UK General Data Protection Regulations and Data Protection Act 2018
Internal Annual Report

Purpose of the Report

1. The report provides an update on the work completed by the Office of the Police and Crime Commissioner (OPCC) to ensure the organisation demonstrates compliancy to UK General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.
    a. EU General Data Protection Regulation 2018
    b. Data Protection Act 2018

2. The following areas will be explored within the report:

    - Requests for Personal Data:
        i. Freedom of Information Requests
        ii. Subject Access Requests
    - Data Breaches
    - Internal GDPR Training to OPCC Staff
    - Privacy Notice
    - Data Audit
    - Data Protection Impact Assessments
    - Data Sharing Agreements/Information Sharing Agreements
    - Appendix – Privacy Notice (Updated for May 2022) and Data Audit Questionnaire

    Please note, arising actions and recommendations will be highlighted in both italic and bold text throughout the report. Moving forwards, the actions will also be recorded on the ICO Recommendations Spreadsheet: ICO Data Protection Audit - APACE task and finish action plan.xlsx (wmpad.local)

Background

3. UK GDPR was enforced on 25th May 2018, applying to processing carried out by organisations in order to reshape approaches and protect data privacy. UK GDPR is tailored by the DPA 2018 and applies a broadly equivalent regime to certain types of processing to which UK GDPR does not apply. Further, the DPA 2018 makes a provision about the processing of personal data by public authorities for law enforcement purposes whilst implementing the Law Enforcement Directive.

4. UK GDPR and the DPA 2018 applies to organisations processing any personal data, including data whereby a person can be identified or identifiable directly from processed information, or whom can be indirectly identified or identifiable from the information in combination with additional information.

5. The following conditions should also be considered by organisations before data is processed:

    - Consent of the data subject
    - Processing is necessary for the performance of a contract with the data subject or to enter into a contract
    - Processing is necessary for compliance with a legal obligation
    - Processing is necessary to protect the vital interests of a data subject or another person
    - Processing is necessary for the performance of a task carried out in the public interest of in the exercise of the official authority vested in the controller
    - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

6. UK GDPR and DPA 2018 applies to all data controllers and data processors; a data controller determines the purposes and means of processing personal data oppose to a data processor who is responsible for processing personal data on behalf of a controller. Controllers are the decision-makers, as they exercise overall control over the purposes of the processing of personal data. Both controllers and processors have specific obligations placed on them under UK GDPR and DPA 2018 which must be complied with.

Requests for Personal Data

Freedom of Information Act (FOIA) 2000:

7. The FOIA 2000 provides public access to information held by public authorities, instructing that public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities.

8. Everyone has a general right of access to information, and any individual can request access to information held by the police force/criminal justice organisations regardless of the purpose of the request. The FOIA 2000 encourages transparency and honesty and all responses are published on the website.

9. The OPCC has the duty to confirm or deny whether we hold the information requested. If held the OPCC has the duty to communicate this information to the requester, unless it falls under an exemption.

    Any information that the OPCC holds for business purposes is considered to be ‘held’ under the FOIA 2000. This includes:

    - Information held at the time of the request
    - Information stored in servers or cloud storage
    - Information held by other organisations and authorities on our behalf

10. The OPCC has 20 working days to respond to requests following the date of receipt, and must respond within this time frame. The working hours required to complete an FOI request is

dependent upon the amount and intricacy of the information being requested, however if the FOI request will exceed a “cost limit” (if we estimate the gathering of information will equate to longer than 18 hours of work) an exemption can be applied.

Dealing with Requests Outside of the FOIA 2000:

11. When a request is made, it is sometimes deemed appropriate to handle a case without reference to the FOIA. The OPC might choose to respond outside of the FOIA where the request is for anything other than recorded information. That is to say anything that is not held on record, either electronic or paper. The OPCC might also respond outside the act where the information requested is regarded to be standard information that is available immediately on the website for example.

12. When the OPCC respond outside the FOI rules, it is not done to avoid providing any information or to circumvent the agencies obligations. The OPCC would only respond outside the act where we are providing a full response and it is deemed more efficient, and more effective for the applicant to do so in this manner. In such cases, the request will be dealt with as general casework.

Volume and Expediency of FOI Requests:

13. 90 FOI requests were received during the 2020 to 2021 financial year, and 75 were received during the 2021 to 2022 financial year. The most commonly noted themes throughout include estates, funding and OPCC costs.

14. The average turnaround time for responding to FOI requests has remained fairly consistent throughout each quarter, with the combined average turnaround at 13 days. Notably, the volume of FOI requests received by the OPCC increased dramatically within quarter four of the 2020 to 2021 financial year. 38 of the 44 FOI requests received were responded to within 20 working days; 5 were sent after 21 days and 1 after 24 days. Despite this high level of demand, the average turnaround time for the quarter was 13 days demonstrating a high level of efficiency and strong compliance to regulations.

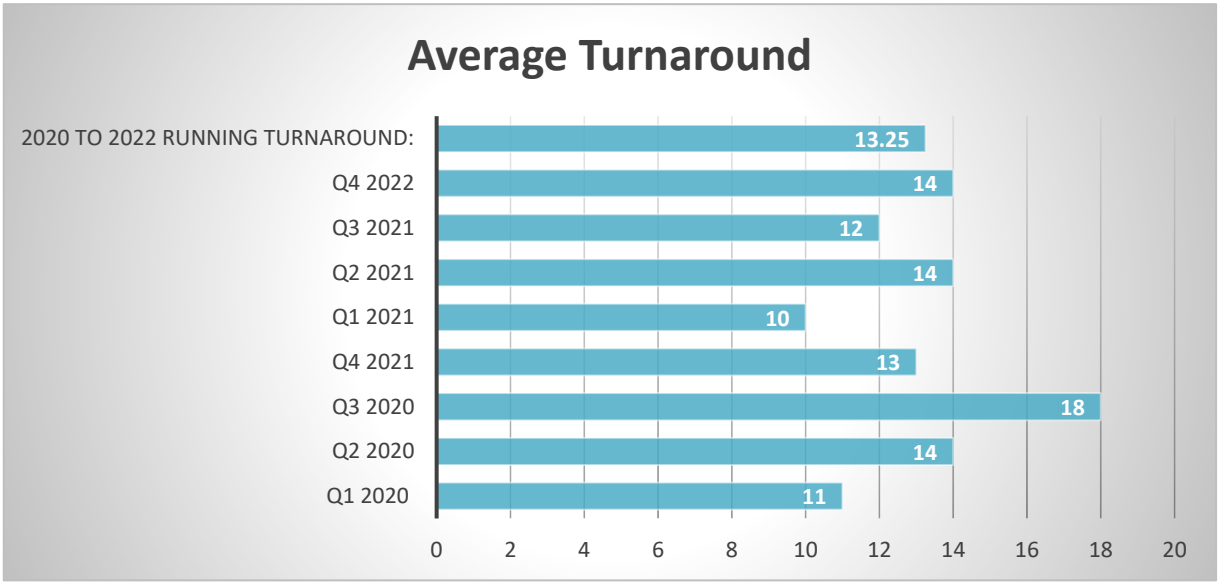
15. It can be assumed that the increase in FOI requests during this period was due to additional information being sought in preparation for the appointment of the new Police and Crime Commissioner on 13th May 2021. During quarter four of the 2020 to 2021 financial year, data displays a trend of direct information requests to the OPCC, including OPCC pay scales, political views and staff roles and titles.

