Police and Crime Commissioner for Derbyshire

Data Protection Policy

EXTERNAL POLICY

Control Sheet

Policy details

Policy Title	Derbyshire OPCC Data Protection Policy 2020
Responsible Officer	Head of Compliance
Security Classification	External
Disclosable under FOIA	Yes
Policy implementation date	July 2020
Next review date	December 2022 (Annually)

Revision details

Revision date	**Changes**
Draft version 1	Altered sub-headings MR
Final version	15 July 2020 MR
Reviewed	Changes in UK GDPR 11 May 2021 MR
Reviewed	Reviewed content changed Chief Executive wording in the policy to Interim Chief Operating Officer and updated the next review date – MR 06/12/2021.

Index list

Introduction

The Office of the Police and Crime Commissioner (OPCC) for Derbyshire is committed to ensuring that all staff undertake their legal duties in a manner that is compatible with the data protection principles.

The UK General Data Protection Regulations (GDPR) states that:

When processing personal data, the OPCC will be guided by the following principles:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Personal data shall be accurate and where necessary kept up to date

5. Personal date shall be kept in a form which permits identification of data subjects for no longer than necessary

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data

All data controllers have a responsibility to make sure they protect personal data and keep it secure. The OPCC will take action to ensure that data isn't unlawfully processed and to stop data being accidentally lost or destroyed. It is essential that all data is collected, used, stored and disposed of in ways that protect its confidentiality, integrity and availability.

The OPCC are committed to providing effective management of data and the safeguarding of personal data and is dedicated to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy is to assist the PCC and OPCC staff in processing personal data in line with the UK General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 by promoting good practice in all its operations. This policy also sets out the expected requirements for staff of the OPCC in relation to the processing of any personal data belonging to an OPCC contact (i.e. a data subject).

Scope

This policy deals with Personal data that is relevant to the day to day running of the Derbyshire OPCC. It covers information relating to those who contact the OPCC, whose personal data may be logged, held and processed. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This Policy also applies to all staff who work part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes volunteers, temporary employees and independent contractors and partners/partnership working at or for the OPCC.

Definitions

Children/Child

For the purpose of this policy means an individual under 18-years-old.

Consent

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

Individual/Data Subject

Any past or current person who contacts the OPCC. A member of the public, a Councillor, an MP.

Data Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of a Data Controller.

Data Protection Officer (DPO)

Meaning the OPCC's Data Protection Officer or staff member who is tasked with the role and responsibilities of a DPO.

Police and Crime Commissioner (PCC)

Means the Police and Crime Commissioner for Derbyshire.

Office of the Police and Crime Commissioner (OPCC)

Means the Derbyshire Officer of the Police and Crime Commissioner.

Information Commissioners Office (ICO)

The UK's independent body set up to uphold information rights.

Data Protection

The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

UK General Data Protection Regulations (GDPR)

The UK GDPR is the UK's post-Brexit version of the EU GDPR.

Data Protection Act 2018 (DPA)

The UK DPA (Data Protection Act) 2018 is a comprehensive, modern data protection law for the UK, which came into force on 25 May 2018

Environmental Information Regulations (EIR)

The Environmental Information Regulations 2004 provides public access to environmental information held by public authorities.

Relevant Data Protection Laws

Meaning the GDPR and the DPA 2018

Data Subject

The identified or identifiable natural person to which the data refers. An individual. A member of the public.

Employee/Staff

An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes volunteers, temporary employees and independent contractors and partners/partnership working at or for the OPCC.

Personal data

Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Information which relates to a living individual who can be identified from the data or from the data and other information which is possession of, or is likely to come into the possession of, the data controller. The information may be in either electronic or manual format.

Personal data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Process, Processed, Processing

Any operation performed on personal data. This may include collecting, recording, using or destroying data.

Profiling

Any form of automated processing of personal data where personal data is used to carry out analysis.

Third Party

An external organisation with which the OPCC conducts business.

Governance

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, the OPCC has appointed a Data Protection Officer (DPO).

