



**POLICE & CRIME
COMMISSIONER
for Leicestershire**

Your voice in Leicester,
Leicestershire & Rutland

Privacy Notice

Contact details

Address –	Office of the Police and Crime Commissioner for Leicestershire Police Headquarters St Johns Enderby, Leicester LE19 2BX
Telephone –	0116 2298980
Email –	police.commissioner@leics.pcc.pnn.gov.uk
Twitter –	@LeicsPCC
Facebook –	www.facebook.com/LeicsPCC

Introduction

The General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA '18), replaced the previous Data Protection Act 1998. These laws give you more rights over how your personal data is used, whilst also imposing greater obligations on the organisations holding and processing your personal data.

One of the key rights enshrined in the legislation is a right to be informed, which means that the Office of the Police and Crime Commissioner (OPCC) must give you detailed information about the ways in which we use, share and store your personal information.

We may need to make changes to our Privacy Notice from time to time, so please continue to check our website for updates. If there are important changes that affect the way we handle your personal data we will contact you directly, in compliance with the requirements of the legislation.

Who are we?

We are the Office of the Police & Crime Commissioner for Leicester, Leicestershire and Rutland (the OPCC). In accordance with the GDPR and DPA '18, the Police and Crime Commissioner's

(PCC) Chief Executive Officer (CEO) is registered as a Data Controller with the Information Commissioner's Office (ICO).

The PCC takes the responsibility for handling personal data very seriously; we take great care to ensure that all personal data is handled in accordance with the law in order to have the public's trust and confidence in the PCC and the OPCC.

This Privacy Notice will explain:

- How we collect, store, use, disclose (pass on), retain and destroy personal data;
- The steps we take to ensure that that your personal data is kept securely; and
- Your rights regarding your personal data held by the OPCC.

Personal data – what is it?

Personal data is any information about a living individual which allows them to be identified from that data (for example a name, photographs, video, email or personal address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual. The processing of personal data in the United Kingdom is governed by the GDPR, the DPA '18 and other key legislation such as the Human Rights Act 1998. The GDPR is the prevailing legislation for the processing of personal data by the OPCC as this covers 'general processing' rather than processing for law enforcement purposes.

The role of the Data Protection Officer

In accordance with the legislation the OPCC have appointed a Data Protection Officer (DPO) to advise on all data protection compliance matters, and to ensure that your individual rights are upheld.

In order to be transparent, members of the public and organisations can contact our DPO directly to discuss any data protection issues or concerns that they may have.

Our current Data Protection Officer is Steven Morris, Head of Information Management and his contact details are:

Address – Information Management
Leicestershire Police Headquarters
St Johns
Enderby, Leicester
LE19 2BX

Telephone – 0116 248 5222

Email – DPO@leicestershire.pnn.police.uk

What data do the OPCC collect and process?

In order to carry out our functions the OPCC may collect personal data about you which includes (but is not limited to) the following:

- 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.

Which legislation does the PCC's main statutory functions derive from?

- Police and Social Responsibility Act 2011
- Police Act 1996
- The Accounts and Audit Regulations 2011
- Local Government & Housing Act 1989 (S155)
- Local Government & Finance Act 1988 Sec 112 and 114
- Local Authorities (Goods & Services) Act 1970
- Elected Local Policing Bodies (Specified Information Order 2011 and amendment order 2012, S1 2012 / 2479)
- Police Pension Fund Regulations 2007
- Police Pensions Act 1976
- Freedom of Information Act 2000
- Police Reform Act 2002
- Employment Rights Act 1996
- The Equality Act 2010

What role and services do the PCC provide?

- Communication from and to members of the public;

- Management of Freedom of Information requests;
- Management of complaints;
- Management of public relations, journalism, advertising and media;
- Vetting;
- Commissioning Services;
- Management of finance;
- Internal review, accounting and auditing;
- Training;
- Property management;
- Insurance management;
- Vehicle and transport management;
- Payroll and benefits management;
- Management of information technology systems;
- Recruitment;
- Sports and recreation;
- Procurement;
- Planning;
- Security;
- Performance management;
- Legal services;
- Health and safety management;
- HR management;
- Information provision;
- Licensing and registration;
- Pensioner administration;
- Staff administration, occupational health and welfare; and
- Research, including surveys.

