OPCC
Office of the Police & Crime Commissioner for Gloucestershire

Information Sharing Agreement

Office of the Police and Crime Commissioner for Gloucestershire

and

Gloucestershire Constabulary

1. Introduction

This Information Sharing Agreement (ISA) has been introduced to regulate sharing of personal data between the Chief Constable of Gloucestershire Constabulary and the Police and Crime Commissioner for Gloucestershire (OPCC), referred to as the "parties".

This agreement has been developed with reference to the Data Protection Act 1998, the Police Reform and Social Responsibility Act 2011 and the Policing and Crime Act 2017 and to the Policing Protocol (SI 2011/2744).

This agreement has been developed to:

- Define the purposes for which the Parties have agreed to share information
- Describe the roles and structures that will support the exchange of information between parties
- Set out the legal gateway through which the information is shared
- Describe the security procedures necessary to ensure compliance with agency specific security responsibilities and requirements
- Describe how this arrangement will be monitored and reviewed

This ISA is not intended to cover information sharing between either party and the Police and Crime Panel, nor any partnership agencies.

2. Purpose

The purpose of this document is to set out the terms and conditions under which data held by Gloucestershire Constabulary will be shared with the OPCC and vice versa. This agreement recognises that effective joint working is vital in the prevention and detection of crime, providing support to victims and witnesses, dealing with complaints and reviews and meeting the expectations of the public.

The Police and Crime Commissioner (PCC) is required by law to hold the Chief Constable to account for the effective and efficient policing of Gloucestershire.

Through the legislation listed at 1, above, the PCC is obliged to:

- Ensure the maintenance of the police force for Gloucestershire
- Ensure that the force is efficient and effective
- Hold the Chief Constable to account for the performance of the force and for the exercise of the functions under the direction and control of the Chief Constable
- Set the police budget, the police share of Council tax and the local 'Police and Crime Plan' which sets out the overall strategy for policing in the area
- Monitor and take a role in police complaints

In order to successfully fulfil these functions, the PCC and the OPCC will need to be supplied by Gloucestershire Constabulary with relevant information about policing matters. The PCC holds an electoral mandate and a public leadership role and, as such, will receive complaints and enquiries about policing matters and other matters within the role of the PCC. Liaison with and the exchange of information with the Chief Constable is necessary in order to ensure and maintain public confidence and provide the best service to the public and those making complaints and enquiries.

Section 36 of the Police Reform and Social Responsibility Act 2011 requires that the Chief Officer of Police must give the relevant elected local policing body (i.e. the PCC) such reports on policing matters that the body may require the Chief Officer to give. The Act also states that such information must be in a form (if any) specified by the elected local policing body.

The Chief Constable of Gloucestershire will provide the OPCC access to Gloucestershire Constabulary information technology systems. This will include all relevant applications required for the OPCC to carry out their role. This will not only provide access to a great deal of required information (e.g. intranet, performance management, HR, finances etc.) but will ensure that costs are reduced by sharing the same technology systems.

The PCC and the OPCC will also require reports and information to be provided from Gloucestershire Constabulary to enable the PCC to carry out effective oversight. These reports will include (but are not exclusive to):

- Financial and budgetary reporting
- Budget planning information
- Information about Gloucestershire Constabulary performance
- Complaints, reviews and associated data
- Information on specific operational queries
- Human resource and diversity monitoring information
- Anti-Social behaviour data to fulfil wider community safety responsibilities
- Information with regard to change programmes and business planning
- Any other information that will allow the PCC to exercise their governance role

Where possible, the OPCC will itself access and use Gloucestershire Constabulary information where it has a lawful purpose and access rights to do so. Reports will be requested where that information is not readily accessible or where it requires interpretation, comment or context from Gloucestershire Constabulary in order for the PCC to best use the information.

Normal practice with regard to freedom of information (FOI) requests will be observed by both Gloucestershire Constabulary and the OPCC. The OPCC will, therefore, use the same procedures for FOI and Subject Access requests as the constabulary, unless notified otherwise.

