Office of the Police and Crime Commissioner for Warwickshire

Policy: Information Governance

Policy Owner	Chief Executive
Version number	1
Policy Implementation Date	March 2024
Next Review Date Prior To	March 2026
Security Classification	Official
Disclosable under Freedom of Information Act?	Yes
Risk Rating	Low
Equality Analysis	Low

1. Introduction

The Office of the Police and Crime Commissioner for Warwickshire (OPCC) is committed to the handling of information in a safe, responsible and secure manner and ensuring the availability, integrity and confidentiality of the information under its control. This policy identifies what information the organisation holds and the principles for use, storage and deletion of information.

This policy also includes detail of how personal data will be dealt with, under the provisions of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018) and how individuals can access their personal data.

Personal data is information that relates to an identified or identifiable individual. The person or organisation who controls the purpose and manner in which data is processed is the data controller. The Police and Crime Commissioner is a data controller.

This policy has been prepared in compliance with relevant legislative regimes and is underpinned by a number of related codes of practice and good practice guidelines. It is applicable to all staff of the OPCC including the Police and Crime Commissioner, Deputy Police and Crime Commissioner (if in post), volunteers, consultants and any other individuals working for the OPCC on a contractual basis or otherwise engaged on OPCC business.

2. Principles

The OPCC has access to a range of different materials, much of which is stored electronically, but some stored physically in hard copy. The OPCC has access to technically secure methods to save and transmit information, using systems procured and managed by Warwickshire Police. This includes technical security measures ranging from secure passwords and system encryption, organisational safeguards ranging from physical building and office security to procedural standards and requirements for the safe handling and storage of information.

The following principles for information management have been established:

- Accurate and relevant information is essential to effective decision making and good records management enables business to be conducted in an orderly efficient and accountable manner.
- Where possible only one copy of a record should be kept, with duplicate records destroyed appropriately. Records should be electronic wherever possible.
- Decisions should be made at all times when information is shared to ensure that only relevant and necessary information is transmitted, with a focus on only sharing the minimum required.
- Personal data and information should not be aggregated unless there is a sound reason to do this.
- Individuals should take personal responsibility for handing personal information, and should openly raise any issues of information security.
- Information should be disposed of in line with the OPCC retention schedule, and should not be retained unnecessarily.
- Training will be provided to ensure that staff members understand their responsibilities in respect of information management.

- The OPCC will demonstrate compliance with the DPA 2018 to meet the requirements of accountability.

This policy supports compliance with legal, national and best practice standards including;

- Freedom of Information Act 2000
- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (UK GDPR)
- Equalities Act 2010
- Human Rights Act 1998
- Crime and Disorder Act 1998, as amended
- Computer Misuse Act 1990
- Official Secrets Act 1989
- Government Security Classification Policy June 2023

The policy should be read in conjunction with relevant force policies relating to information security and IT acceptable use.

3. Roles and Responsibilities

The following roles and responsibilities are applicable under this policy:

- Data Controller – This is the PCC, who has overall responsibility for the safe handling of personal data and information. This cannot be delegated as it relates to the operation of the law.
- Senior Information Risk Owner (SIRO) - The Chief Executive is the SIRO. The SIRO's role is to ensure information assets and risks within the organisation are managed as a business process rather than as a technical issue. The SIRO should be a champion of governance and must ensure there are consistent and repeatable approaches to managing risk at all levels of the organisation. The SIRO must own the organisation's overall information management policy and risks and ensure they are implemented / mitigated consistently. The SIRO is responsible for ensuring that the data protection legislation and policy is applied and maintained consistently throughout the organisation, owning and reviewing information-based risks, ensuring that Data Protection Impact Assessments (DPIAs) are carried out on all new projects when required, understanding the information risks faced by the organisation, its partners and commissioned services ensuring that they are addressed, and that they inform strategic priorities and ensuring that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny
- Data Protection Officer (DPO) – As a public body, the OPCC is under a statutory duty to appoint a Data Protection Officer. This is the Head of Business Services and Assurance. The DPO assists the OPCC to monitor internal compliance, inform and advise the organisation on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the ICO. They are

also responsible for ensuring that the staff undertaking Subject Access Requests comply with the law. The DPO will ensure a programme of training for staff is prepared and delivered and will manage the arrangements for retaining and disposing of data. The Head of Business Services and Assurance is also responsible for ensuring compliance with the Freedom of Information Act 2000 and for paying the Annual Fee to the ICO.