16. It should also be noted that all FOI requests must be approved by the OPCC’s Deputy Chief Executive, and therefore factors such as additional demands, sickness or annual leave may have extended turnaround time on occasion.

17. Data concerning the average turnaround time and total volume of FOI requests received by the OPCC can be visualised below, divided into quarters starting from Q1 April 1st 2020:

Quarter	N. of FOI's	Average Turnaround
Q1 2020	9	11
Q2 2020	12	14
Q3 2020	25	18
Q4 2021	44	13

Q1 2021	22	10
Q2 2021	22	14
Q3 2021	15	12
Q4 2022	16	14
2020 to 2022 Running Turnaround:	165	13



Further Compliance with the FOIA:

18. The Section 45 Code of Practice provides recommendations to organisations and has been incorporated within the OPCC's approach to responding to requests. Examples of this include providing advice and assistance to those making requests and informing recipients of the appropriate complaints' procedure should they be dissatisfied with the response to their request. Any person who has requested information from the OPCC and is unhappy with the way their request for information has been handled can request a review of their case; the complaint procedure information is detailed within every FOI response. Since 2020, the OPCC Data Protection Officer has responded to only 3 requests for reviews into cases.

19. Further, the OPCC are also compliant with the Section 46 Code of Practice which covers *"good records management practice and the obligations of public authorities under the Public Records Acts to maintain their records in an ordered and managed way, so that they can readily retrieve information when it is needed."* This compliance is reflected within the average turnaround statistics; across 2020 and 2021 delays have ***not*** been presented as a cause of information being difficult to retrieve exemplifying organisation and efficient communication methods between staff.

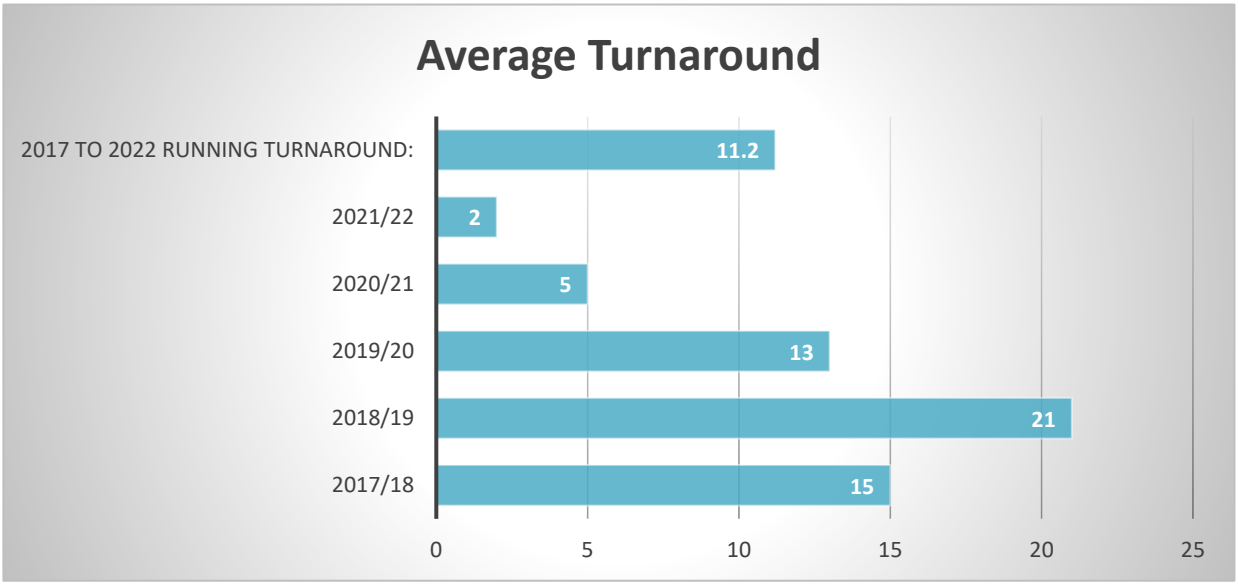
Subject Access Requests (SAR)

20. The OPCC, as data controller, must facilitate all data subject rights which are clarified in Article 15 to Article 22 in relation to employees and members of the public. Circumstantial exemptions may apply; however, rights of the individual should be incorporated within the OPCC's operating model and failure to comply risks being in breach of Article 12. The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data under Article 15 of the UK GDPR. It helps individuals to understand both how and why the OPCC are using data, and if we are doing so lawfully.

21. In accordance with Article 5 there is also a fundamental need for data to be processed in a transparent manner in relation to the data subject, and SAR's contribute to the monitoring of this. Individuals have the right to be provided with privacy information and to be informed of both the assembly and use of their personal data as per the essential requirement under UK GDPR. Exceptions to this are displayed in Article 14 and include any circumstance in which the data subject already holds the information, or if it would be a disproportionate effort to provide the information.

