them to keep, use or share it with a third party or another controller. The right can be exercised by requesting one controller to provide it directly to another. The right only applies where the personal data is in electronic form.

4.5.6 *Right to object*

A Data Controller must have a lawful basis for processing personal data. However, where that lawful basis is either “public interest” or “legitimate interests”, these lawful bases are not absolute and data subjects may have a right to object to such processing. The right to object is a conditional right and can be refused if legitimate interests or public interest override the data subject’s rights or where the processing is for the establishment, exercise or defence of a legal claim.

4.5.7 *Right to not be evaluated on the basis of automated processing*

Data subjects have the right not to be evaluated in any material sense solely on the basis of automated processing of their personal data.

4.6 Staff training and supervision in handling personal data

4.6.1 The PCC take seriously the need for ongoing training and support in all matters relating to data protection. In addition to the basic data protection induction delivered to all OPCC staff and volunteers at the commencement of their role, there is also an ongoing programme of training and awareness-raising established for the OPCC. This includes online-learning which is required on an annual basis (NCALT), monthly training delivered as part of the wider OPCC team meetings, in addition to awareness raising as and when needed in response to specific incidents or near-misses. This ensures that the OPCC are dynamically managing the risks around data protection, and

are able to identify and address training gaps swiftly. Specialist training for specific data protection matters, such as DPIAs and SARs are delivered to individuals and small groups on an ad-hoc basis in response to the business need – where appropriate external training may also be used, e.g. SARs, Audit.

4.6.2 On a day-to-day basis, staff will be supervised by their Line Management who will escalate any compliance issues of note. The Force's Professional Standards Department (PSD) Section and Audit team will remotely audit processing activities, both routinely and is response to a specific concern.

4.6.3 Information relating to breaches or near-misses will be shared between the DPO, Director of Governance and Performance, Policy & Compliance Officer and Chief Executive (SIRO) so that any learning from can be shared with the wider OPCC – this will be ad-hoc, in the weekly team meetings, or in the quarterly meetings, as and when required. Bespoke training will be delivered to individuals or the wider OPCC as appropriate and necessary to address any issues identified.

4.7 Role of the Data Protection Officer (DPO)

4.7.1 As a public authority, the OPCC are required by the UK GDPR and UK GDPR and Data Protection Act 2018 to appoint a DPO – the responsibilities of the DPO include:

- Monitoring internal compliance;
- Informing and advising on the data protection obligations;
- Providing advice regarding DPIAs; and
- Providing a contact point for data subjects and the supervisory authority – ICO.

4.7.2 The PCC has designated the Leicestershire Police DPO to take responsibility for Data Protection compliance within the OPCC. The DPO will ensure that this role is performed independently of that for the Force – where there is a conflict of interest, this will be managed as per the DPO's Managing Conflicts of Interest documentation.

4.8 How data processing activities are recorded

4.8.1 Under Article 30 for the UK GDPR and Data Protection Act 2018, the OPCC are required to create and maintain a Record of Processing Activities (ROPA). The ROPA will include a detailed overview of the processing activities and the most important details about the processing activity, which must be available upon request of a supervisory authority.

4.8.2 The ROPA will be recorded in electronic form to allow for the content to be added, removed and amended as appropriate.

4.8.3 As a living document, the ROPA will be updated in response to any new or amended processing (including ceasing). This will be overseen by the Operations and Compliance Manager whose responsibility it will be to ensure that the ROPA continues to be kept accurate and up-to-date by the relevant business leads as to the processing activities of the OPCC.

4.84 Where at all possible, the OPCC will put in place mechanisms to ensure that the business leads are immediately advised of any changes to processing activities, i.e. it will be a requirement of project initiation and finalisation, to ensure that the ROPA is kept up-to-date in a timely fashion.

4.9 Demonstrating Accountability

4.9.1 Under the UK GDPR and Data Protection Act 2018, organisations must be able to demonstrate through evidence their compliance with the legislation. The PCC will demonstrate their Accountability to the ICO through the following measures:

- The adoption and implementation of data protection policies and procedures;
- Taking a 'data protection by design and default' approach;
- Putting written contracts in place with organisations that process personal data on behalf of the PCC;
- Maintaining documentation of your processing activities (ROPA);
- Implementing appropriate security measures;
- Recording and, where necessary, reporting personal data breaches;
- Carrying out DPIAs for uses of personal data that are likely to result in a high risk to data subjects' interests;
- Appointing a DPO; and
- Adhering to any relevant codes of conduct and signing up to certification schemes.