- All Staff - All staff are required to read and comply with the organisation's information management policies and seek the advice of the DPO where appropriate. Disregard for this policy may be regarded as misconduct or gross misconduct and may lead to dismissal. In the case of contractors, representatives, workers and volunteers, this may be grounds for termination of that relationship with the OPCC.

This policy is underpinned by a number of other policies and procedures and should be read alongside those referenced.

4. Creation of records

All staff will be responsible for managing the information they process which can include the creation, receipt, holding, and transmission of information. Staff must:

1. Know what information they are responsible for
2. Make sure they achieve high standards of accuracy and quality when creating and recording any information.
3. Keep the information up to date.
4. Classify and protect information according to its sensitivity, value, and importance.
5. Understand how information should be handled, who should receive and/or have access to it.
6. Make sure the information is secured, both physically and electronically
7. Keep information for no longer than necessary – use agreed retention and disposal schedules applicable to the information in their control.
8. Respect people's rights to privacy and confidentiality, and rights to access to their own personal information
9. Respect people's right to access information that the OPCC creates, owns or holds and assist them in accessing it.
10. Make the best use of information to deliver and improve services.
11. Report any security incidents, potential or actual losses of information or equipment to their line manager and Data Protection Officer, or the SIRO in their absence.
12. Understand and adhere to the OPCC's information governance policies and procedures.
13. Seek advice and guidance whenever required.
14. Regularly review records created and ensure they are handed over, archived, or disposed of (if applicable, and in line with the OPCC retention schedule) at the termination of appointment with the OPCC.

The Information Commissioner's Office has the responsibility for making sure organisations comply with information legislation and issues good practice which we incorporate into our policies and procedures. Failure by the OPCC to comply with legislation and good practice may lead to enforcement and improvement measures, possible fines and loss of reputation.

In compliance with the UK GDPR the OPCC maps and maintains a register of information assets, known as a Record of Processing Activities (ROPA). It is the responsibility of the DPO to ensure that this is regularly reviewed to ensure it is up to date.

The OPCC will adhere to the principles of data protection:

- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Sharing of personal data should be for specified and legitimate purposes.
- Personal data shared should be adequate, relevant and limited to what is necessary.
- Personal data held must be accurate and where necessary kept up to date.
- Personal data held must be kept in a form which permits identification of data subjects for no longer than is necessary.
- Personal data held must be processed in a manner that ensures appropriate security of the personal data.
- The OPCC must demonstrate compliance with the DPA/GDPR to meet the requirements of accountability.

5. Information Classification

It is everyone's responsibility to ensure that all information that has been shared receives the appropriate degree of care and protection. Individuals are expected to:

- handle information appropriately in accordance with the risk
- follow specific handling instructions related to information.
- check with their line manager or the information owner if the risk categorisation or handling instructions are not clear

The OPCC use the Government Security Classification Policy. This supports proactive decision making in respect of what information can and should be shared. Information assets should be identified, and clear decisions made to determine whether they can be shared and who with. All OPCC staff are vetted in accordance with the College of Policing Authorised Professional Practice. Different vetting levels determine what information can be accessed by whom.

There are three classifications of information:

a. OFFICIAL: 'The majority of information that is created, processed, sent or received in the public sector and by partner organisations, which could cause no more than moderate damage if compromised and must be defended against a broad range of threat actors with differing capabilities using nuanced protective controls.'

b. SECRET: 'Very sensitive information that requires enhanced protective controls, including the use of secure networks on secured dedicated physical infrastructure and appropriately defined and implemented boundary security controls, suitable to defend against highly capable and determined threat actors, whereby a compromise could threaten life (an individual or group), seriously damage the UK's security and/or international relations, its financial security/stability or impede its ability to investigate serious and organised crime.'

c. TOP SECRET: 'Exceptionally sensitive information assets that directly support or inform the national security of the UK or its allies AND require an extremely high assurance of protection from all threats with the use of secure networks on highly secured dedicated physical infrastructure, and robustly defined and implemented boundary security controls'.