22. Please see the data below for the number of SAR's received from April 1st 2017 to March 31st 2022; the data exemplifying an increase of 115 SAR's between the 2020/21 and 2021/22 financial year. As a large proportion of the SAR's received are directed to West Midlands Police, the OPCC's response to recipients can be sent without delay. This is reflected within the average turnaround figures in the table below; for 2021/22 the average turnaround was 2 days, reduced by 13 days since the 2017/18 financial year.

Year	N. of SAR's Received	Average Turnaround
2017/18	2	15
2018/19	2	21
2019/20	7	13
2020/21	28	5
2021/22	143	2
2017 to 2022 Running Turnaround:	182	11.2



Developments 2020-2021:

23. An auditing 'tagging' system was introduced to provide FOI requests and SAR's with a unique number, ensuring each request can be monitored and is easily locatable on OPCC systems.
24. In January 2021, the GDPR BSO attended an online FOIA Training Course to increase expertise and resilience across the OPCC. Training was then provided to other BSO's.
25. In June 2021, FOIA and SAR Training was presented to the Violence Reduction Unit by the OPCC Data Protection Officer and GDPR BSO. The aim was to expand knowledge of the subject and to ensure that GDPR processes are complied with across the wider office.

26. The OPCC's relationship with the WMP FOI Team has strengthened through the GDPR BSO initiating contact and meeting face to face with the Team. This relationship is continuously strengthening, with advice and best practice shared.

Data Breaches:

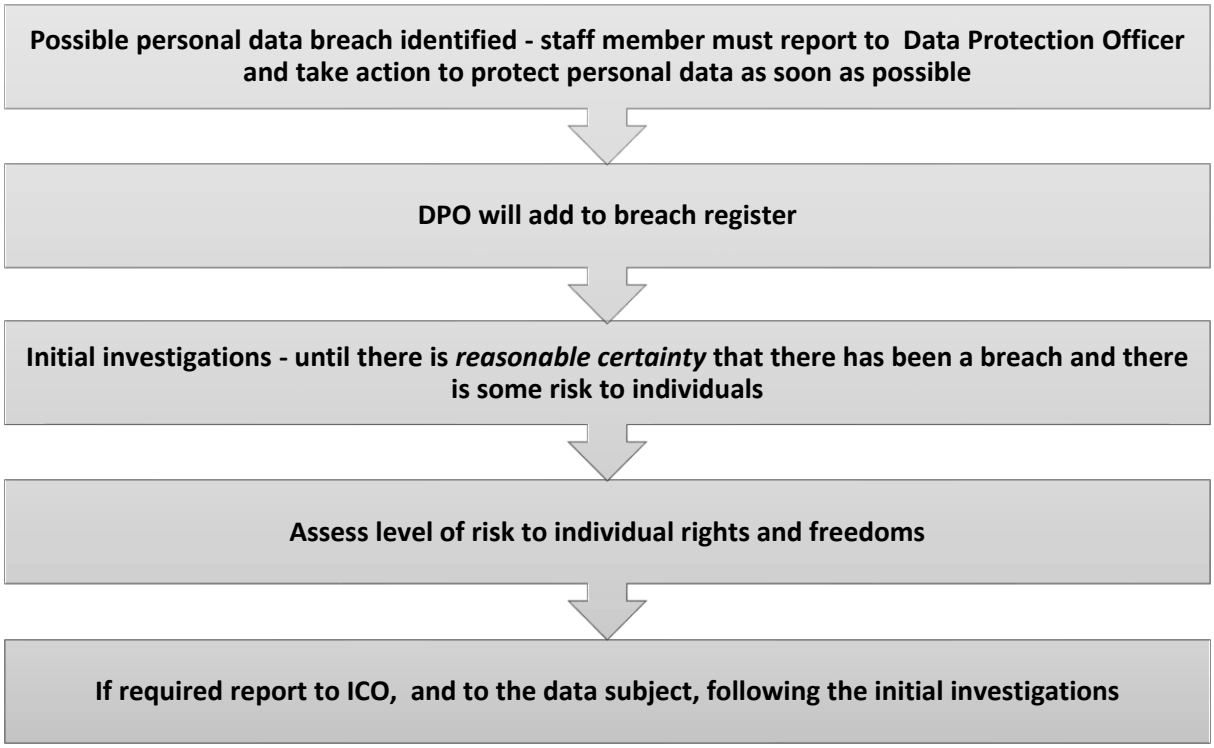
27. In order to comply with UK GDPR an DPA 2018 guidance, the OPCC maintains a record of any personal data breaches that occur within a Data Breach Inventory including facts surrounding the breach, the consequences, and the remedial action taken.

28. A personal data breach can be exemplified as: ***"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."***

29. Breaches are categorised as follows:

    - **Confidentiality Breach** – unauthorised or accidental disclosure of, or access to personal data.
    - **Integrity Breach** – unauthorised or accidental alteration of personal data.
    - **Availability Breach** – accidental or unauthorised loss of access to, or destruction of, personal data.

30. The OPCC has implemented a formal instructive process for when a personal data breach occurs, as displayed below:



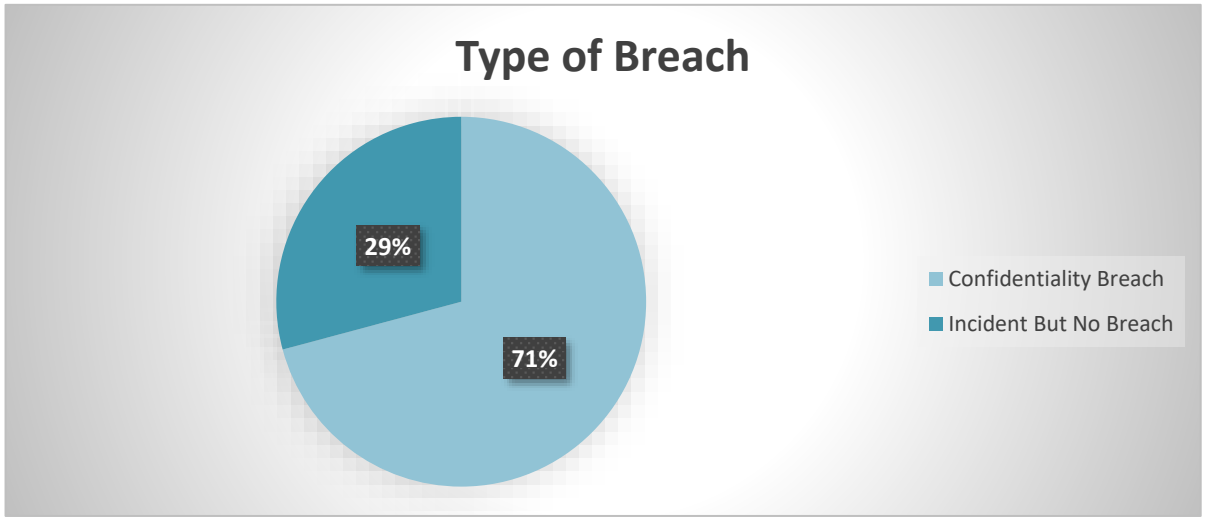
Volume and Expediency of Data Breaches:

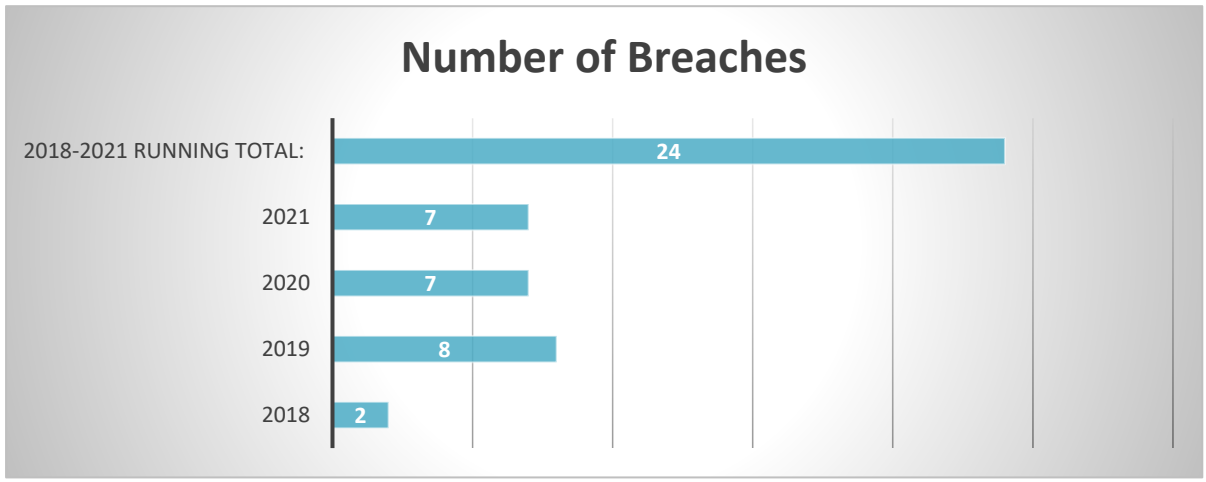
31. The Data Breach Inventory was introduced within the OPCC in 2018, with 24 breaches recorded from then until the conclusion of 2021. 71% of the 24 were categorised as a confidentiality breach however none were notified to the ICO, due to the low risk to individuals

rights and freedoms. The most commonly noted themes within the confidentiality breaches from 2018 to 2021 include data sent to the incorrect recipient, unintentionally releasing or publishing information and loss of paperwork. The remaining 29% of the 24 breaches were categorised as an incident but no breach; 6 of the 7 incidents but no breach was explained as individuals misplacing their encrypted work mobile.

32. Data concerning the number of breaches is divided annually below, alongside a visual breakdown of the type of breach:

Type of Breach	Number of Breaches	%
Confidentiality Breach	17	71%
Incident but No Breach	7	29%
2018-2021 Running Total:	24	100%





33. ***It should be noted that how to recognise a data security incident and the appropriate consequential actions are discussed with all staff members during their internal UK GDPR and DPA 2018 training, ran by the OPCC Data Protection Officer. This will continue to be discussed within training sessions moving forwards.***

Internal UK GDPR and DPA 2018 Training to OPCC Staff:

34. The internal session is designed to support OPCC staff to comply with UK GDPR, and is mandatory for all new starters within the organisation. The session is typically held twice a year, situated around quarters with higher recruitment levels, and covers various elements of UK GDPR and DPA 2018 including defining personal data, rights to individuals, the six principles of GDPR, breaches and the OPCC's overall approach.

35. Situated within the below table the dates and number of attendees at the training sessions which have ran from 2020 until present day. As displayed there were only 3 attendees for the first session held on 3rd April 2020; the circumstantial reasoning for the low number of attendees could be explained as a consequence of the pandemic, as the OPCC were following government guidance and the West Midlands were under lockdown restrictions. Although the session was transformed to virtual oppose to face to face, the OPCC were adjusting to working from home and focusing on the social and economic impact of the pandemic during this time period.

36. 87 members of staff were employed from the beginning of January 2020 until present day, with 56 attending the training session. Despite the invitation extending to members of staff who have attended a session previously, it can be assumed that since 2020 to date the total number of attendees across 2020 to date were new members of staff. This exemplifies that 64% of the 87 new starters have undertaken the mandatory training.

Date	N. of Attendees
20.04.2020	3
07.12.2020	9
Date Unknown	2
29.04.2021	22
21.06.2021	4
12.01.2022	16
2020 - 2022 Running Total:	56

Developments 2020-2022:

37. ***The OPCC Data Protection Officer and GDPR BSO have a future aim to ensure that the sessions are increasingly interactive. Ideas on how to ensure employees are actively involved in the session include questionnaires and the discussion of case studies within a refresher session after the initial training has been undertaken.***

38. ***The OPCC Data Protection Officer and GDPR BSO also aim to ensure all members of staff have received GDPR Training, either through visiting targeted team meetings or increasing the number of sessions throughout the year.***

Privacy Notice:

39. The OPCC Privacy Notice has been updated for May 2022, and has been published on our website. After conducting research, it was noted that our Privacy Notice provided only minimal information in terms of our Complaint Review Function; the updated Privacy Notice therefore includes additional information regarding this function.