Details of the Gloucestershire Constabulary FOI process can be found here. Details of the OPCC FOI process can be found here

Complaints

Part Two The Policing and Crime Act 2017 is likely to be enacted in February 2020 and seeks to make a number of changes to the handling of police complaints in order to increase confidence in, and improve the efficiency and effectiveness of, the complaints process. It seeks to strengthen the role of PCCs in the complaints process by introducing mandatory duties for PCCs, namely an explicit duty in relation to oversight and performance of the complaints process and for PCCs to become the body to deal with all reviews, previously known as appeals and dealt with by the Chief Constable, known as 'Model 1'.

The new legislation will allow PCCs to delegate their complaint handling powers and, locally, the current PCC has agreed that the recording, handling and management of complaints will remain the function of the Constabulary, overseen by the Professional Standards Department. The review function will be delegated to the Independent Review Officer.

In order to carry out the functions outlined in Model 1, access to the Constabulary's MIS, UNIFI, Storm and MG Wizard systems is required by the key personnel directly involved in handling

complaints and reviews, as well as requiring limited access (by specific, relevant personnel) to the Centurion system. Access to these databases and data will be limited to only those persons within the OPCC who have a role and function to play in the handling of reviews and the oversight and performance of the complaints process, namely the Contact and Complaints Officer, Independent Review Officer, Head of Policy, Performance and Strategy and, the Chief Executive Officer. Further details regarding the sharing of specific complaints and review data can be found at 4, below.

3. Powers/ Legal Framework

The principal pieces of legislation that should be considered when sharing information under this agreement are:

- Police Reform and Social responsibility Act (2011)
- Policing and Crime Act 2017

Information, including personal data, may be shared by the parties in order to allow each to fulfil their statutory functions. In addition, if not required for statutory purposes, such data may be supplied with the consent of the subject(s) of the data for the better performance of their respective roles.

4. The Agreement

This agreement relates to any personal or confidential information, irrespective of the medium in which it is held e.g. paper based, electronic, images or disc. Legal advice on this agreement should be sought in any case of doubt. It should be applied while following established and agreed processes within the signatory organisations.

4.1 Complaints

Access by the OPCC to Policing information in respect of its statutory Review role in respect of complaints under the Policing and Crime Act 2017.

- It is accepted that the OPCC's Independent Review Officer and Contact and Complaints Officer routinely require access to Gloucestershire Constabulary's core policing data systems (including but not limited to Storm, Unifi, MG Wizard) in order to carry out its statutory duties in respect of Reviews of decisions made by the Professional Standards Department in complaints matters. The IOPC Guidance makes plain that the Chief Constable is required to provide the Relevant Appeal Body (OPCC) with all relevant material that is reasonably required to carry out its statutory Review role;

- The OPCC's Independent Review Officer and Contact and Complaints officer shall therefore be provided with the relevant limited electronic access to all relevant Gloucestershire Constabulary's core policing systems in order to properly fulfil such duties. The Head of Policy, Performance and Strategy and the Chief Executive will have limited access in order to undertake the complaints duties of the Contact and Complaints Officer and as line manager to the Independent Review Officer where it is necessary to do so (e.g. absences from the office)

- Such access shall, however, be limited to the carrying out of such Reviews only. Information obtained by the Independent Review Officer or the Contact and Complaints Officer for the purpose of carrying out a Review shall not be used for any other purpose whether by the Independent Review Officer or Contact and Complaints Officer, or by any other member of OPCC staff.

4.2 Non Complaints matters

In line with the Act as outlined above, the following principles will be applied when sharing information between the parties:

- The default will be to share all information required for the PCC to carry out their functions in an open and transparent way
- Information requests will not interfere with operational policing e.g. there should be no need to routinely request information about individual offenders or victims, unless of high profile or public concern, or for the purposes of managing complaint reviews. There will be exceptions to this but these will be dealt with on a case by case basis, with a full rationale in writing submitted to the Data Controller for the appropriate agency.
- Information requests will be proportionate, for a clearly defined purpose and will not place an unreasonable administrative burden on either party in this agreement and will seek to avoid unnecessary duplication of work
- Data shall be shared using secure systems and when no longer required shall be disposed of securely in accordance with agreed procedures. This includes but is not limited to: retention periods, breach policies, training policies and privacy impact assessments
- Gloucestershire Constabulary, the PCC and the OPCC will work together to resolve any differences and find an appropriate way forward for working together
- Personal data will be shared when it is the only effective way to allow the parties to fulfil their respective roles
- When practicable, personal data will be anonymized or provided with pseudonymity but only where this will not impact on the ability of the parties to fulfil their statutory functions
- The data will not be further shared without the other party's consent, and then only to organisations within the EU or EEA having similar security arrangements
- The parties will make the data available after it is shared only to those who need to have it to carry out their functions
- The effectiveness of this agreement will be reviewed by the parties annually
- Special category data may also be shared pursuant to this agreement but usual additional consideration as to the need to share it in order to allow the parties to fulfil their statutory obligations will be given
- The OPCC will observe the requirement of the constabulary with regard to vetting and physical security of officers, systems and offices where data is shared. The Head of Governance and Compliance is the single point of contact (SPOC) for all matters related to information sharing. The SPOC will advise on the legality and practicality of sharing data. As much notice as is reasonably possible should be given to request. However, this should be at least 10 working days for formal information requests. All information should be provided back to the OPCC as soon as practicable in a timely manner. Officers in the OPCC have access to force systems and have contacts with force colleagues in their area of business and will use these contacts as appropriate for less formal requests. Unmarked documents that are shared between the parties are presumed OFFICIAL.

Information classified as OFFICIAL includes:

- The day to day business of policing, including crime records and intelligence
- The majority of public safety, criminal justice, and law enforcement activities
- Many aspects of defence, security, and resilience
- Any commercial interests, including information provided in confidence and intellectual property
- Personal information that is required to be protected under legislation

OFFICIAL SENSITIVE is sub category of OFFICIAL used to denote particularly sensitive personal, operational or other data where inappropriate access may have damaging consequences for the individual or organisation. If correspondence bears this marking it should NOT be shared without the express permission of the originator and in accordance with the handling instructions.

It is the responsibility of each signatory to ensure that:

- Information shared is in accordance with the law
- Appropriate staff training and awareness sessions are provided in relation to this agreement

- Information is shared responsibly and in accordance with professional and ethical standards
- All information is shared, received, stored and disposed of securely
- Any restrictions on the sharing of the information contained in the disclosure, in addition to those contained within this agreement, should be clearly noted
- Information refusals will be recorded in such a way as to provide an auditable record
- Any electronic information exchange is fully secure (to IL/3 standard, e.g., those email addresses with PNN or GSI etc. extensions)
- Arrangements are in place to check that this agreement, its associated working practices, and legal requirements are being adhered to
- Any data will only be used for the specific purpose for which it is shared, and recipients will not release information to any third party without obtaining the express written authority of the Gloucestershire Constabulary SPOC, including requests from the public
- The PCC and the OPCC must have been trained in appropriate procedures for the secure handling of Gloucestershire Constabulary information. NCALT training is available and should form part of the induction process for new staff and annually thereafter.

5. Movement, Storage and Disposal of information

OPCC information will be kept on the OPCC secured shared drive, in folders which only members of the OPCC have access to. Access permissions to these folders are only granted on a 'need-to-know' basis and access to the Gloucestershire Constabulary network is only possible with an individual username and password.

Constabulary information will be kept on its own secured shared drives, in folders which only relevant members of the Constabulary have access to. Access permissions to these folders are granted on a 'need-to-know' basis and access to the network, its secure systems and databases is only possible with an individual username and password.

When information is shared, it should be done so in the most appropriate manner at that time and in accordance with the general principles of GDPR and the agreed policies of the parties.
The ways in which information may be shared are likely to include:

- Verbally (e.g. meetings or via telephone)
- In hard copy (e.g. reports, forms, printouts, documents)
- Digitally (e.g. secure email, access to IT systems, digital media, video-conferencing

Should information be shared in hard copy format, it will be the printing party's responsibility to keep the information secure by measures such as storing documents in a locked container when not in use. Access to printed documents must be limited only to those with a valid 'need-to-know' that information.

Both parties adhere to the clear desk policy where information will only be accessed when needed and stored correctly and securely when not in use.