Official Sensitive is not a standalone classification but the use of the marking 'Sensitive', will be used when information is of a sensitive nature, such as personal data, and not intended for public release.

It is rare that OPCC staff would have access to Secret or Top Secret information, and handling instructions will be given if this is required. There may be occasions where OPCC staff attend restricted sites, and on those occasions, individuals will be briefed and, where required, instructed where to store personal items such as mobile phones.

It is important to remember the 'need-to-know' principle; the dissemination of sensitive information should be no wider than is required for the efficient conduct of an individual's job function and restricted to those who are authorised to have access is fundamental to all aspects of security.

6. Personal Information

The DPA 2018 requires the OPCC to handle personal information in a safe, responsible and secure manner. It is incumbent on parties to strike a balance between the privacy rights of individuals and the legitimate interests of other parties who need to access that information for specified purposes. The OPCC expects all staff to recognise their responsibility for treating personal information with the care and respect it deserves. Information should be marked appropriately so that its handling instructions are easily understood. Data will be:

- processed fairly, lawfully and in a transparent manner in relation to the data subject.
- processed or shared only for specified, and legitimate purposes.

- shared only in a way that is adequate, relevant and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled and stored in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

6.1 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a way to analyse systematically and comprehensively the approach to processing personal data, in order to help to identify and minimise data protection risks. The OPCC will carry out a DPIA before processing any information which is likely to impact on individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data. This non exhaustive list gives guidance on when a DPIA might be appropriate.

- To participate in any major project involving the use of personal data.
- To process sensitive data, data of a highly personal nature, or data relating to children or vulnerable people.
- To use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- To process special-category data or criminal-offence data on a large scale.
- To systematically monitor a publicly accessible place on a large scale. eg CCTV systems
- To combine, compare or match data from multiple sources.
- To process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the guidelines.
- To process personal data that could result in a risk of physical harm in the event of a security breach.

An assessment may be required when the OPCC plans to carry out:

- evaluation or scoring
- automated decision-making with significant effects
- systematic monitoring
- processing on a large scale
- innovative technological or organisational solutions
- processing that involves preventing data subjects from exercising a right or using a service or contract.

The OPCC will complete a new DPIA if there is a change to the nature, scope, context or purposes of its processing. If a decision is made not to carry out a DPIA, the reasons will be documented.

A template has been designed, based on ICO good practice, to guide the process of completing a DPIA. The questions within the template will assist in understanding the impact to an individual of their personal data being processed in the proposed way. To assess the level of risk, both the likelihood and the severity of any impact on individuals should be considered. A DPIA does not have to indicate that all risks have been eradicated but that all risks have been considered and any remaining risks justified. Identified actions should be integrated into the project or process development, and monitoring of such actions should take place regularly.

The assessment should be completed by the lead officer for the project or process and needs to be submitted to the Data Protection Officer once completed. The Data Protection Officer will review the assessment, and may decide on further actions to be taken, which could also include consultation with the ICO. The Data Protection Officer will ensure the DPIA is added to the tracker.

6.2 Subject Access Requests

Individuals have a right to receive a copy of any of their personal data held by the OPCC. This is referred to as a Subject Access Request. It is preferred that an individual makes a Subject Access Request in writing, using the template designed for that purpose. The template helps the individual shape their request and clarify to the OPCC what information they are looking for. Where possible individuals are requested to be specific in their request, so that the information can be located and shared in a timely manner. The OPCC may request proof of identify before the request is processed.

The OPCC will ordinarily respond to a Subject Access Request within 1 calendar month, although if a large amount of information is requested or the request is complex, the OPCC may need more time to respond. In such cases, the OPCC is permitted a further 2-month extension, and the requester will be informed of these altered timescales. If the request is repetitious or manifestly excessive the request may be refused or a reasonable fee based on the administrative cost of providing the information may be charged, and the information will not be gathered until the fee is received.