4.10 Privacy notices

4.10.1 The PCC understands that a key element of the UK GDPR and Data Protection Act 2018 is transparency – this means providing readily accessible information to data subjects about how their data is processed by the PCC. This is achieved through the PCCs Privacy Policy which is published on the PCC website; this is periodically reviewed and updated.

4.10.2 When data is collected from a data subject, they will be informed about why the PCC are collecting their data and how it will be processed. Data subjects will be provided with a privacy notice which sets out all the privacy information at the point at which the data is collected from them. This will include:

- The name and contact details of the PCC as Data Controller and the collector of the data;
- The purpose/s and legal basis/es for processing the data (i.e. why the data is being collected);
- How the data will be used;
- Who the data will be shared with (any third parties);
- How long the data will be retained; and
- The data subjects rights under the UK GDPR and Data Protection Act 2018.

4.10.3 A privacy notice will be issued to data subjects, including those who apply for a role within the OPCC (whether appointed or not), contacts, correspondents and complaints, and as described in section 4.2.2 above. In the case of job vacancies, this requirement will arise at the point of application. For the other examples, this will be carried out at the earliest opportunity. In the case of job applications, the PCC informs applicants of the requirement to process personal data for the purposes of considering the application, and if appointed, the subsequent discharge of the appointment and associated matters.

4.10.4 A template privacy notice for those who apply for roles with the PCC can be found at **Appendix A**. This notice should be issued to all data subjects who apply for a role (whether appointed or not) at the point of application.

4.10.5 In view of some of the arrangements detailed at paragraph 4.1, the personal data of some data subjects will of necessity be required to be shared with the Chief Constable of Leicestershire Police, e.g. HR, ICT etc. This will be described in the privacy notice.

4.10.6 Further privacy notices are shown at **Appendix B and C** – these should be provided to data subjects as appropriate for the processing and action taken by the OPCC.

4.11 Consent

4.11.1 The PCC has a policy and procedure that specifically details how consent is to be used and managed by the OPCC.

4.12 Systems security – technical and organisational measures

4.12.1 The PCC will use the technical and organisation measures employed by the Force for the security of their systems – this is to guard against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. In addition to these measures, the PCC utilise the following security procedures:

- **Entry Controls** – the PCC employ restricted access controls for the offices of the OPCC;
- **Secure lockable desks and drawers** – desks and cupboards are kept locked if they contain personal/confidential information of any kind;
- **Methods of disposal** – paper documents are shredded, digital storage devices are physically destroyed when they are no longer required;
- **Equipment** – PCC employees will ensure that individual monitors do not show confidential information to passers-by and that they locked their PC when it is left unattended; and
- **IT Security** – IT provision and security is provided for the PCC by Leicestershire Police IT Department and Information Management Section.

4.12.2 The OPCC has adopted the Government Security Classification (GSC) Scheme and operates a Clear Desk, Clear Screen Policy.

4.13 Data breaches

4.13.1 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.

4.13.2 Any suspected personal data breach shall be notified to the Leicestershire Police Information Security team and DPO via the Information Security page of the Force website without delay – this is to enable them to consider and take the appropriate course of action. The Chief Executive (SIRO) and Executive Director must also be notified.

4.13.3 In the case of a personal data breach, the data controller shall, without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

4.13.4 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay. The communication should include the nature of the breach and recommendations for mitigating adverse effects.

4.14 Contracts and commissioning

4.14.1 In the arrangements between the PCC and the Chief Constable, for the purposes of contracts and procurement, the PCC has overall responsibility for property and contracts. The PCC (through the MOU) has given delegated this responsibility to the Chief Constable for the daily administration of contracts in accordance with the Financial Regulations and Contracts Standing Orders. All contracts are required to be entered into in the name of the PCC.

4.14.2 The Chief Constable therefore has responsibility for the daily administration of contracts. The PCC requires that the Chief Constable ensures that all existing and future contracts are UK GDPR and Data Protection Act 2018 compliant. In this regard, appropriate due diligence is undertaken by the Chief Constable's procurement function. Whereas the PCC is the Data Controller in relevant contracts, by virtue of his letting a contract or call-off from a Framework Agreement, the Chief Constable will also be a Data Controller/Data Processor. This will be provided for in the MOU between the PCC and the Chief Constable.