What is the lawful basis for processing your personal data?

Under Article 6 of the GDPR, the PCC may process personal data for the following reasons:

- Where you have given **consent** to provide us with the information;
- For the performance of a **contract** with you, the data subject, in order to assist you with your desire to work with the Police and Crime Commissioner;
- Where there is a **legal obligation** to do so (to comply with the law);
- Where the processing is necessary to protect the **vital interests** of the data subject or another individual; and/or
- Where the processing is necessary in the performance of a **task carried out in the public interest** which is laid down in law.

Under Article 9 of the GDPR, the PCC may process special categories of personal data¹ for the following reasons:

- Where you have given **explicit consent** to the processing;
- Processing is necessary for the purposes of carrying out obligations and exercising specific rights of the Data Controller – the PCC – or of you, the Data Subject in the field 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;
- Processing is necessary to protect **the vital interests** of you as the data subject, or of another natural person where you the data subject is physically or legally incapable of giving consent;
- Processing relates to personal data which is already in the **public domain** by you the data subject;
- Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity; and/or
- Processing is necessary for reasons of **substantial public interest**.

What is meant by ‘consent’?

The GDPR sets a high standard for consent – this means that organisations such as the OPCC must offer individuals real choice and control over their personal data where consent is the lawful basis for processing. Much of the data processed by the OPCC uses consent as the lawful basis, and the OPCC recognises that managing this is essential for accountable compliance with Data Protection legislation, and also for building trust and confidence with the public.

In order to be valid, consent must be:

- **Clear and concise** – explicit consent requires a very clear and specific statement of consent, clear plain language must be used and the request should be separate from any terms and conditions;
- **Freely given** – this cannot be a precondition for a service – public authorities and employers must take extra care to show that consent is freely given, and should avoid over-reliance on consent;
- **Evidenced** – a record should be kept re who, when, how and what you told people;
- **Reviewed** – periodically or if there is an intention to change the processing;
- **Granular** – this should be specific to the purpose – different purposes require separate consent, and vague or blanket consent is not appropriate;

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

- **A positive opt-in** – pre-ticked boxes or any other form of default consent are not permitted;
- **Able to be withdrawn** – it should be as easy to withdraw consent as it is to give it – if this is not the case, it is unlikely to be the appropriate lawful basis.

If you have given consent for the OPCC to process your data and you have changed your mind – please make contact with the OPCC via the details at the top of this Privacy Notice to advise that you wish to withdraw your consent.

How do the OPCC get the personal data and why do they have it?

Most of the personal data the OPCC process is provided to us directly from you (the data subject) for one of the following reasons:

Source of the personal data	Data type	Lawful basis
Persons making an enquiry or complaint	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Made public by the data subject • Legal claims or judicial acts
Individuals themselves	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Made public by the data subject • Legal claims or judicial acts
Relatives, guardians or other persons associated with the individual	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Made public by the data subject • Legal claims or judicial acts
Other Police and Crime Commissioners	Personal data	<ul style="list-style-type: none"> • Public task • Legal obligation
Leicestershire Police	Personal data, special category data, criminal offence data	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Vital interests • Legal claims or judicial acts
HM Revenue and Customs (HMRC)	Personal data	<ul style="list-style-type: none"> • Contract • Legal obligation • Public task
International law enforcement agencies and bodies	Personal data	<ul style="list-style-type: none"> • Consent (explicit for special category data)