The OPCC will make reasonable efforts to gather the information requested and will disclose it securely. The organisation will only share information that has been requested. If the information is not held by the OPCC, the requester may be directed to an alternative potential organisation if appropriate. If the information requested reveals personal data about a third party, either that individual's consent will be sought before responding to the request, or third parties' personal data will be redacted before responding. If the OPCC is unable to provide access to personal data because disclosure would violate the rights and freedoms of third parties, this decision will be notified to the requester.

Applicable law may allow or require the OPCC to refuse to provide access to some or all personal data held, or data may have been destroyed, erased, or made anonymous in accordance with record retention obligations and practices. If personal data cannot be provided, this will be notified.

If an individual is dissatisfied with the information provided or the OPCC's handling of the subject access request they can make a complaint to the OPCC or ICO. The Information Commissioner is empowered to assess whether there has been a failure to comply with Data Protection laws. The Commissioner can issue enforcement proceedings if satisfied that there has been a contravention of the data protection principles.

6.3 Data Breaches

A data breach is 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. OPCC staff are expected to report when a breach takes place, or there is near miss. It is acknowledged that things can go wrong and information can be shared inappropriately, and it is important that these matters are dealt with promptly and appropriately for the severity of the incident. It is important to:

- Ensure timely containment and risk management of all information security incidents.
- Support identification of whether the incident should be notified to the ICO and the individual(s) affected by the incident.
- Monitor trends and determine whether further controls or actions are required.
- Evaluate lessons learnt and communicate areas for improvement to staff.

Information security incidents can cover many situations, but generally will involve an adverse event which results, or has the potential to result in the compromise, misuse, or loss of OPCC owned or held information or assets. This may include personal or sensitive / special category personal data as defined under the data protection legislation and also confidential business information. Data breaches can be categorised according to the following three information security principles:

- Confidentiality breach – where there is an unauthorised or accidental disclosure of, or access to, personal data.
- Availability breach – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

Examples could include the loss or theft of information or equipment, incorrect handling of protectively marked information, poor physical security, hacking, information disclosed in error and unauthorised use or access to information or systems.

The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage. The purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

These same principles can also apply to cyber incidents i.e. any incident that could or has compromised information assets within the OPCC's digital network as provided to the OPCC by Warwickshire Police, e.g. phishing emails or hacking attacks. Any cyber related incident will be handled in accordance with police policies on cyber security. In the event that a cyber incident also involves a data breach then it shall remain subject to this procedure and the Data Protection Officer will work in conjunction with the police cyber security team.

When a breach occurs

In the first instance, and on the day of the breach the DPO should be notified of the matter. The Data Breach Template should be completed on the same working day and submitted to the DPO for review. If the breach is significant both the DPO and the SIRO should be notified immediately and unambiguously (ie in person, by telephone, or by an email which is acknowledged).

If the incident occurs out of hours the same individuals should also be contacted if the breach is significant, either directly or via a line manager.

Any incidents involving lost or stolen equipment or a network security issue should also be reported to the ICT Service provider's service desk immediately. For the purposes of this procedure lost or stolen hardware will be logged and may be subject to further investigation depending on the circumstances giving cause to the incident. The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained. It is the member of staff who has had the equipment stolen who is responsible for notifying the police.

The severity of an information security incident will be determined in accordance with the incident levels set out below:

Levels	Description
No Risk	No breach as data protected and no impact.
Low Risk	Breach of personal or business data but low risk and impact to individuals.
Medium Risk	Breach of sensitive personal or confidential personal or confidential business data and medium risk and impact to individual(s). The personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons.