4.14.3 In some instances, the PCC may pass personal data under his control to a contractor. In that situation, the PCC must ensure as Data Controller that where personal data is passed to a Data Processor, the contract ensures that the Data Processor complies with their GDPR responsibilities and obligations in accordance with Article 28 of the GDPR.

4.14.4 The PCC has the power to arrange for the provision of services that secure the reduction of crime and disorder, or help victims, witnesses and others affected by anti-social behaviour and offences. It is unlikely that any GDPR issues arise for the PCC as Data Controller as the external organisations who are commissioned to provide such services are not using PCC data to meet the PCC's purpose. Notwithstanding this position, the service must be arranged under an agreement that places specific conditions on the external organisation, that in relation to the service being commissioned, the external organisation must ensure that any processing carried out will meet the requirements of the UK GDPR and Data Protection Act 2018, and ensure the rights of the data subject.

5. Legal Basis

5.1 The vast majority of the data collected and held by the OPCC is necessary for compliance with the legal obligations associated with the role of the PCC, who is data controller for such data. See **Appendix D** for a table illustrating the lawful bases used by the OPCC for processing all types of data.

5.2 Through legislation, codes of practice and associated guidance, the PCC is required to carry out certain duties including the appointment of a Chief Constable, Audit Committee members, Legally Qualified Chairs, Independent Members of Misconduct Panels, and Custody Visitors. The PCC is required to provide the link between the police and communities, as well as working with partners. The PCC are therefore required to process personal data in relation to their performance of these functions.

5.3 The PCC has responsibility for handling complaints against the Chief Constable. The PCC may also receive complaints about themselves; in this instance, the any complaints are directed to the Solicitor at the City Council who manages this process on behalf of the Police and Crime Panel. The OPCC Chief Executive undertakes no actions in this regard other than pass on.

5.4 The PCC employs staff to statutory and other roles within his office, acting through the statutory powers invested in him as the PCC. In this regard, the processing is necessary for the performance of employment contracts.

5.5 The PCC discharges a number of statutory responsibilities, where he is duty-bound to act. This can involve the processing of personal data. The lawful basis under the UK GDPR for the processing of such personal data is that the processing is necessary for compliance with a legal obligation to which the PCC as Data Controller is subject.

5.6 The PCC performs statutory functions and derives his authority from legislation. As such, he has a legal foundation for processing personal data. The corollary of this is that neither the PCC nor the OPCC should be involved in the processing of personal data either electronically nor otherwise that is not connected or associated with the PCC or OPCC functions.

6. Monitoring

6.1 Whilst every individual working in the OPCC is responsible for their own compliance with the data protection legislation, the day-to-day monitoring of this compliance is the responsibility of the supervisors who are required to report any issues to the Operations and Compliance Manager who will highlight this to the Senior Management Team. This role is overseen by the Deputy Chief Executive who liaises regularly with the DPO to ensure that any Data Protection issues are managed effectively and efficiently.

6.2 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 and the information is up to date;
- Verify that any published procedures are being applied and complied with; and
- Ensure the aims of the policy are being achieved.

6.3 Staff engaged within business areas will also be expected to undertake personal responsibility to ensure the policy is adhered to.

Associated Documents:

OPCC Policy and Procedure for DPIAs

OPCC Privacy Notice

OPCC Policy and Procedure for Consent

OPCC Policy for Records Management

OPCC Policy for Clear Desk, Clear Screen

Appendices

Appendix A

Applications for Appointments

The Police and Crime Commissioner for Leicestershire (PCC) is a Data Controller for the purposes of the UK GDPR and Data Protection Act 2018 (GDPR). In the discharge of his statutory functions it is necessitous for personal data to be collected from data subjects.

The PCC, in pursuance of his statutory functions, makes appointments relating to the Chief Constable, the PCC's statutory officers, his employees, the Audit Committee, Legally Qualified Chairs and Independent Members of Misconduct Panels, and Custody Visitors. In order to make these appointments, he requires access to the personal data of applicants. The data collected in the application process will be used to make appointment decisions.

In the case of unsuccessful applicants, the data will be retained and disposed of in accordance with the time period specified in the OPCC's Policy for Records Management (available on the PCC's website).