The Data Controller is the Police and Crime Commissioner (PCC). The PCC has delegated day to day responsibility for data control to the OPCC's Interim Chief Operating Officer, who in turn has delegated this to the Head of Compliance who is also the OPCC's Data Protection Officer - DPO.

How does the OPCC handle personal information?

The OPCC will handle personal information in accordance with data protection laws and will ensure that all personal information is handled fairly and lawfully with appropriate justification. Personal information will only be used for lawful purposes and any personal information will be held securely on OPCC systems and accessed only by OPCC staff in accordance with their contract.

The OPCC will strive to ensure that any personal information processed is of the highest quality in terms of accuracy, relevance, adequacy, not excessive, kept as up to date as possible and is protected appropriately. Regularly reviews of the personal data processed will take place to ensure it is still required and that it is lawful for the OPCC to continue to retain it. Once personal data is no longer required then it will be securely destroyed.

Why the OPCC collects and processes personal data

The OPCC's lawful basis for processing information comes under the following categories:

- **Legitimate interest** – responding to queries, running of events, providing media statements and press releases

- **Consent** – passing information over to Derbyshire Police where this is appropriate
- **Contract** – issuing grants and commissioning services

- **Legal obligation** – dealing with complaints against the Chief Constable or members of OPCC staff, HR data and applications

- **Performance of a task** – any official functions that are set out in law, (mainly the Police Reform and Social Responsibility Act 2011) - ensuring an efficient and effective police force in Derbyshire, community safety and the prevention of crime.

For more information relating to Lawful Basis please see the ICO's guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

The OPCC uses the personal data of its contacts for the following broad purposes:

- Strategic planning;
- Holding the Chief Constable to account, including complaint handling;
- Partnership working;
- Appointment of OPCC statutory officers;
- Appointment, suspension and removal of Chief Constable;
- Information and engagement;
- Financial reasons;
- Maintaining our accounts and records;
- Promoting our services and activities;
- Carrying out research;
- Managing recruitment and volunteers.

The type of personal information the OPCC holds will vary depending upon the reason the data subject has made contact with the OPCC but may include;

- Name and address;
- Photograph, video and sound and visual images;
- Family data;
- Lifestyle data;

- Social circumstances;
- Education and training data;
- Employment data;
- Financial data;
- Goods or services provided data;
- Racial or ethnic origin;
- Political opinions;
- Religious or other beliefs of a similar nature,
- Trade union membership;
- Physical or mental health or condition;
- Sexual life; offences and alleged offences;
- Criminal proceedings;
- Outcomes and sentences;
- Cautions data;
- Criminal intelligence;
- Complaint data;
- Incident data;
- Civil litigation and accident data.

Data is collected via e-mail, telephone, in person, via letter or social media.

For more information regarding processing purposes please see the OPCC's Privacy Statement - https://www.derbyshire-pcc.gov.uk/Transparency/Privacy-Statement.aspx

Personal data will be collected only from the Data Subject unless one of the following applies:

- The nature of the purpose necessitates collection of the personal data from other persons or bodies.

- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If Personal data is collected from someone other than the data subject, the data subject will be informed of the collection unless one of the following applies:

- The data subject has received the required information by other means

- The information must remain confidential due to a professional secrecy obligation

- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification will occur promptly and no later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

How does the OPCC keep personal information safe?

The OPCC takes the security of all personal data very seriously and will comply with the relevant parts of data protection law relating to security. The OPCC adopts appropriate physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed to by virtue of human action or the physical or natural environment. The OPCC will ensure that appropriate policy, training, technical and procedural measures are in place.

Some of the personal data related security measures taken include, but are not limited to:

- ensuring all buildings are secure and protected by adequate physical means, (burglar alarms, access coded doors, lockable windows, CCTV);
- areas within the OPCC are restricted to OPCC staff and are only accessible by those holding the appropriate identification and have legitimate reasons for entry;
- any systems meet appropriate industry and government security standards;
- giving adequate training to staff regarding security of personal data;
- having lockable filing cabinets and desk drawers;
- having confidential waste bins;
- carryout data protection audits to test that privacy controls are working and are fit for purpose.