Data Audit:

40. Audits are critical in providing an organisational assessment as to whether efficient data protection practices are understood, implemented and followed; audits also consider controls alongside fit for purpose procedures to support an organisation's obligations against UK GDPR and DPA 2018.

41. In August 2021 the OPCC launched a data audit of the organisation, aiming to monitor both how and why personal data is being processed and to ensure a library of how and why we use personal data is kept. Purposefully, the audit also aims to identify any recommendations for the organisation in order to strengthen business processes, governance arrangements and manage risk. An audit will be completed for each of the different departments within the OPCC before a joint summary report is written.

42. A template of the ICO's Data Processing Inventory was modified by the GDPR BSO to form a complex and structured spreadsheet, including prompts and categories for data such as:

    - Article 30 Record of Processing Activities
    - Privacy Notices
    - Consent
    - Purpose of Processing
    - Categories of Personal Data
    - Names of third-party organisations that personal data may be transferred from
    - Safeguards for exceptional transfers of personal data to third party organisations
    - Retention Schedule

    The Data Processing Inventory also allows for categorisation of specific business functions under each department within the OPCC.

43. Each organisation's audit is unique and the timescales for completion are dependent on the size, scope and organisation requirements. The individual scope area audited can also be rated against an assurance scale, recommended by the ICO. The assurance ratings are as follows:

Level of Assurance	Definition
High Assurance	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.
Reasonable Assurance	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Limited Assurance	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Very Limited Assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

44. At present, two teams within the OPCC have been subject to undertaking questionnaires alongside the completion of their Data Processing Inventory with an update for these provided below. Purposefully, the distribution of the questionnaires upon initial oversight of the audit meant that the analysis of results can be straightforward, alongside ensuring that the most appropriate and accurate data is gathered through asking experts within their specific field.

45. ***Please note, the Data Audit is an ongoing task that will be carried out throughout the year. Once the initial audit is complete, the information will be monitored and reviewed.***

Business Support: *Rated Reasonable Assurance*

46. Business Support were the initial OPCC function to undertake the data audit. Firstly, members of the Team were asked to complete a questionnaire (a template of which is included within the appendices) based on each function completed within their job role, oppose to their job role as an entirety. The questionnaires were titled and completed under the following functions:

    - Human Resources
    - Custody Visitors/Appropriate Adults
    - Legally Qualified Chaired and Independent Panel Members
    - Work Experience
    - Professional Standards Department Referrals
    - Chief Constable Complaints
    - Complaint Reviews
    - Freedom of Information/Subject Access Requests
    - Casework
    - Finance
    - Meetings/Diary Entries and Invitations
    - Board Member Information
    - Breaches
    - WMPCC Main Inbox and Post

47. The information gathered from the questionnaires has since been inputted into the Data Processing Inventory, available via the following link: Data Processing Inventory 2021 - Business Support.xlsx (wmpad.local).

Business Support Recommendations:

48. A number of recommendations were identified through the completion of the data audit for Business Support, summarised within the list below and then explained in further detail below:

    a. ***To transfer from saving files containing complaint review data from SharePoint and Centurion to only Centurion.***
    b. ***A yearly review of data to be conducted to ensure data is kept up to date and accurate.***
    c. ***Complete an audit of SAR's to ensure traceability.***
    d. ***Revisit and update automated responses to shared inboxes.***

49. The first and most significant recommendation relates to the Police and Crime Commissioner's complaint review function, as we have a statutory responsibility as the Relevant Review Body for complaints resolved by Professional Standards Department recorded under Schedule 3 of the Police Reform Act 2002. The individuals aligned to the complaint review function are situated within the Business Support Team, and require an additional level of vetting, management vetting (MV), to view complainant details and information from the police complaints database titled Centurion. Often, the information sought from Centurion is special category data or relates to the behaviours and conduct of West Midlands Police officers.

    The data sought from Centurion is often used within complaint review and casework responses and is therefore saved on the OPCC system SharePoint, a system that all members of staff have access to. As a result of the data audit, it was revealed that through saving data from Centurion onto SharePoint, we were potentially allowing individuals without the appropriate level of vetting to view this personal data.

    Following the data audit, a new process was implemented and the Business Support Team moved from saving files relating to complaint reviews on both SharePoint and Centurion to only Centurion, securing the data whilst ensuring those with only the appropriate level of management vetting have access. SharePoint cases are still created where it will list that "John Doe has an ongoing review under reference: RW/XXX/XX". Purposefully, this allows the Business Support Team to easily locate the names of individuals who have ongoing reviews when those individuals inevitably call the office. The files that relate to complaint reviews that were previously saved on SharePoint have not been removed. The removal of such documents would be extremely time consuming, however this task can be completed should the removal be a necessity in the future.

50. Exploring the recommendations further, the audit also identified that there was a lack of consistency in methods to ensure that personal data is accurate and kept up to date. The importance of the six Data Protection Principles (Article 5), which includes accuracy of data, is recognised by the Information Commissioner's Office (ICO), as "the principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows." It is the responsibility of the data controller to demonstrate compliance with the six principles; failing to comply will result in a breach of Article 5(2). As a result of this, it is advised for a yearly review of data to be conducted to ensure good practice is followed and that data is up to date and accurate.

51. Other noted recommendations include implementing an auditing process for SAR's to ensure they are easily traceable and revisiting automated responses to shared inboxes, particularly focusing on the clarity of the explanation that information may be shared with third party organisations such as West Midlands Police. Both of these recommendations have been actioned and completed.