Personal data obtained from successful applicants will be used to facilitate the successful delivery of the appointments. It will be shared with Chief Constable of Leicestershire Police in order to deliver, where appropriate, the functions relating to service delivery, e.g. HR, pension, payroll, ICT, vetting and other such necessary functions. The personal data of successful applicants will be retained and disposed of, again in accordance with the time period in the OPCC's Policy for Records Management.

Appropriate personal data such as contact data will also be shared within the functional groupings of appointees in order to facilitate the more efficient performance of the statutory functions requiring to be performed. In the case of Legally Qualified Chairs and Independent Members of the East Midlands Region Panels, appropriate personal data will be shared with other Regional PCCs, Chief Constables, Constabularies and Police Forces.

Your personal data will only be reasonably used to enable the discharge of statutory functions. The OPCC has adopted a Data Protection Policy which sets out his approach to handling personal data. It is available through the PCC's website, or alternatively a copy may be requested by contacting the PCC at the address below.

As a data subject, you have the following rights under the UK GDPR and Data Protection Act 2018:

- The right to informed about the collection and use of your personal data;
- The right of access to your personal data;
- The right to require a controller to rectify errors in their personal data;

- The right to require a controller to delete your personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of your personal data;
- The right to transfer your personal data between controllers where appropriate;
- The right to object to the processing of your data in certain circumstances; and
- The right not to be evaluated on the basis of automated processing.

These rights are explored in more detail in the OPCC's Data Protection Policy.

The contact details for the PCC are:

Address –	Office of the Police and Crime Commissioner for Leicestershire Police Headquarters St Johns Enderby, Leicester LE19 2BX
Telephone –	0116 2298980
Email –	OPCC@leics.police.uk

Appendix B

For use with Correspondents and Complainants

The Police and Crime Commissioner for Leicestershire (PCC) is a Data Controller for the purposes of the UK GDPR and Data Protection Act 2018. In the discharge of his statutory functions it is necessitous for personal data to be collected from data subjects.

The PCC, in pursuance of his statutory functions, receives and responds to correspondence from members of the public, and receives complaints about the Chief Constable, Leicestershire Police, himself and others. This means that he will receive and process personal data relating to these data subjects. In some instances, in order to respond to correspondents and deal with complaints, the Office of the Police and Crime Commissioner (OPCC) will need to pass that personal data on to a third party, such as the Chief Constable of Leicestershire Police, in order to obtain information to inform a response to the issue being raised or to ensure that the data is received by the most appropriate agency.

Where the PCC has a statutory obligation to share the information (required by law) or this is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller, this data will be shared and you will be advised of the actions taken (provided it is appropriate to do so). Where there is no other lawful basis to share the data but the OPCC would still like to share the information, they will seek your consent (explicit for special categories of personal data or data relating to criminal offences/convictions). A written record is preferred (email or letter) as this provides a clear audit trail, however the OPCC will also record consent (including explicit) given orally

If you wish to withdraw your consent at any time, please contact the OPCC using the details to advise them of this.

The OPCC has adopted a Data Protection Policy which sets out his approach to handling personal data. It is available through the PCC's website, or alternatively a copy may be requested by contacting the PCC at the address below.

As a data subject, you have the following rights under the UK GDPR and Data Protection Act 2018:

- The right to informed about the collection and use of your personal data;

- The right of access to your personal data;
- The right to require a controller to rectify errors in their personal data;
- The right to require a controller to delete your personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of your personal data;
- The right to transfer your personal data between controllers where appropriate;
- The right to object to the processing of your data in certain circumstances; and
- The right not to be evaluated on the basis of automated processing.

These rights are explored in more detail in the OPCC's Data Protection Policy.

The contact details for the PCC are:

Address –	Office of the Police and Crime Commissioner for Leicestershire
	Police Headquarters
	St Johns
	Enderby, Leicester
	LE19 2BX
Telephone –	0116 2298980
Email –	OPCC@leics.police.uk

Appendix C

For use with Contacts

The Police and Crime Commissioner for Leicestershire (PCC) is a Data Controller for the purposes of the UK GDPR and Data Protection Act 2018. In the discharge of his statutory functions it is necessitous for personal data to be collected from data subjects.

The PCC, in pursuance of his statutory functions, collects the personal data of data subjects with whom he liaises for the purposes of governance, dissemination of information, public and business meetings, surveys and consultations.

The PCC seeks explicit consent from such data subjects to process their personal data as above. A written record is preferred (email or letter) as this provides a clear audit trail, however the OPCC will also record consent given orally.