- protecting records/files held on computer with appropriate managed permissions to ensure access is restricted only to those who are entitled to access files;

- password protecting equipment.

- keeping paper files in locked cabinets, with access to keys limited to authorised staff;

- transmitting personal data electronically to secure e-mail addresses using password protection where necessary;

- ensuring all removable media (USB) are OPCC/Derbyshire Constabulary issued and are encrypted for security;

- using secure delivery methods such as “guaranteed delivery/recorded delivery” if sending personal data through the post;
- regularly backing up electronic files through OPCC/Derbyshire Constabulary IS systems;

- ensure all staff members have relevant and regular training regarding Data Protection, Security and Information Management and apply that training practically;

- auditing the above list to scrutinise and evaluate data protection compliance.

Information Security

Both the GDPR and the DPA contain the requirements for the security of personal information to include the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of the personal data.

Appropriate technical and organisational measures may include but are not limited to:

a) using and developing technological solutions to ensure compliance with the data protection legislation (data protection by design and default);

b) using physical measures to protect OPCC assets;

c) ensuring the reliability of any persons who have access to OPCC information;

d) report and investigate security breaches;

e) carryout audits;

f) use of confidential waste bins.

These obligations include the need to consider the nature of the information to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction or damage.

Good information security is also achieved through policy and procedural controls, details of which are documented in the Derbyshire Constabulary Information Security Policy which the OPCC follows as all technological and asset security is implemented and controlled by the Derbyshire Constabulary.

Access to Personal Data

Personal data from the OPCC systems will, in the first instance, only be disclosed to OPCC staff who require such information to carry out their official duties.

Any personal information held by the OPCC will be for the OPCC's use but may be approved to be disclosed to other organisations abiding by the relevant data protection laws.

Information Sharing

Any personal information he OPCC process may be shared with other organisations such as policing organisations (Derbyshire Constabulary), local authorities, other public services (NHS organisations) and ombudsmen and regulatory authorities (Information Commissioners Office ICO).

Personal information will only be shared when the OPCC are permitted to share it as required to do so by law or have your consent to do so as required by data protection law.

The OPCC does not pass personal data to other organisations for marketing purposes without your consent.

Your personal information may be processed by an external service provider acting on the OPCC's behalf to provide services however, any third party service provider will be controlled under contract and have to abide by the rules in the contract and detailed in this policy when processing personal data.

Information that is not for the OPCC

The OPCC may pass personal data through to the Derbyshire Police where it is deemed that the OPCC is not the appropriate authority to deal with the issues raised by a data subject. Where the appropriate authority may be another separate organisation the OPCC will communicate this to the data subject so that they can contact that organisation directly themselves. The OPCC will always send an acknowledgement response to the data subject detailing what action has been taken and a record of that response will be stored for audit purposes.

Where the data subject has contacted the OPCC and stipulates that they do not want Derbyshire Police's involvement, then consent will be sought before passing any personal details to them. There are two exceptions to this:

- Complaints – where the OPCC receives a compliant about a member of Derbyshire Police staff or Derbyshire Police processes then the OPCC are required by legislation to pass this onto Derbyshire Police to investigate;

- Concerns for welfare or safety – where the OPCC receives contact where there are concerns for the data subject, or another individuals, safety and well-being, the OPCC will pass this onto the Derbyshire Police for a safeguarding referral to be made.

For more information relating to consent please see the ICO's guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Data Quality

The OPCC will ensure, were possible, that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject.

The measures adopted by the OPCC to ensure data quality include but are not limited to:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification;

- Keeping personal data only for the period of time necessary to satisfy the permitted processing or applicable statutory retention period;

- The removal/deletion of personal data if in violation of any of the data protection principles or if the personal data is no longer required;

- Recording any changes to altered personal data for audit purposes.

Restriction of personal data, rather than deletion, insofar as:

- A law prohibits erasure;

- Erasure would impair the legitimate interests of the data subject;

- The data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect so restriction of the personal data is applied until a determination is made.