High Risk	Breach of sensitive personal or confidential personal or confidential business data and high risk and impact to individual(s). The personal data breach is likely to result in a risk to the rights and freedoms of natural persons **Decision if to report to ICO** **Decision if to report to data subjects**

An incident will be rated in accordance with a risk classification based on agreed criteria for assessing the likelihood, severity and impact of risk. Matters to consider will include:

- The nature, sensitivity and volume of personal data.
- Ease of identification of individuals.
- Severity of consequences for affected individuals.
- Special characteristics of people that may be affected (e.g. age, vulnerabilities).
- The number of affected individuals.
- Nature of breach (e.g. error, mistake or intentional action and malicious).
- Financial or legal implications and reputational damage.

It is difficult to provide a definitive list of incidents by level as each case varies depending on the circumstances, including containment and recovery, which may reduce or escalate the level at any given point. An initial incident rating will be awarded upon incident notification and may change once the facts and impact of risks has been determined. Generally, the less serious incidents will involve encrypted data or low-level data including near misses whereby the severity is reduced due to swift remedial action. The more serious incidents will involve high level data which poses actual or potential high risk to people's rights and freedoms or to the organisation e.g. through the loss or release of highly sensitive personal or confidential business information.

The DPO will, seeking legal advice as appropriate:

- provide instructions on notifications to appropriate persons – eg data subjects
- consider whether any internal notifications or external stakeholder notifications are required to be made
- make notification to the ICO within 72 hours if required
- maintain a log of all information security incidents
- keep under review the risk severity assessment, and change category if required

The DPO will investigate the incident proportionally to the breach and risk severity assessment. If required a nominated individual may be asked to carry out the investigation. Investigation should be completed within 2 weeks, and a report produced noting (i) observations and conclusions about any information governance

non-compliance issues, risks, adverse consequences or implications; and (ii) remedial recommendations to mitigate the risks and impact including preventative measures to address areas for improvement and training needs with target dates for completion. Any repeat or previous similar incidents will be flagged in the final incident report and may result in additional or escalated action.

Where misconduct may have occurred, the disciplinary process will be used to determine any further action to be taken.

7. Sharing information with others

The OPCC will ensure that a Privacy Notice is published to outline what data is collected and processed about individuals. There are currently two privacy notices in place, one for general activity and the other for employee information. Both privacy notices are published on the OPCC website, which also has a cookie policy and a website privacy notice.

Where the Privacy Notice specifies that information is shared with other bodies, it is appropriate to ensure that secure arrangements are in place to ensure that information is safeguarded and shared appropriately. Where significant information is shared a DPIA will need to be conducted. In addition to this consideration should be given to the production of an Information Sharing Agreement, where a need is identified in accordance with this policy. The DPO will provide advice and arrange for Information Sharing Agreements to be created, in liaison with legal services, and will maintain a register of ISAs.

The OPCC is responsible for ensuring that personal data is shared fairly and lawfully and in a reasonable and proportionate way in compliance with the DPA. Information will only be shared where there is a statutory power to share and at least one lawful basis for sharing data has been identified. Advice should be sought on a case by case basis for large volumes of sensitive personal data, such as special categories of personal data.

When preparing an information sharing agreement the following should be considered:

- What is the sharing meant to achieve? What information do we need to share?
- Could the objectives be achieved without sharing personal data or by anonymising it?
- What risks does the data sharing pose to individuals? Consider physical, emotional, economic and social harms. Is any individual likely to object? Could it undermine individuals' trust in the organisations that keep records about them?
- Is it right to share data in this way? You should consider the potential benefits and risks, to both society and individuals, of sharing the data. Where

appropriate, ethics should form a part of those considerations. The proportionality of the data sharing exercise should be central to the analysis.

- What would happen if we did not share the data? The likely results of not sharing the data should also be considered.
- Are the OPCC allowed to share the information? Does the OPCC have the legal power to share the information? Is there a legal basis identified to share the information lawfully and fairly?
- Who requires access to the personal data? “Need to know” principles, should be adopted meaning that the OPCC should only share data to the extent that it is proportionate to do so: other organisations should only have access to OPCC data if they need it; and only relevant staff within those organisations should have access to the data. Are there any necessary restrictions the OPCC may need to impose on the onward sharing of data with third parties.
- When should the OPCC share it? Is the sharing to be an ongoing, routine process or should it only take place in response to particular events?
- How should the OPCC share it? What are the processes for sharing the data? This must include security considerations and procedures around the transmission of data, and access to it by all those involved.
- How can the OPCC check the sharing is achieving its objectives? The OPCC should refer to the objectives for sharing. What are the OPCC attempting to achieve by sharing this data? Being clear about this will help the OPCC measure whether the sharing has been successful including judging whether the data sharing is still appropriate, and whether the safeguards still match the risks.
- Are there any ethical factors that need to be borne in mind in addition to legal and technical considerations when deciding whether to share personal data?

