west midlands police and crime commissioner

OPCC Data and Analytics Strategy

1. *Aim*

1.1. The purpose of the Office of the Police and Crime Commissioner's Data and Analytics Strategy is to provide the strategic direction to enable collaborative working and to utilise the assets of data and technology to make the West Midlands safer and help the Police and Crime Commissioner (PCC) deliver statutory functions which enable an excellent West Midlands Police (WMP) force.

1.2. This also includes the West Midlands Violence Reduction Partnership (VRP), who are hosted by the Office of the Police and Crime Commissioner (OPCC) and have a focus on strengthening access to relevant data amongst partners to prevent and reduce serious youth violence.

1.3. Reference to the OPCC and PCC encompasses the VRP and their work with partners and specified authorities in terms of improving the flow of data between them.

2. *Objectives*

2.1. Deliver timely, precise, and actionable insights to the PCC, VRP and partners, supporting evidence-based decision-making and commissioning across policing and crime prevention.

2.2. Ensure that data is consistently accurate, high-quality, and readily accessible to all relevant stakeholders, enabling efficient analysis and well-informed decisions.

2.3. Cultivate strong partnerships and establish secure, ethical data-sharing protocols with local, regional, and national entities, thereby improving collective efforts to address crime and safety concerns.

2.4. Adhere to data protection laws and ethical standards, safeguarding personal information and ensuring responsible data usage.

2.5. Invest in and utilise state-of-the-art technologies and analytical tools to gain deeper insights into risks, threats, and crime trends as well as assist in predicting and mitigating future challenges, understanding police performance and resource allocation.

3. *Introduction*

3.1. Data is at the forefront of the OPCC holding to account function. Analysing data to provide insight for the PCC and partners to make informed, evidence-based decisions on a wide range of areas from police and partnership performance, to detailed analysis on local crime issues, the criminal justice system and commissioning. Data is a strategic asset, this strategy outlines how the OPCC will harness data assets effectively, legally, and how to efficiently share and store its data.

3.2. Information is the foundation of contemporary policing and broader partnership working and data and analytics are critical to the delivery of this work. Most traditional crime now has a digital element to it; in terms of both how it was committed, and how it is resolved. Digital technology develops rapidly, which results in the development of more data dissemination opportunities. This growth of data goes together with an increasing need to analyse large datasets, including data from other agencies, to discover and understand crime trends, to analyse performance and the use of technology to support decision making with data insights drawn from information which directly informs OPCC organisational decisions, strategies, and plans.

3.3. The quantity of data available to the OPCC is ever-growing, vast amounts of data are collected and collated on different systems and software packages, provided by a variety of partners. This data holds a value, the potential impact it can have on the achievement of the Police and Crime Plan priorities and the delivery of improving police and crime issues that really matter to the communities in the West Midlands.

3.4. Furthermore, public bodies are held to account for how they use public money and spend on commissioning services, they must have sufficient arrangements in place to monitor the efficiency and effectiveness of services. PCCs are required to publish certain information to allow the public to hold them to account, this is often disseminated through the OPCC website.

3.5. Holding data that is a key asset brings considerable responsibilities. Requiring the OPCC to ensure that the approach to data and analysis remains legal, ethical, and secure. We must balance the benefits and risks of handling and sharing data, this is the key to the successful delivery of this strategy.

3.6. The PCC is classified as a Crown Servant under the Official Secrets Act 1989, which subjects them to the same obligations regarding sensitive information as Government Ministers.

3.7. Under Section 36 of the Police Reform and Social Responsibility Act 2011, the Chief Constable of WMP is required to provide the elected local policing body with any information on policing matters that the body may request.

3.8. In summary, the overall vision of this strategy is to provide the foundation for excellent oversight of partnerships, crime and policing for the local communities of the West Midlands through data-driven insights constructed on ethical, responsible, and lawful ways of working.

4. Approach

4.1. The way the OPCC works, makes use of data, exploits technologies, and collaborates with partners, will be driven from these strategic capabilities outlined below.

5. Governance and responsibilities

5.1. A memorandum of understanding exists between the OPCC and WMP to ensure both parties can meet their statutory obligations. The OPCC is responsible for holding the Chief Constable accountable for their duties, as well as the duties of those under their direction and control.

5.2. The OPCC has a Data Protection Officer (DPO) within the Business Support Team who is responsible for monitoring and overseeing data governance, ensuring that data protection measures are consistently adhered to throughout all projects.

5.3. The OPCC is responsible for the safeguarding of personal information which is held by the office; therefore, it is essential that we monitor and ensure compliance with the UK General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, especially with the handling of special category data.

5.4. Data access will be managed under strict governance protocols to ensure compliance with legal and ethical standards. General principles for data access will be established, ensuring that only authorised personnel can access data as required for their roles. Specific provisions for data sharing and usage will be further outlined and formalised in Information Sharing Agreements (ISAs), which will detail the conditions, purposes, and limitations of data access between parties.

5.5. Data retention will be governed by clear protocols to ensure compliance with regulatory and organisational requirements. General principles for the retention and disposal of data will be established to maintain data integrity and security. Further specific details, including retention periods and conditions for data deletion, will be outlined in the Information Governance framework, ensuring alignment with legal and operational obligations.

5.6. To facilitate multi-agency collaboration in addressing serious violence, the data strategy will integrate data sharing requirements that align with the Serious Violence Duty (SVD). This includes the development and implementation of a regional ISA under the SVD, ensuring that all parties involved adhere to secure and efficient data practices. Once the ISA is finalised, the strategy will be updated to reflect this framework, promoting sustainable data sharing in full compliance with legal and regulatory obligations.

5.7. Adhere with the police information and records management Code of Practice.

5.8. Ensure an effective information governance framework is in place that aligns data-related workstreams, priorities and decisions with the delivery of the OPCCs organisational purposes.

6. Partnerships

6.1. Work in collaboration with OPCC partners to legally and ethically secure access to data so we can further analyse and draw meaningful insights through partnership data.

6.2. Maintain mutual data sharing agreements that meet legal and ethical standards for collection, use, retention, and disposal of data.

6.3. Work with external providers, WMP and PCC staff to improve data collection to support more consistent and methodical approaches.

7. Processes

7.1. Ensure that the OPCC carries out Data Protection Impact Assessments (DPIA) for data sharing that is likely to result in a high risk to individuals especially for major projects that involve disclosing personal data, or any plans for routine data sharing, even if there is no specific indicator of likely high risk.

7.2. Every new project undergoes a DPIA screening, with a full DPIA conducted for projects that demonstrate data complexity. ISAs will be devised and implemented with relevant partners to further safeguard the secure and compliant sharing and use of data.

7.3. The OPCC maintains data security by protecting the confidentiality, veracity, and availability of personal data, through actions and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

7.4. Ensure that all data security breaches or incidents are responded to in the correct way and the necessary processes are followed.

7.5. Ensure that data provided to handlers is accurate, relevant, and provided in a timely manner.

7.6. Continuously improve data insights and source system interactions to maximise efficiency.

8. Staff

8.1. Mandatory training for all staff on data protection and GDPR, with regular refresher training.

8.2. Compulsory GDPR training for new starters as part of the OPCC induction process.

8.3. Support staff with data protection responsibilities to ensure they are trained and empowered to provide advice and technical support on data protection queries and breaches.

8.4. Ensure that all employees have practical and up to date digital technology and the required support and data literacy to be able to make the most of available data tool.

9. Relevant Policies

9.1. The OPCC has additional policies on Privacy and Information Governance.