What is the OPCC's personal data breach process?

In the event of a personal data breach the OPCC will follow the OPCC's Personal Data Breach Policy and Incident Response Plan.

The Policy describes the process that must be followed if a personal data breach occurs.

This includes but is not limit to;

a) a breach process for staff to follow;

b) all near-misses and breaches to be recorded to aid with accountability;

c) referring certain breaches to the ICO within the statutory timescale of 72 hours;

d) ensuring lessons are learnt from breaches to avoid further breaches and to fully demonstrate that the OPCC is a learning organisation.

All OPCC staff have received training regarding data breaches and are fully committed to adhering to the OPCC's Personal Data Breach Policy and Incident Response Plan.

Individual Rights

Under the GDPR data subjects have certain rights.

These rights are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The OPCC will respect these rights and will follow the ICO's guidance on Individual Rights - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

The right to be informed

The right to be informed is an obligation to provide 'fair processing information' to a data subject, typically through a privacy notice. It emphasises the need for transparency over how personal data is processed.

The right of access

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

This is normally processed as a Subject Access Request (SAR).

For more information regarding SAR please see the OPCC's Access to Information Policy which is available on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

The right to rectification

Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete.

If the OPCC has disclosed the personal data in question to third parties, then they must be informed of the rectification where possible. The OPCC must also inform the data subject about the third parties to whom the data has been disclosed where appropriate.

The right to erasure

The right to erasure is also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable a data subject to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to restrict processing

Data subjects have a right to ‘block’ or suppress processing of their personal data.

When processing is restricted, the OPCC are permitted to store the personal data, but not further process it, just enough information about the individual should be kept to ensure that the restriction is respected in future.

The right to data portability

The right to data portability allows data subjects to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

It enables data subjects to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to object

Data subjects have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling

The GDPR provides safeguards for data subjects against the risk that a potentially damaging decision is taken without human intervention. If any decisions are based on solely automated decision making then the data subject can ask for a review to be done by a human to determine if the decision made by the automated process was correct or not.

Are Individual Rights absolute?

It is important to make clear that data subject’s rights are never absolute. If a data subject has exercised one or more of their rights by submitting an Individual Rights Request (IRR) to the OPCC it doesn’t mean the OPCC will conform and do as the data subject has requested, as there may well be conditions and exceptions to consider alongside the data subjects individual rights. For example, the OPCC may have a legal obligation as to why that personal data is processed or there might be contractual stipulations which override a data subject rights.

The OPCC will assess any data rights requests individually and will communicate with the data subject on any decisions or actions taken accordingly.

Consent

The OPCC will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the processing of their personal data, the OPCC is committed to seeking such consent.

Withdrawing Consent

Where a data subject has provided consent for the OPCC to process their personal data, they then also have a right to withdraw that consent at any time without any detriment to them.

Withdrawing consent given should be as easy to do as it was to give the consent in the first place and the OPCC will ensure that any withdrawal of consent is acted upon quickly.

Should a data subject wish to exercise their right to withdraw their consent, they should contact the OPCC using the contact details below.

Submitting an Individual Rights Request (IRR) to the OPCC

Data Subjects who wish to exercise any of the above-mentioned rights, need to submit an IRR to the OPCC using the details below. The OPCC will acknowledge all individual rights requests within 5 working days and will respond with the decision taken within one month unless the scale or complexity of the request makes that unachievable. However, if any time extension is needed then correspondence will be sent to the data subject confirm this. A time extension of a further two months can be applied.

For an IRR to be valid it must:

a) be in writing;

b) include a name and address for correspondence (email address is sufficient);

c) detail the personal information that there is concern over.

Requests should be sent via email to:

PCCOffice@Derbyshire.PNN.POLICE.uk

or by post to:

The Office of the Police and Crime Commissioner for Derbyshire
Butterley Hall
Ripley
Derbyshire
DE5 3RS

Or submitted via the online form on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Information-Request-Form.aspx

NOTE - Please ring – 0300 122 600 if any additional help with submitting an information request is needed.