8. Retention and Disposal of data and records

There are inherent risks attached to the retention and disposal of records which directly affect public confidence, legal issues and complaints legislation. The OPCC will take a common and consistent approach to the retention and disposal of records that seeks to balance proportionality and necessity. This will:

- prevent the premature destruction of records.
- provide consistency of preservation and destruction or records.
- improve records management.
- ensure adherence with legislation.

Records are retained for four main reasons, as follows:

- to provide evidence for actions undertaken and support transparent business decision making.

- to enable the OPCC to discharge its functions in a timely and effective manner.
- to comply with legislative and regulatory requirements.
- to preserve the OPCC's corporate memory.

Records will be retained for as long as required to comply with the requirements set out above and in line with the DPA 2018. Wherever there is a potential for litigation or a request under access to information legislation, the records that are likely to be affected should not be amended or disposed of until the threat of litigation or actual litigation has ceased including any appeal processes.

Records should be stored securely having regard to the sensitivity and confidentiality of the information and to avoid potential misuse or loss. Records should be easily identified and accessible to those who need to have access to them, including for resilience purposes. The OPCC operates a paper-free environment where possible but makes available secure storage where necessary.

Records marked for destruction should be disposed of through confidential waste processes.

In accordance with the timescales and actions detailed in the Retention Schedule a record must be maintained where information is archived or disposed of.

The DPA 2018 provides individuals, in certain circumstances, with the right to request correction of personal data held about them. This enables any incomplete or inaccurate information held to be corrected. Any changes made to a record needs to be made to each copy of the record. Having one copy of each record will assist with compliance to this obligation. Individuals also are entitled to object to their data being used, and to ask for their personal data to be deleted.

8.1 Retention Schedule

The majority of records that the OPCC holds are listed in the Retention Schedule. Records should be retained for the amount of time indicated in the Retention Schedule. All retention periods are shown in whole years. Where indicated within the Retention Schedule, some records will be retained indefinitely. A record must not be retained beyond the period indicated in the Retention Schedule, unless a valid reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention.

Any type of record may contain personal data; that is data that identifies living individuals. Personal data should not be retained longer than is necessary for the purposes for which it is processed (the principle of storage limitation). Staff should take into account the principle of storage limitation when deciding whether to retain any record. Where records containing personal data have been listed in the Retention Schedule, the OPCC has taken into account the principle of storage limitation and balanced this against the requirements to retain the data.

Some records do not need to be kept at all. In most cases, information which is duplicated, unimportant or of short-term use can be destroyed when it is no longer of any practical use, this might include: circulars, trivial email messages, out of date distribution lists, signing in books, hard copies of documents where an electronic copy has been created and saved.

The Retention Schedule will be reviewed annually, and this review will be led by the Head of Business Services.

9. Transparency and Publication of Information

The OPCC aims to share information transparently where it is in the public interest and primarily uses the OPCC website to do so. The OPCC maintains publication schemes to meet the requirements of the Specified Information Order and the Freedom of Information Act 2000, which are published on the OPCC website.

9.1 Specified Information Order (as amended)

The OPCC seeks to comply with the publication requirements outlined in the Specified Information Orders, listed below.

- The Elected Local Policing Bodies (Specified Information) Order 2011
- The Elected Local Policing Bodies (Specified Information) (Amendment) Order 2012
- The Elected Local Policing Bodies (Specified Information) (Amendment) Order 2013
- The Elected Local Policing Bodies (Specified Information) (Amendment) Order 2021

The publication scheme is based on the ICO model template for PCCs (described as local policing bodies.) The Head of Media and Communications is responsible for ensuring the required information is published.