Policy: ***Rated Limited Assurance***

52. The Policy Team audit commenced in September 2021, again with the sharing and collaborating of questionnaires, divided into the following functions:

    - Monitoring
    - Bid Writing
    - Developing Service Specifications
    - Coordinating Delivery Groups
    - Commissioning
    - Lobbying
    - Researching and Horizon Scanning
    - Responding to National Consultations
    - Responding to HMIC Reports
    - Holding Events and Event Planning
    - Sending out Meeting Invites

53. The information gathered from the questionnaires has since been inputted into the Data Processing Inventory, available via the following link: Data Processing Inventory 2021 - Policy.xlsx (wmpad.local)

Policy Recommendations:

54. After considering the data provided by the Policy Team within the questionnaires, it is advised that further assurance and information is needed in order to ascertain whether this department is fully compliant to UK GDPR. Please see the recommendations summarised within the list below and then explained in further detail below:

    a. ***Establish a list of projects that the OPCC Policy Team commissions.***
    b. ***Complete dip sampling for 25 different projects and their grant conditions.***
    c. ***Meet with the Head of Policy to discuss the data audit and methods of progression.***

55. The largest area of concern in terms of limited information was commissioning and monitoring service delivery; due to the Team working and collaborating with a multitude of projects and services, there is a need for an entire list of projects that the OPCC Policy Team commission to be included within the Data Processing Inventory. Then, in order to assess the level of GDPR compliancy within these projects, it is advised that the GDPR BSO completes a dip sampling exercise for 25 different projects and their grant conditions. The data sharing agreements and grant conditions will be checked for compliancy; a sample of this size would also allow for potential multiple issues to be highlighted or, alternatively, consistency around compliancy.

56. As previously mentioned, the purpose of the audit is to ensure that a complex library of data and how we process it is stored – in relation to the Policy Team we require further information in order to be able to meet this purpose and ensure compliancy, should the OPCC be subject to an investigation by the ICO.

Violence Reduction Unit (VRU):

57. In December 2021, the GDPR BSO requested support from the VRU's Governance Assistants in rolling out the data audit for the VRU. The Governance Assistants will be broadcasting the data audit questionnaires to each portfolio lead in order for them to share as much information as possible for each business function. After all questionnaires have been returned, the data can then be inputted into the Data Processing Inventory. Due to additional demands within the VRU and the conclusion of the end of the financial year, the data audit has not yet commenced.

Data Protection Impact Assessments (DPIA's):

58. Although DPIA's are typically used for large-scale processing operations, an assessment should also be made where personal data is processed for "taking decisions regarding specific natural persons" and "following the processing of special categories of personal data" as stated in UK GDPR. The completion of a DPIA allows for an initial examination of any risks whilst considering the nature, context, procedures and purposes of processing personal data. DPIA's also exemplify any appropriate safeguarding and mitigating risk measures. Without the completion of DPIA's, organisations risk breaching Article 35, potentially resulting in a proportionate fine issued by the ICO.

59. The OPCC are not systematically using DPIA's at present, however it is advised DPIA's should be implemented where necessary with emphasis placed on the assessment of risks to rights and freedoms of individuals. DPIA's should be completed at the initial stage of such circumstances, and it our responsibility to designate a member of the staff to lead such assessments. ICO guidance also states that organisations should have a DPIA policy in place; we would be complying with Article 34(7) along with advice provided by the WP29 if a policy was practiced.

60. ***This is an area which the OPCC can start to embed through training, and implement as good practice moving forwards.***

Data Sharing Agreements / Information Sharing Agreements

61. Data Sharing Agreements (DSA's) set out the purpose of data sharing between organisations and covers what happens to the data at each stage, set standards and allows for identification of responsibilities. DSA's demonstrate compliance to UK GDPR and DPA 2018.

62. ***At present, the OPCC does not have a full, comprehensive list detailing all DSA's. As a recommendation, this list will be generated moving forwards for monitoring, tracking and auditing purposes.***

Data Controllers for Commissioned Services:

63. APACE guidance states "in instances where an OPCC is commissioning services from the force, it is not entirely clear who the data controller is. This involves police owned data and not the OPCCs. With commissioned services, even if no data is handled, there is a belief that this increases the OPCC risk.

64. It was agreed that when a PCC is the commissioning agent of the police, the Chief Constable is the data controller for their own police data e.g. victims' etc. PCCs are not joint controllers. The ICO guidance states that a data controller is one who makes decisions about data. The responsibility for the data sits with the competent authority e.g. police or fire authority, but not

the PCC. PCCs need to provide reassurance to the ICO that the contracts commissioned by PCCs from the force will have appropriate scrutiny/reassurance checks built in. This means that the police are responsible for having appropriate data sharing and processing agreements in place. PCCs are the commissioning agents with a responsibility to ensure the relevant data controllers have the correct processes in place to handle data appropriately. It can be said that an umbrella aspect is a statutory one for PCCs to ensure efficient and effective policing, which would include data protection."

Developments for 2022/2023

65. ***The DPO and GDPR BSO will be meeting with the Commissioning Officers twice a year moving forwards to discuss the process and any updates.***

66. ***New commissioning files have been implemented for this financial year; this will allow for increased efficiency in terms of recording and monitoring for those organisations with a Data Sharing Agreement. There is a consideration for the agreements to define that the agreement applies for the organisation's current contract, and will continue to apply should the contract be renewed. Alternatively, there is also a consideration for an organisation's contract renewal to state that the pre-existing Data Sharing Agreement applies. This will be agreed and shared throughout the OPCC to ensure consistency.***

67. ***The VRU have proposed the collection of information from Commissioned Provider's regarding staff DBS checks, in order to demonstrate compliancy and ensure that staff working directly with young people have a current DBS. This will be reviewed due to the collection of personal data impacting our data sharing if this was to be undertaken.***

68. ***The Commissioning Team are placing emphasis onto the Project Leads to make the decision regarding the OPCC's role as either data controller or joint controller.***

69. ***The information shared with providers when the OPCC provides the Data Sharing Agreement template will be reviewed. At present, the information is as follows:***

    "It is a requirement that all funded providers openly engage with internal and external evaluation. A Data Sharing Agreement is attached for completion alongside these Grant Conditions. The parts for the project lead to complete are highlighted in yellow and parts for the provider to complete highlighted in green. If you have any questions or require any further information, please don't hesitate to contact us."

Appendix:

PRIVACY NOTICE

West Midlands Police and Crime Commissioner is committed to ensuring the privacy and security of your personal data. The following Privacy Policy sets out the personal data that we collect about you as a partner, a colleague or a user of our services, including how and why we process your personal data, who we share it with, and your rights and choices when it comes to your personal data.

In this Privacy Policy, when we refer to "personal data", we mean information which could directly identify you (for example, your name or email address) and information which could indirectly identify you, meaning that it could identify you when combined with other information which we hold about you (for example, your gender or date of birth). "Process" or "processing" means just about any conceivable use of personal data, including recording, storing, viewing or disclosing personal data.