If the data subject is unhappy with the OPCC's decision they receive regarding their IRR then they can ask for an internal review of that decision. The internal review is normally carried out under the same internal review process afforded to subject access requests (SAR).

For more information regarding the internal review process please see the OPCC's Access to Information Policy and on the OPCC's website – https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

For more information regarding individuals rights and how to submit a request please see the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

For more information regarding individuals right please see the ICO's website - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Privacy Statement

The OPCC is transparent about its personal data processing activities and this is further evidenced in the OPCC's Privacy Statement which is available on the website.

The OPCC will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data, this is normally done through directing the requester to the OPCC's Privacy Statement on the website but might also be sent out in hard copy to data subjects via the post.

For more information regarding the OPCC's privacy statement please see the website - https://www.derbyshire-pcc.gov.uk/Transparency/Privacy-Statement.aspx

Subject Access Request (SAR)

When the data subject requests a copy of their own personal information held by the OPCC this is known as a Subject Access Request (SAR), disclosure will be made unless one of the following apply:

- The data subject already has the information
- An exemption applies to the data

- Clarification of the request is asked for by the OPCC and no response is received by the data subject within a set timescale.

All requests relating to personal data will be processed by the OPCC free of charge unless the request is deemed to be unnecessary or excessive in nature in which case the data subject will be notified of any charges or determinations accordingly.

All SAR's will be considered in accordance with all applicable data protection laws and will be processed in line with the OPCC's Access to Information Policy.

For more information regarding the process of SAR's please see the OPCC's Access to Information Policy on the website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

For more information regarding SAR's please see the ICO's guidance on the website - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Interaction with the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR)

There will inevitably be a link between the UK General Data Protection Regulations (GDPR) the Data Protection Act (DPA), the Freedom of Information Act (FOIA) and the Environmental Information Regulations (EIR) as they are all legislations that are designed to help individuals gain information from public authorities.

When an individual submits a request for information the OPCC will assess which legislation the information falls under and will process the request in line with that legislation.

For more information regarding information requests please see the OPCC's Access to Information Policy on the OPCC's website – https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

Digital Marketing

As a general rule the OPCC will not send promotional or direct marketing material to a contact through digital channels such as mobile phones, email and the Internet, without first obtaining the individuals consent.

Any consent is recorded and stored for audit purposes and when sending marketing material to consenting individuals an opt-out option is available for them to alter their marketing and contact preferences accordingly.

Children

The OPCC does not specifically market itself towards or encourage contact directly with children (defined as those who are under 13). If personal data is collected with regard to a child, consent should be sought from the person who holds parental responsibility over the child or their carer.

For legal purposes, if there is a complaint or a concern for the welfare of a child, consent does not need to be sought.

If a child submits a SAR to the OPCC then there are specific processes the OPCC will follow to ensure that the child is mature enough to understand what they are requesting and if in doubt the person with parental responsibility or their carer will be notified.

For more information regarding SAR's submitted from children please see the OPCC's Access to Information Policy on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

Cookie Notice

The OPCC's website displays a cookie notice explaining what cookies are used when visiting the website.

Having a visible and effective cookie notice ensures that the OPCC takes a pro-active stance in ensuring that individuals are aware of how their personal data is process.

More information regarding cookies can also be found in the OPCC's Privacy Statement which is on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Privacy-Statement.aspx

Information Sharing Agreements (ISA's)

Information sharing agreements (ISA's) are agreements that set out the lawful basis for the use of personal data by the public sector, across traditional organisational boundaries, to achieve better policies and deliver better services.

The principle legislative instruments that provide powers to lawfully share information between the OPCC and Derbyshire Constabulary are the Reform and Social Responsibility Act 2011 and the Policing Protocol.