All data will be disposed of in line with the party's data retention policies on an annual basis and / or once it is no longer needed. If information is printed off an electric system, parties will ensure that the papers will be disposed of either via their confidential waste disposal system, or via a cross-shredder. Security ISO/IEC 27002:2013 code of practice for information security management provides a baseline for security arrangements. Parties should ensure they have appropriate security arrangements in place. Certification For ISO/IEC 27002:2013 may not be possible for some partners, but both parties should seek to comply with the principles it contains.

Should a party receive any request for information (such as Subject Access request or Freedom of Information Request) that concerns information that should be provided by the other party, they will advise the person making the application as soon as possible and request permission to reallocate the request for information to the correct party

6. Liability

It is agreed that each party is responsible for their own breaches and that any breach made by an officer or employee of that party will be the subject of an internal inquiry, carried out by the party responsible for the breach.

All information that is disclosed under this agreement remains the property of the original data owner, and partners must obtain expressed permissions from the original owner prior to further dissemination. The original data owner is responsible for the accuracy of its information, and must inform partners of any subsequent changes to it. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants, or agents. Any disclosure of information by an employee which is made in bad faith, or for motives of personal gain, will be the subject of an internal inquiry and be treated as a serious matter. It is the responsibility of the party to ensure it complies with this agreement and any associated legislation.

It is understood that breaches of this agreement could lead to the termination of this agreement, and the destruction of all previously shared information. All breaches must be reported to the relevant Data Controller of the other party within 24 hours of being made aware of a breach. If the data is jointly owned, the party responsible for the breach will be responsible for reporting that breach, however, the other party should also be made aware of the breach as soon as possible. Both parties will provide reasonable assistance to the other when handing a data breach and each have a process and/or policy in place on how the reporting and investigation of breaches is to be managed.

In the event of action in respect of a data breach being brought by a data subject or the Information Commissioner's office (ICO) concerning the processing for shared personal data, against either one or both parties, each party will inform the other about any such action and will cooperate with a view to settling them amicably and in a timely fashion.

7. Management and Operation of the Protocol

This ISA will be active from January 2020. The review of this protocol will be completed 6 months after commencement, and annually from the date of commencement thereafter or after an appointment of a new PCC, Chief Constable or Data Controller for the OPCC. This will be undertaken by both parties. The purpose of the review is to ensure it is fit for purpose, covers all that is required and is neither too extensive nor too narrow for its purpose. The OPCC will adopt the information management policies of Gloucestershire Constabulary where possible, although it may, after consulting with the Gloucestershire Constabulary SPOC or Chief Constable, adapt those policies where appropriate.

Signatories to this agreement shall grant the Chief Executive, Head of Policy, Performance and Strategy and the Head of Governance and Compliance or delegated persons all reasonable access to enable an audit to take place to ensure compliance with the information management, and security requirements & obligations of this agreement. Signatories shall provide all reasonable assistance to enable the audit to be completed. Each signatory can exercise its right under this agreement to audit compliance in relation to its own information shared with the other party.

Both parties agree that they may withdraw from the ISA upon giving written notice to the other party. A party who does withdraw must continue to comply with the terms of this ISA in respect of any information previous provided by the other party. Notwithstanding this, any party who withdraws from the ISA must continue to comply with the requirements of the Police and Crime Act, Police and Social Responsibility Act and the Policing Protocol, as is required by statute.

Both parties agree that this ISA can be made available to the public in its entirety.

8. Signatories to the agreement

By signing this agreement, the parties acknowledge and accept the requirements placed upon them and others within their organisations by the agreement.

Chief Constable, Gloucestershire Constabulary

Print Name ..... R HANSEN .....

Signatory ..... R. Hansen .....

Dated ..... 3.2.2020 .....

Chief Executive, Office of the Police and Crime Commissioner for Gloucestershire

Print Name ..... RICHARD BRADLEY .....

Signatory .....

Dated ..... 29.1.20 .....

Police and Crime Commissioner for Gloucestershire

Print Name ..... MARTIN SURL .....

Signatory .....

Dated ..... 21/1/2020 .....