The Police and Crime Commissioner is the data controller of your personal data (referred to in this Policy as 'the Commissioner' or "we").

The Commissioner will comply with data protection law. You can view our Data Protection Policy on the Police and Crime Commissioner's website: www.westmidlands-pcc.gov.uk. This policy includes details about our data retention rules here. More information about data protection and your rights can be found on the Information Commissioner's website: https://ico.org.uk/for-the-public/

Your rights and your personal data
You have the following rights with respect to your personal data:

1) ***The right to access personal data we hold on you***
   At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
2) ***The right to correct and update the personal data we hold on you***
   If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
3) ***The right to have your personal data erased***
   If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
4) ***The right to object to processing of your personal data or to restrict it to certain purposes only***
   You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.
5) ***The right to data portability***
   You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
6) ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) The right to lodge a complaint with the Information Commissioner's Office.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

How long do we keep your personal data?

Our data retention schedule states how long we keep different categories of data. The Schedule forms part of our Information and Records Management Policy and can be viewed on the Police and Crime Commissioner's website: www.westmidlands-pcc.gov.uk

Changes to 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 prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on the Commissioner's website: www.westmidlands-pcc.gov.uk

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Contact

If you have any questions about your personal data which are not answered by this Policy, please contact:

Data Protection Officer
West Midlands Police and Crime Commissioner
Lloyd House
Colmore Circus
Queensway
Birmingham
B4 6NQ
Email: wmpcc@west-midlands.pnn.police.uk

Contents of this privacy notice:

We process personal data for a number of different purposes. Click on the link below to see the most appropriate paragraphs of this privacy notice:

When you contact us, we:

- Will retain and store your details, including copies of everything you send to us.
- May also share your personal data and any of the information you have provided with other organisations if we need to do so in order to deal with your contact properly. Most commonly this would be West Midlands Police, but it may include other organisations if required in order to deal with your contact (e.g. local authorities, or the Police and Crime Panel).
- Will contact you to discuss the matters you have raised with us.
- Complaints about West Midlands Police officers or staff must be dealt with by the appropriate authority which is the Professional Standards Department (PSD). If your complaint is about a police officer or member of police staff **we will refer it to PSD**.
- If your complaint is about the Chief Constable, we will contact West Midlands Police in order to investigate your complaint and gather all of the information we need in order to do so. This may include us sharing details of your complaint with the Chief Constable.
- If your complaint is about someone who works for the PCC, we may share details about your complaint with the member of staff concerned, or with other staff within in the office, where it is necessary for us to do so in order to investigate the complaint.

What personal information will we collect if you contact us?

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to your query/suggestion or complaint, we may ask for and process other information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

We use your personal data for some or all of the following purposes:

- To follow up with you after correspondence;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how policing and other services are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the Commissioner;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our news, facilities, services, events and staff, Board members and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives.

Complaint Reviews:

- We have a statutory responsibility as the Relevant Review Body for some complaints dealt with by PSD in accordance with the Police Reform Act 2002, where the complainant is unsatisfied with the way that their original complaint has been handled. PSD will provide details of how a review can be requested from the relevant review body in their original outcome letter to the complainant.

What personal information will we collect to process your complaint review?

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to your complaint, we may ask for and process other information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation;
- Complaint details and original complaint documentation;
- Allegations of misconduct.

We use the personal information processed for your complaint review for the following purposes:

- To identify your original complaint and to conduct a review of the way your complaint has been handled;
- To provide learning recommendations to West Midlands Police where the review has identified further action or improvement;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury.

What is our legal basis for processing your personal data?

The Commissioner is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the Commissioner's public powers and duties. We will always take into account your interests and rights.

For the complaint review function, our legal basis for processing your personal data is to perform a public task with official authority under the following legislation: Policing and Crime Act 2017 and the Police Reform Act 2002 (Part 2 and Schedule 3, paragraph 25). This is supported by the Police Complaints and Misconduct Regulations 2020.

Sharing your personal data

If it is necessary we may share your personal data with third parties. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. They may include:

- West Midlands Police
- Local authorities
- Home Office
- West Midlands Police and Crime Panel
- Other police forces

- Community groups
- Charities
- Other not for profit entities
- Contractors
- Employment agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to us, and enable the Commissioner to fulfil his public duty or his legal obligations. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the Commissioner and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

Attending our meetings or events, circulation and contact lists

Our meetings and events

Most of our meetings, summits and events are held in public, and many are also webcast. Copies of webcasts are available for public viewing from the PCC's website. We sometimes take photographs of meetings and events, and people who attend may appear in these photographs. In addition we normally take notes of meetings and events and these notes may include the names or other information about people who attend.

This means that if you attend one of our meetings or events:

- You may appear on the webcast
- You may appear in photographs of the event
- Your name may be included in the notes/minutes

What legal basis do we rely upon?

Meetings and events take place to support the Commissioner in undertaking his public task. We will rely upon contractual obligation for people who are regular members of our boards, groups or committees. For other events we shall obtain consent from those present before commencing webcasting, photography or including personal data in our notes or minutes.

We will always respect your privacy, and take the following steps:

- Before webcasting commences everybody present will be informed and if they prefer not to be webcast they will have the opportunity to withdraw or to sit in a part of the room not covered by the webcast.
- Members of our regular boards or groups (most notably the Strategic Policing and Crime Board and the Audit Committee, but this may also include other groups which have a regular membership) will have a contract with us which includes being included in webcast, photographs, notes and minutes of meetings.

Contact and circulation lists

If you attend one of our meetings or events we will ask you for the following information:

- Name
- Contact email and telephone number
- Your organisation and your position
- Accessibility and dietary requirements

We will use these to provide you with information about the meeting or event; to help us plan and also for health and safety planning in case of fire or other emergency. We will not share this information with any third party without your prior consent.

We may use a third party such as Eventbrite to help us organise events. In such cases, the third party is a data processor for your data, and will be responsible for your data. If we use a third party to help us in this way, you shall receive a separate privacy notice from them.