On the whole the OPCC does not share personal data outside of the above legislation and although the OPCC commission services they do not normally process any personal data relating to those services. If the OPCC needs to have access to personal data then an ISA will be drawn up accordingly. The Derbyshire Constabulary and the commissioned service provider/s will draw up an ISA so they can process personal data between themselves lawfully. However, the OPCC will audit that the services commissioned are fit for purpose by looking at output via anonymised data to assess areas like, take up rates and identify any concerning trends, this is part of the OPCC's monitoring role to ensure that public funds are being used effectively and efficiently.

Third Party Processing

Where processing of OPCC information is carried out by a third party on behalf of the OPCC then the Data Protection Officer (DPO) must be involved from the very start of the procurement process to ensure that the third party provides sufficient guarantees in respect of data protection law and the technical and organisational measures governing the processing to be undertaken. This means that appropriate contractual terms and conditions will be imposed on any third-party processor to ensure they act only on the instructions from the controller (OPCC) in regard to any processing of personal data.

Any processing of personal data by a third-party must be deemed necessary and approved by the OPCC's DPO. The DPO can help prepare terms and conditions for any contract requiring the processor to comply with obligations equivalent to what the OPCC would expect.

Data Protection by Design

The OPCC's current processes have been reviewed to ensure that all data protection requirements have been identified and addressed if required, data impact assessments (DPIA's) along with an equality impact assessment (EIA's) will be carried out for all new processes, systems and decisions that impact on individuals.

It is the responsibility of all OPCC staff to involve the OPCC's DPO when they are procuring, developing or altering any policies, systems or databases to ensure that data protection by design and default is embedded and a DPIA is carried out where necessary. The development of new systems provides an opportunity to build in data protection compliance at the time of the design by ensuring data protection is considered from the start of the project and provides security against any breaches of data protection law. The OPCC's DPO also then has a chance to raise any concerns and make challenges where necessary regarding data protection compliance before the processing commences.

Data Protection Impact Assessment

The ICO stipulates that there must be a completed data protection impact assessment (DPIA) for any personal data processing that is **likely to result in a high risk** to individuals. Where the potential for high risk personal data processing is identified, the OPCC will undertake a DPIA to assess and mitigate any risks. Any risks that cannot be mitigated will be referred through to the ICO for a final determination before any processing commences.

There are particular circumstances where a DPIA is required which include:

- Systematic and extensive profiling of data subjects or automated decision-making to make significant decisions
- Processing of special category personal data or criminal offence data on a large scale;
- Systematically monitoring of a publicly accessible place on a large scale.

In addition, the ICO has advised that a DPIA should always be carried out where the processing involves any of the following:

- The use of innovative technology;
- The use of profiling, automated decision making or special category data to help to make decisions on someone's access to a service, opportunity or benefit;
- Carrying out profiling on a large scale;
- Processing of biometric or genetic data;
- Combining, comparing or matching data from multiple sources;
- Processing of personal data without providing a privacy notice directly to the data subject;
- Processing personal data in a way which involves tracking individuals online or offline location or behaviour;
- Processing of children's data for profiling or automated decision-making or for marketing purposes, or offering online services directly to them;

- Processing of personal data which could result in a risk of physical harm in the event of a security breach.

The ICO also advises that the OPCC should consider carrying out a DPIA if the processing involves any of the following:

- evaluating and scoring;
- automated decision making with significant effects;

  systematic processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions.
- processing involving preventing data subjects from exercising a right or using a service or contract.

If it is decided that a DPIA is not carried out then the reasons for that decision will be clearly document.

All DPIA's will be carried out by the OPCC's DPO and will be stored for audit and accountability purposes.

The OPCC will follow the ICO guidance relating to DPIA's.

For more information regarding DPIA's please see the ICO's website - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Data Retention

To ensure fair processing, personal data will not be retained by the OPCC for longer than necessary in relation to the purposes for which it was originally collected, or for which it may be further processed.

The length of time for which the OPCC needs to retain personal data is set out in the OPCC's Retention Policy, available on the OPCC's website.

For more information relating to retention timescales please see the OPCC's Retention Policy on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Document-Library/Transparency/Public-Information/Policies-Procedures-and-Protocols/23-Retention-Policy.pdf

Audit and Monitoring

In order to ensure compliance with the GDPR, DPA 2018 and any other relevant legislations, the OPCC is obliged to have an audit regime to measure performance to comply with legislative requirements and thereby help in evidencing the accountability principle under the GDPR.