9.2 Freedom of Information Act 2000

The Freedom of Information Act imposes a duty for a public body:

1. To confirm or deny that the information requested is held.
2. If the information is held, to communicate it to the applicant

Anyone may make a request for recorded information held by or on behalf of the OPCC. For the request to be valid under the Act, it should be in writing. It is preferred that requests are made to OPCC generic email address, but requests received through other routes will also be deemed valid, and although good practice, requests do not need to mention the Act. Requests under the Act will be logged in

order that their completion can be tracked and monitored. Once information is released it will also be placed on the OPCC website.

The OPCC must reply within 20 working days starting from the day after the request is received, unless more time can be allowed through an exemption. The OPCC will contact the requester if the request is not clear or further clarification is required, and the response time will commence once the request has been clarified. If the information is held by another organisation, the applicant will be directed to that entity.

The OPCC will determine whether the information can be released, in full, in part or not at all. In some cases the OPCC will neither confirm nor deny whether the information is held. If the OPCC does not hold the information, new information will not be created in order to respond to the request. Where an exemption is applied the relevant section of the Act will be quoted, and the requestor will be informed if a public interest test has been undertaken, in accordance with the ICO process. If the OPCC is to charge for the release of information, either for communication costs or due to the staff time it will take to respond to the request, the requester will be informed of this, and no information will be released unless fees are received.

A request may be refused if it will take too much staff time to fulfil the request. A time limit of 18 hours is applicable and it is the OPCC's usual policy to refuse requests which exceed the time limit. The OPCC will work with the requester to refine the request into something more manageable, so that information can be provided. It may also be refused if it is repetitious, vexatious or is a request for personal data which is in scope of the Data Protection Act.

If a requester is unhappy with the outcome of a FOI request, they can request an internal review. This should be requested within 40 days of the date of the outcome letter. The internal review will be conducted by the Chief Executive or someone not involved with the initial handling of the matter, and should be conducted within 20 working days, or 40 working days in certain circumstances. Information about the internal review process will be detailed in the response letter to the requester.

9.3 Environmental Information Regulations 2004

The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities. The Regulations do this in two ways; public authorities must make environmental information available proactively and members of the public are entitled to request environmental information from public authorities.

Anyone can make a request under the Act and requests can be made verbally or in writing. They must be responded to in writing and this should take place within 20 working days (starting from the day after the request is received). If a large volume of information is requested this time limit can be extended to 40 working days, and the OPCC will inform the requester of this.

If the information is held it will be shared unless one of the exemptions apply.

If a requester is unhappy with the outcome of a EIR request, they can request an internal review. The internal review will be conducted by someone not involved with the initial handling of the matter and should be conducted within 40 working days. Information about the internal review process will be detailed in the response letter to the requester.

10. Processing Special Category and Criminal Offence Data

As part of the OPCCs statutory and corporate functions, the organisation processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of GDPR and Schedule 1 of the DPA 2018 and as such must have an appropriate policy in place. This section of the policy explains the processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. In addition it provides some further information about the OPCC's processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements the privacy notice and staff privacy notice.

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.
- Criminal offence data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

10.1 Conditions for processing special category and criminal offence data

The OPCC processes special categories of personal data under the following of the UK GDPR Articles:

- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the PCC or the data subject in connection with employment, social security or social protection. Examples include monitoring and managing staff sickness absence and administering benefits such as statutory maternity pay.
- Article 9(2)(g) - reasons of substantial public interest. The PCC is a public authority and has certain powers and obligations pursuant to the Police Reform & Social Responsibility Act 2011. The PCC is statutorily required to secure the maintenance of the police force for Warwickshire and to secure that the police force is efficient and effective. The processing of personal data in this context is for the purposes of substantial public interest and is necessary for carrying out the role. Examples of processing include the information sought and received as part of (i) the PCC's handling of complaints against the Chief Constable, pursuant to the Police Reform Act 2002; and the PCC's duty under the Policing and Crime Act 2017 to review complaints handled by Warwickshire Police under Section 3 of the Police Reform Act 2002
- Article 9(2)(f) – for the establishment, exercise or defence of legal claims. Examples of processing include processing relating to any Police Appeals Tribunal cases or other litigation.
- Article 9(2)(a) – explicit consent. In the limited circumstances where the OPCC may seek consent, the office ensures that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of processing include staff dietary requirements.
- Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person. An example of the processing would be using health information about a member of staff in a medical emergency.
- The OPCC processes criminal offence data under Article 10 of the UK GDPR. Examples the processing of criminal offence data include pre-employment police vetting checks.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an appropriate policy document (see Schedule 1 paragraphs 1 and 5) and this section of the Information Management policy serves as the appropriate policy document for this purpose. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. The OPCC processes special category personal data in other instances where it is not a requirement to keep an appropriate policy document. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and staff privacy notice.

10.2 Descriptions of Data Processed

Special category data about employees is processed when it is necessary to fulfil obligations as an employer. This includes information about health and wellbeing, ethnicity, photographs and membership of any trade union. Further information about this processing can be found in the staff privacy notice. Processing for reasons of substantial public interest relates to the data received or obtained in order to fulfil statutory functions. For example, this may be information provided as part of a complaint against the Chief Constable. Further information about this processing can be found in the privacy notice.

The OPCC also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Special category data

We process special category data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1)** employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)** statutory, etc. purposes
- **Paragraph 8(1)** equality of opportunity or treatment
- **Paragraph 23(1) and (2)** elected representative responding to requests
- **Paragraph 24(1) and (2)** disclosure to elected representatives

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection
- **Paragraph 6(2)(a)** – statutory, etc. purposes

Securing compliance with the Data Protection principles (GDPR Article 5)

In summary the principles set out in Article 5 of the GDPR are as follows:

Principle (a): lawfulness, fairness and transparency

Principle (b): purpose limitation

Principle (c): data minimisation

Principle (d): accuracy

Principle (e): storage limitation

Principle (f): integrity and confidentiality (security)

In addition, Article 5 requires that the data controller is responsible for and can demonstrate compliance with the above principles (the accountability principle)

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing (in compliance with GDPR articles 6 and 9) in our privacy notice, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of functions conferred on the PCC pursuant to the Police Reform and Social Responsibility Act 2011.

Our processing for the purposes of employment relates to our obligations as an employer. We also process special category personal data to comply with other obligations imposed on the OPCC in its capacity as a public authority e.g. the Equality Act.

Principle (b): purpose limitation

We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our statutory functions, to comply with obligations under equalities legislation, for responding to requests or for disclosures to elected representatives.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose, through an information sharing agreement, based upon the ICO's data sharing statutory code of practice, which sets out good practice principles of information sharing with other data controllers.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it. We have in place arrangements for completing data protection impact assessments (see Section 6) and conduct DPIAs for high risk processing to ensure that any data that is processed is adequate for fulfilling our statutory requirements but not excessive for our needs.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in the section of this policy relating to storage and disposal of records (see Section 8). The retention period for data is based on our legal obligations and the necessity of its retention for our business needs.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within a secure ICT network provided by Warwickshire police force and the OPCC has adopted relevant police force ICT policies and procedures. Information is protectively marked in accordance with the government security classification scheme. The systems used to process personal data allow the erasure or updating of personal data at any point in time where appropriate.

We have in place mandatory training for staff in the secure handling of information which includes refresher training and briefing sessions. We have arrangements in place for reporting data breaches or near-misses (see Section 6) and staff are trained in the identification, containment and management of any breach of information, should this occur.

All our staff and volunteers are required to be police vetted in line with non-police personnel vetting requirements.

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer.
- Maintaining a record of our processing activities (ROPA).

- Adopting and implementing data protection policies and ensuring written contracts are in place with our data processors.
- Implementing appropriate security measures in relation to the personal data processed.
- Carrying out data protection impact assessments for high risk processing.
- Reviewing policies in a timely manner

11. Revision Record

Date of change	Nature of revision
March 2024	Consolidation of a number of standalone policies