If you wish to withdraw your consent at any time, please contact the OPCC to advise them of this.

Your personal data will only be reasonably used for the purposes of the PCC discharging his statutory functions. The OPCC has adopted a Data Protection Policy which sets out his approach to handling personal data. It is available through the PCC's website, or alternatively a copy may be requested by contacting the PCC at the address below.

A data subject has the following rights under the UK GDPR and Data Protection Act 2018:

- The right of access to their personal data;
- The right to require a controller to rectify errors in their personal data;
- The right to require a controller to delete their personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of their personal data;
- The right to transfer their personal data between controllers where appropriate;
- The right to object to the processing of their data in certain circumstances; and
- The right not to be evaluated on the basis of automated processing.

These rights are explored in more detail in the OPCC's Data Protection Policy.

The contact details for the PCC are:

Address –	Office of the Police and Crime Commissioner for Leicestershire
	Police Headquarters
	St Johns
	Enderby, Leicester
	LE19 2BX
Telephone –	0116 2298980
Email –	OPCC@leics.police.uk

Appendix D

Table illustrating the lawful bases used by the OPCC

Before processing personal data, the OPCC must firstly determine the lawful basis for the processing – the PCC has both 'legal obligations' and is a public authority which carries out 'tasks in the public interest' as set out by law (as well, as being able to use 'vital interests' and 'contract') – and so 'consent' is often not the most appropriate basis for processing.

Under Article 6 of the UK GDPR and Data Protection Act 2018, the PCC may process personal data for the following reasons:

Lawful basis	Example	Action by OPCC
• Is the processing necessary for the performance of a **contract** with the data subject, in order to assist you with your desire to work with the OPCC?	• Payroll and benefits management. • Recruitment. • Pension administration. • Procurement.	• Data subject to be advised of how the data will be processed by the OPCC and/or Force via a privacy notice.
• Is there a **legal obligation** to share the data (to comply with an express requirement of the law)?	• Management of Complaints Appeals. • Safeguarding matters. • Holding the Chief Constable and his staff/officers to account. • Issuing the Police and Crime Plan. • Securing an efficient and effective police force for the area. • Setting the Force budget and determining the precept. • Bringing together community safety and criminal justice partners, ensuring local priorities are joined up. • Promoting and facilitating partnership working arrangements.	• Data subject to be advised of the legal (statutory) requirement of the OPCC to process the personal data. • OPCC may also be obliged to share data with the Force to progress the matter and the data subject should be informed of this in order to meet the OPCC's requirements for transparency.

Lawful basis	Example	Action by OPCC
	• Co-operative working with the police area • Commissioning local victim support services. • Funding crime prevention services.	
• Is the processing necessary to protect the **vital interests** of the data subject or another individual?	• Correspondence giving rise to 'threat to life' concerns for the data subject or another individual.	• Share data immediately with the relevant agencies – advise data subject/s only if appropriate to do so.
• Is the processing necessary in the performance of a **task carried out in the public interest** by the OPCC which is laid down in law?	• Engagement with the public at events, through surveys, in response to correspondence etc. • General communication or correspondence with the public. • Dealing with potentially 'misdirected' contact (i.e. that is more appropriately dealt with elsewhere) – examples and actions as given below. N.B. any information sharing should be considered on a case-by-case basis – this table is intended as a guide for potential lawful bases.	• OPCC to consider whether there is a lawful basis for the processing the data in the first instance, and then if there is a lawful basis to share the information elsewhere if there is a perceived requirement for sharing with the Force or other agencies. • If no other lawful basis for sharing the data outside of the OPCC identified, consent (explicit where it relates to special category or criminal offence data) must be sought from the data subject prior to sharing.
	• Complaints re policing that have not been to Professional Standards Dept.	• Will be shared with the Force PSD section to enable to the allegation to be fully investigated (this is part of public task in the public interest and statutory duty to hold the Chief and his staff to account).