A Strategic Audit Plan has been developed to assess the effectiveness of all data protection controls and to monitor the OPCC's compliance with the ICO and any other regulatory bodies. The purpose of an audit is to provide a systematic examination to determine whether activities involving data protection compliance and the processing of OPCC data are carried out in accordance with the organisation's policies and relevant data protection law.

The Strategic Audit Plan is carried out annually and a log of outcomes and recommendations is produced, actioned and shared with relevant parties accordingly.

Strategic Audit Plan

The Strategic Audit Plan will review the following but is not limited to:

- personal data collection and processing – Personal Data Asset Register (PDAR);
- processing of Individual Rights Requests (IRR);
- processing of Subject Access Requests (SAR);
- privacy notice;
- policy reviews;
- staff training and awareness;
- security protocols;
- personal data transfers;
- data retention;
- third party processing;
- personal data sharing.

This list can change according to any new or emerging identified areas of data protection risk and threat.

All reviews are carried out annually as per the ICO's advice and documented actions from those reviews will be stored to aid with transparency, audit and accountability purposes.

Misconduct

The OPCC recognises the sensitivity regarding the processing of personal data. Any processing of OPCC information for any unauthorised, private purpose or any other non – work related purpose is prohibited. Deliberate unauthorised processing or interference with any computer or ancillary equipment or data, soft or hard copy, is also strictly prohibited. Any instances of unauthorised processing will be managed under the OPCC's Staff Code of Conduct and could lead to disciplinary proceedings.

Any such concerns should be reported to the OPCC's DPO immediately for further investigation using the contact details below.

Register of Fee Payers

The independent national body for the upholding of data protection legislation is the Information Commissioner's Office (ICO).

The Data Protection (Charges and Information) Regulations 2018 requires every organisation that processes personal information to pay a fee to the ICO, unless they are exempt.

The ICO publishes a register of the fee-paying organisations on their website at https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/ the Office of the Police and Crime Commissioner (OPCC) for Derbyshire is listed on that register.

The register serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the GDPR and DPA 2018 that the public can enquire which organisations are registered with the ICO and what type of processing of personal data they undertake.

Complaints regarding Data Protection

If a data subject is concerned about the way the OPCC have handled their personal information then the best course of action would be to contact the OPCC (contact details below) to discuss the situation in more detail. The OPCC's DPO will investigate the matter and will respond to the data subject accordingly, this is normally carried out under the same internal review process afforded to subject access requests (SAR).

For more information regarding the internal review process please see the OPCC's Access to Information Policy and on the OPCC's website – https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

Data Protection Officer/OPCC contact details

E-mail: PCCOffice@Derbyshire.PNN.Police.UK

By post:
Data Protection Officer for the Police and Crime Commissioner
Office for Derbyshire
Butterley Hall
Ripley
Derbyshire
DE5 3RS

By phone:
0300 122 6003

Right to lodge a complaint with the ICO

A data subject can complain to the Information Commissioners Office (ICO) if they are unhappy with the internal review that has taken place or any aspect of how the OPCC uses their personal data.

A data subject can contact the ICO using the following contact details:

Address:

Information Commissioner's Office,

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire

SK9 5AF

E-mail: casework@ico.org.uk

Tel: 0303 123 1113

Website: https://ico.org.uk/

Equality

This policy has been through an equality impact assessment by the OPCC.

Questions

Any questions regarding this Policy should be referred through to the OPCC's DPO (contact details above).

Linked Policies

This Policy also links in with the OPCC's Access to Information Policy is available on the OPCC's website - https://www.derbyshire-pcc.gov.uk/Transparency/Freedom-of-Information/Freedom-of-Information-and-Data-Protection.aspx

Policy Review Date

This policy will be reviewed annually however, it will be updated as necessary to reflect best practice and to ensure compliance with changes in any relevant legislations.