		<ul style="list-style-type: none"> • Legal obligation • Public task • Vital interests
Legal representatives	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Local Authority and Parliamentary representatives	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Partner agencies involved in crime and disorder strategies	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public Task
Private sector organisations and people working with the Police and PCC	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task • Contract
Voluntary sector organisations	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task • Contract
Approved organisations and people working with the Police and PCC	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task • Contract
The Independent Office for Police Conduct (IOPC)	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS)	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Auditors	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Central government, governmental agencies and departments	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Local government	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Emergency services	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Vital interests
Current, past or prospective employers of an individual	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Explicit consent • Employment, social security and social protection
Healthcare, social and welfare advisors or practitioners	Personal data, (potentially also special category data, criminal offence data)	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task • Vital interests
Education, training establishments and examining bodies	Personal data	<ul style="list-style-type: none"> • Consent • Contract
Business associates and other professional advisors	Personal data	<ul style="list-style-type: none"> • Consent • Contract
Employees and agents of the Police	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task

Suppliers, providers of goods and services	Personal data	<ul style="list-style-type: none"> • Contract
Financial organisations and advisors	Personal data	<ul style="list-style-type: none"> • Contract
Credit reference agencies	Personal data	<ul style="list-style-type: none"> • Explicit consent • Contract
Survey and research organisations	Personal data (potentially also special category or criminal offence data)	<ul style="list-style-type: none"> • Consent (potentially explicit depending on content) • Public task
Trade, employer associations and professional bodies	Personal data and special category data	<ul style="list-style-type: none"> • Explicit consent
Voluntary and charitable organisations	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
The media	Personal data (potentially also special category or criminal offence data)	<ul style="list-style-type: none"> • Public task • Reasons of substantial public interest (with a basis in law)
Data Processors working on behalf of the PCC	Personal data	<ul style="list-style-type: none"> • Contract
Members of Parliament	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
Commissioned service providers	Personal data	<ul style="list-style-type: none"> • Contract
The PCC may also obtain personal information from other sources such as internal correspondence	Personal data, special category data, criminal offence data	<ul style="list-style-type: none"> • Consent (explicit for special category data) • Legal obligation • Public task
Ombudsmen and regulatory authorities	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task
The Information Commissioner's Office	Personal data	<ul style="list-style-type: none"> • Legal obligation • Public task

Our Data Protection Obligations

The OPCC is required to comply with Data Protection Law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent manner;
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have told you about and limited only to those purposes;
- Be accurate and up-to-date;
- Kept only as long as is necessary to carry out our functions; and
- Storing your personal data in a secure manner and ensuring its secure destruction when it is no longer necessary to process your personal data.

For more information on the data protection legislation please visit the ICO website which can be found here www.ico.org.uk

How do we use your personal data?

We know that your personal data belongs to you and not us. That's why when you, or a third party share your personal information with the OPCC, we make sure that we keep it private and safe. Our main aim in gathering your personal information is to provide you with a customised service. If you input your details into our 'Contact Us' section, we use your personal information in order that we can contact you and respond to any questions and needs that you may have. We use your personal information so that we can carry out your requests or to follow up complaints you have made.

We may also use aggregate personal information and statistics for the purposes of monitoring website usage in order to help us develop the website and our services and may provide such aggregate personal information to third parties. These statistics will not include any data that can be used to identify any individual. If, at some time in the future, we wish to use your personal data in ways other than those set out in this privacy notice, then we will notify you about this and seek your permission to do so.

When will we share your personal data?

In order to carry out the role and duties of the OPCC we may disclose personal data outside of the OPCC. This may include disclosures to the Police and other law enforcement agencies, other PCCs, partner agencies working on crime reduction initiatives, partners in the Criminal Justice arena, Victim Support and to bodies or individuals working on our behalf such as IT contractors or survey organisations.

Where appropriate and required to do so, the OPCC may share your information with Leicestershire Police in order to resolve any complaints or queries that you have raised with us directly, or to facilitate and support the PCC's role and remit, and to deliver statutory functions.

We may also engage the services of commercial companies to store and manage your information on our behalf. Where we have these arrangements, there is always a contract, memorandum of understanding or information sharing agreement in place to ensure the requirements of the data protection legislation are met. The PCC may also disclose to other bodies (including the Police) or other individuals where necessary to prevent harm to individuals.