Lawful basis	Example	Action by OPCC
		• The data subject must be advised that this is the course of action and that their information has been shared with the Force and the reasons for this.
	• Complaints re the lack of update / contact / communication following an incident or crime.	• Liaison between the OPCC and Force Liaison Officer to resolve the issue. • OPCC will provide an update to the data subject re the actions taken and will require the OIC or Police Liaison Officer to make contact re the incident or crime.
	• Issues that relate to other agencies, e.g. local authorities, fire service.	• Correspondent should be directed to contact the appropriate agency. • The query may be shared with the appropriate agency using consent (explicit if special category or criminal offence/conviction data) – rarely would there be a lawful basis to share with another agency under any other lawful basis other than consent.
	• Correspondence that relates to operational policing issues.	• This will be sent to the Force as this this links into the OPCC statutory obligations to work cooperatively with the police area for crime and disorder, and also in their obligations to secure and efficient and effective police force for the area. • The data subject must be advised that this is the course of action and that their information has been shared with the Force and the reasons for this.
If the none of the above lawful bases apply		
• Does the data subject **consent** to the processing of the data?	• Collection and publication of photographs for marketing purposes.	• Consent must be recorded – who consented to what, and when. • Data subject should be advised how to withdraw their consent.

Under Article 9 of the UK GDPR and Data Protection Act 2018, the PCC may process special categories of personal data[1] for the following reasons:

Lawful basis	Example	Action by OPCC
• Is the processing necessary for the purposes of **employment and social security and social protection law** and providing for appropriate safeguards for the fundamental rights and the interests of you, the data subject?	• Payroll and benefits management.	• Data subject to be advised of how the data will be processed by the OPCC and/or Force via a privacy notice.
• Is the processing necessary to protect the **vital interests** of the data subject or another individual?	• Correspondence giving rise to 'threat to life' concerns for the data subject or another individual.	• Share data immediately with the relevant agencies – advise data subject if appropriate to do so.
• Is the personal data already in the **public domain**?	• OPCC responding to an incident already released by the media or the Force.	• Data subject does not need to be contacted for consent or with a privacy notice provided that the information is only that which is already in the public domain.

[1] Special categories of personal data, as defined within the GDPR, includes: racial or ethnic origin, political opinions, religious or philosophical beliefs, health, sex life or sexual orientation, or trade union membership, and genetic data and biometric data – previously referred to as sensitive data.

Lawful basis	Example	Action by OPCC
• Is the processing **substantially in the public interest** (with a basis in law)? *(has the Public Interest Test been carried out?)*	• Statutory and government purposes. • Administration of justice and parliamentary purposes. • Equality of opportunity or treatment. • Racial and ethnic diversity at senior levels. • Preventing or detecting unlawful acts. • Protecting the public. • Regulatory requirements. • Preventing fraud. • Support for individuals with a particular disability or medical condition. • Safeguarding of children and individuals at risk. • Safeguarding of economic well-being of certain individuals. N.B. See Schedule 1 of the DPA 2018 for a comprehensive list of the substantial public interest conditions.	• OPCC must identify which of these conditions appears to most closely reflect the purpose for the intended processing – this will require the OPCC to refer to the detailed provisions for each condition in the legislation itself to make sure you can demonstrate it applies. • For some of these conditions, the substantial public interest element is built in. For others, the OPCC need to be able to demonstrate that the specific processing is "necessary for reasons of substantial public interest", on a case-by-case basis. • For some of the conditions, the OPCC also need to justify why they cannot give individuals a choice and get explicit consent for the processing. • In many cases, the OPCC must have an 'appropriate policy document' in place to process the data – although there are exemptions for disclosing data to relevant authorities. • As with other sharing – the OPCC should be transparent about any data that is shared (unless this would put someone in danger or frustrate the purpose for the sharing e.g. part of an investigation). N.B. See the legislation and ICO guidance for further detail.
• Is the processing part of a **legal claim or judicial act**?	• Criminal investigation. • Civil claim against the Force in which the OPCC has been involved.	• May be appropriate or a requirement to share data with Leicestershire Police. • As with other sharing – the OPCC should be transparent about any data that is shared (unless this would put someone in danger or frustrate the purpose for the sharing e.g. part of an investigation).
If the none of the above lawful bases apply		

Lawful basis	Example	Action by OPCC
• Does the data subject **explicitly consent** to the processing?	• Correspondence re case – sent by local MP, family member, friend etc. on behalf of the data subject.	• Consent must be fully recorded (must include the 'script' for consent).

Article 10 of the UK GDPR and Data Protection Act 2018 – processing of criminal convictions or offences:

- To process personal data about criminal offences or convictions the OPCC must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
- The Data Protection Act 2018 deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- See the legislation and ICO guidance for more detail about this type of processing – it is unlikely this will concern the OPCC to any great extent.