Circulation lists
We hold a number of lists of people's contact details. We hold lists so that we can invite people to suitable events and meetings and also so that we can contact people with information and news. You will be asked for your consent for your name and other contact details to be included on our circulation list. You may withdraw this consent at any time and your details will then be removed from our list.

Public petitions and questions at Strategic Policing and Crime Board
The Commissioner invites members of the public to submit questions and petitions to meetings of the Strategic Policing and Crime Board. More information on the process for this can be found on the website: www.westmidlands-pcc.gov.uk

If you submit a petition or question, your personal details may be shared with West Midlands Police or any other third party necessary in order to address the question or the petition. Your name and other details may be included in the notes of the meeting, and if you attend the meeting you may appear in the webcast and photographs of the event.

Application for funding, or recipient of our funding

Applicants for funding will normally be required to provide us with personal data including:

- Name, address, email and other contact information
- Details of the people and organisation making the application
- Bank and other financial information
- For some projects or applications, sensitive personal information (where this is relevant to the project)

We use your personal data for some or all of the following purposes:

- To follow up with you after correspondence;
- To assess your application for funding;
- To monitor progress of projects that have been funded;
- To make payments to you in accordance with our agreement;
- To provide publicity, media releases and information on the Commissioner's website.
- To confirm your identity;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp or similar);
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the Commissioner;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our news, facilities, services, events and staff, Board members and other role holders;

- To share with internal or external auditors, for the purpose of undertaking an audit, or undertaking an investigation in accordance with their legal obligations and powers.
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives.

What is our legal basis for processing your personal data?
The Commissioner is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the Commissioner's public powers and duties.

If personal data is used in publicity materials about a project, in most cases we do so in reliance upon the terms of the contractual agreement between us. If this is not covered by the agreement between us, we shall seek your consent before using personal data in any publicity materials. We will always take into account your interests and rights.

Sharing your personal data
If it is necessary we may share your personal data with third parties. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. They may include:

- West Midlands Police
- Local authorities
- Home Office
- West Midlands Police and Crime Panel
- Other police forces
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Employment agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to us, and enable the Commissioner to fulfil his public duty or his legal obligations. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the Commissioner and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

Staff, volunteers, members of Strategic Policing and Crime Board, members of PCC committees and groups, suppliers and contractors

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis
**This also includes applicants or candidates for any of these roles.

What personal data will we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.

- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed, and invoice payments.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- Your public use of social media.
- CCTV footage and other information obtained through electronic means such as smartcard or swipecard records.
- Information about your use of our information and communications systems.
- Information about your time keeping and attendance.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and undertaking regular audit processes.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud and/or corruption.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer a register of gifts, hospitality and personal interests
- To provide a reference.
- It is paramount that the public have trust and confidence in the Police and Crime Commissioner, and we will monitor your public use of social media in order to ensure that you do not bring the organisation into disrepute.
- We will assess social media use for all potential employees, volunteers or contractors and we may use this as part of our recruitment/appointment decision making.
- We will also assess and monitor your public use of social media in order to check that you are properly fulfilling your employment contract. For example, most posts are politically restricted, and we will check that your social media is complaint with this.
- We will use information about your time keeping and attendance to assess your work performance, and it may also be used in decisions about pay increments, and in disciplinary proceedings.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

We may process sensitive personal data including, as appropriate:

  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.
We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.
We will also process your data in order to assist you in fulfilling your role.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- West Midlands Police, which runs or hosts many of our HR functions.
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
- Other persons or organisations operating within local community.
- internal or external auditors, for the purpose of undertaking an audit, or undertaking an investigation in accordance with their legal obligations and powers.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- pension providers
- Former and prospective employers
- National and local vetting services
- Recruitment Agencies
- Professional advisors
- Trade unions or employee representatives

In addition, The Police and Crime Commissioner is engaged with the National Fraud Initiative. This is an exercise managed by the Cabinet Office that matches electronic data between public and private sector bodies to prevent and detect fraud. This is a government backed initiative to protect public

funds. If you would like to know how your information is used in this initiative please read more on NFI Privacy.'

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Data Mapping Audit – Questionnaire

The Office of the Police and Crime Commissioner (OPCC) is completing an internal audit in order to monitor both how and why personal data is being processed within our organisation. A library of how and why we use personal data will be kept after the audit is complete. Any recommendations which are identified during the audit to strengthen business processes, governance arrangements and manage risk, will be reported to management.

Note, a separate questionnaire must be completed for each business function.

Please complete the questionnaire below detailing as much information as possible. If required, please consult each member of staff who is involved within the specific business function.
The questionnaire should be returned to Gemma Bridgwater (Business Support) upon completion.

Team:	
Completed by:	
Date:	
Business Function: E.g. Casework	

Question:	**Response:** *Please detail as much information as possible.*
1. What personal data do you collect and hold? *Personal data is information that relates to an identified or identifiable individual.*	
2. What is the purpose for collecting and holding this personal data?	
3. Do you collect any sensitive or special category data? *Special Category Data can be defined as:* • *personal data revealing racial or ethnic origin;* • *personal data revealing political opinions;* • *personal data revealing religious or philosophical beliefs;* • *personal data revealing trade union membership;* • *genetic data;* • *biometric data (where used for identification purposes);* • *data concerning health;* • *data concerning a person's sex life; and* • *data concerning a person's sexual orientation.*	

4. Do you collect any information relating to individuals under 18 years of age?	
5. Do you request for consent or contracts for this? Please attached relevant documents.	
6. How and where do you store the data collected? *E.g. SharePoint, Files.*	
7. Do you tell individuals how their data will be used and where it will be stored? How do you advise the individuals?	
8. Do you share identifiable data with any third parties? *E.g. PSD, WMP, Home Office.*	
9. If yes, how do you transfer the data?	
10. Do you have a Retention Policy around this data? *Retention policies list the types of record or information you hold, what you use it for, and how long you intend to keep it.*	
11. How do you ensure data is kept up to date?	
12. How do individuals request for their data to be deleted?	
13. Is the Office of the Police and Crime Commissioner's Privacy Notice shared with the individuals?	
14. Do you receive data from anyone else for this business function? *E.g. PSD, WMP, Home Office.*	
15. Do you use any websites in your use of this data? *E.g. Mail Chimp, PCC Website, Eventbrite.*	