Information will only be shared with other agencies where there is a clear legal basis for doing so and this will predominantly be undertaken with your consent. Disclosures of personal information will only ever be made on a case-by-case basis, using the personal information appropriate to a specific purpose and circumstances, and with necessary controls in place.

We do not currently envisage our wishing to transfer personal information about you outside of the European Economic Area, but in the unlikely event we should wish to do so in future, we will only do so to the extent that it is permitted under all privacy and communications legislation applicable within the United Kingdom. Of course if we need your specific and express consent to do this, we will obtain it before transferring any personal information. In all cases, any use of your personal information by the OPCC will comply with this privacy policy.

How long do we keep your personal data?

Personal data will be kept in line with our Retention Policy which can be found on our website. We keep your personal information as long as is necessary for the particular purpose or purposes for which it is held. This varies for different types of personal data and documents. Personal information is retained, reviewed and deleted in accordance with agreed retention times which are subject to review.

How do we keep your information secure?

Your information is securely stored within a sectioned off part of the Leicestershire Police infrastructure. This is segregated from the Police systems and data, and **cannot** be accessed by the Force.

We are committed to ensuring that your personal data is safe. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information that we hold about you. These include:

- Secure work areas;
- Data protection and information security awareness for our staff;
- Appropriate policies and procedures;
- Access controls on relevant systems;
- Audit and monitoring;
- Encryption of personal data; and
- Testing, assessing and evaluating the effectiveness of technical security controls.

The internet is not a secure medium and the OPCC cannot absolutely guarantee the security of your personal information provided over the internet. However we have put in place various security measures as set out below. Our website and associated databases are protected by certified firewalls in order to protect your personal information from access by unauthorised persons and against unlawful processing. The website uses the latest technology with full backups. We also keep your personal information confidential. All outgoing and incoming emails are scanned for viruses.

Your rights and your personal data

You have more control over your data than ever before and this includes various rights within the law. The GDPR supports your right to have your privacy respected and your data protected. It is designed to give you confidence that the personal information we hold about you is accurate, up-to-date and well managed, and to give you easier access to that information if you wish to check or change it.

These requests (associated to the rights detailed below) can be made in **writing**, by **phone** or by **email**. Please contact the **Data Protection Officer** (using the contact details shown above) with the following information:

- Your name and contact details;
- Any information used by the organisation which would distinguish you from others with the same name (reference numbers, date of birth etc.); and
- Specific details of the information you are referring to, together with any relevant dates – this should help the OPCC deal with your request more quickly.

Please be aware that you may be asked to provide further information so that your identity can be confirmed.

Right to be Informed

You have the right to be informed about the collection and use of your personal data. We will endeavour to provide information which is concise, transparent and easy to understand. We must provide you with information including:

- Our purposes for processing your personal data;
- How long we keep your personal data (i.e. the retention periods);
- Who it will be shared with.

We call this 'privacy information' and this is within this Privacy Notice. We must provide privacy information to you at the time we collect your personal data, this is why the PCC's email address has an automatic acknowledgement and contains a link to this Privacy Notice. If we obtain personal data from other sources, e.g. third-parties, then we must provide you with privacy information within a reasonable period of obtaining the data and no later than one month. There are a few circumstances in which we do not need to provide you with privacy information, such as if you already have the information or if it would involve a disproportionate effort to provide it to you.

All information provided to you by the OPCC should be concise, transparent, intelligible, easily accessible, and it must be in clear and plain language. We provide privacy information to people at different times and in a number of formats, such as in an email reply, on the PCC's website and on our telephone recorded message. If you have any feedback on how effective the delivery of our privacy information is then we would welcome your comments.

We regularly review, and where necessary, update our privacy information. If we have any new uses of your personal data then we will bring it to your attention before we start the processing. Getting the 'right to be informed' correct helps us comply with other aspects of the GDPR and to build trust with you. Getting it wrong means that we may be fined and can also lead to reputational damage for us. There may be occasions when it is necessary and proportionate to restrict the provision of information in the context of law enforcement.

Right of Access

The most commonly exercised right is that used by individuals to obtain a copy (subject to exemptions) of their personal information processed by the OPCC – commonly referred to as a Subject Access Request (SAR). Making a SAR is free of charge and can be requested by contacting the DPO.

If the request is considered excessive or for any further copies requested by you, we will either charge a reasonable fee based on our administration costs or we may refuse the request and give reasons for doing so. We will always discuss this with you and explain the reasons for any charges. We will reply without delay and will use all reasonable measures to verify your identity if you request access to your personal information. We will send a final response within one month of receiving the request.

Right to Rectification

We want to make sure that your personal information is accurate and up-to-date.

You have the right to ask us for the rectification of inaccurate personal information concerning you. Taking into account our purposes for the holding and processing of your data, you have the right to have incomplete personal information completed, including any supplementary statement you wish to make for us to hold.

Right of Erasure ('Right to be forgotten')

You have the right to ask us to erase your personal information and we will do this without undue delay where your personal data is no longer necessary for the purpose that we were collecting and holding or processing it. This is subject to compliance with any legal obligation for us. We will also inform any third-party if we have shared your personal information, to inform them of the erasure.

Right to Restriction of Processing

You have the right to ask us for a restriction on the processing of your personal information if it is inaccurate, unlawful or we no longer need your personal information, but we are required by you to store the data regarding a legal claim, or you object to our processing and whilst this is reviewed. We can continue to store your personal information, but we will be restricted to the ways that we can use it.

Right to Data Portability

You have more access and control over what happens to your personal information. You have the right to receive your personal data that you have provided to us and you have the right to directly transmit your personal data to another Data Controller (an organisation that controls personal information) without undue delay from us. This is only where you have given consent or where there is a contract for us to handle your personal information, and the processing that we do is carried out in an automated way. This doesn't apply where we are acting under official authority or in the public interest.

Right to Object

You have the right to object to, at any time (on grounds relating to your particular situation), the processing of your personal data where the processing is necessary for the performance of a task carried out in the public interest or official authority for us; or provides the legal foundation of legitimate interests of us. We will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Automated Decision-Making, including Profiling

Please note that we do not use automated decision-making or profiling. However, for completeness we want to confirm this general right.

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you. This right doesn't apply if it is necessary for entering into, or performance of, a contract between you and us as the Data Controller; or it is authorised by a Union or Member State law to which our Data Controller is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or it is based on your explicit consent.

Right to request the Information Commissioner to assess our Processing

You can ask the ICO to make an assessment if you believe that you have been adversely affected by the handling of your personal information by us, or if you believe that we have not complied with the requirements of Data Protection Law. You can directly contact the ICO using the contact details below.

Generally if you have any concerns about the way that your personal information is handled by us or the lawfulness, fairness or quality (accuracy, relevance, non-excessiveness) of your personal information, then you are welcome to raise them with us in the first instance in order to allow us to try and address your concerns (see Contact Details).

The ICO is the independent regulator responsible for enforcing Data Protection regulations and can provide useful information about the requirements and your rights. ICO may be contacted in the following ways:

Post – The Information Commissioner's Office, Wycliffe House, Wilmslow, Cheshire, SK9 5AF

Telephone – 0303 123 1113 (local-rate) or 01625 545 745 if you prefer to use a national-rate number.

How do the OPCC use cookies?

Cookies are small text files that websites put on your computer or mobile device while you're browsing. The OPCC website uses cookies – please see the Cookie Policy on our website for details of how this is used.

Further Processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use. This will be provided prior to commencing the new processing and will set out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Monitoring

Subject to the law, we'll monitor or record and retain your telephone calls, texts, emails, social media posts and other communications in relation to your dealings with us.

We do this for regulatory compliance, self-regulatory practices, crime prevention and detection, to protect the security of our communications systems and procedures, to check for obscene or profane content, for quality control and staff training and when we need to see a record of what's been stated. We aim to communicate and correspond efficiently and effectively with you and to assist the role and remit of the PCC.

Changes to this notice

We keep this privacy notice under regular review and we will place any updates on the website

www.leics-pcc.police.uk