



STAFFORDSHIRE
POLICE

Information Sharing Agreement

Staffordshire Police
And
Keele University

Version	Version date	Requester of change	Summary of change(s)
0.1			Ist Draft
0.2			Accepted amends
1.0			Final version

DOCUMENT REFERENCES

Ref	Document Name	Version Number

Contents

1 Introduction	3
2 Purpose	3
3 Powers and Legal Framework	3
4 The Agreement	6
5 Data-Sharing Protocol	7
6 Publication	9
7 Security	9
8 Liability	10
9 Management and Operation of the Protocol	10
10 Signatures	11
Appendix A: The Lawful basis' for processing Personal Data within UK GDPR	12
Appendix B: The Conditions for processing Special Category Data within UK GDPR	13
Appendix C: Flowchart of When and How to Share	14
Appendix D: Definitions	15
Appendix E: Confidentiality Agreement	17

1 Introduction

No current formal information sharing arrangements are in place for the sharing of information between Keele University and Staffordshire Police. This agreement seeks to clarify the arrangements as the data controller (in this case the Chief Constable) there are certain responsibilities that that are responsible for and this agreement seeks to formalise these.

2 Purpose

The purpose of this document is to set out the terms and conditions under which data held by Staffordshire Police will be shared with Keele University. This framework recognises that effective joint working is vital in the prevention of crime, protecting the public, and helping those in need.

The purpose of sharing this information is to enable academic research to assist in extending our understanding as to why policing activity is disproportionate to ethnic minority communities. The data will all be anonymised therefore the risks of sharing this data are minimal whilst the benefit of developing our understanding in this area of policing is significant. It is hoped that this research will enable policing to make operational and organisational changes to deal with the root causes of disproportionality of service.

The data to be shared includes:

- Describe briefly what information is to be shared, is generalised anonymous data that contains characteristics of locations, persons involved, times, dates and outcomes

This purpose is consistent with Staffordshire Police's obligations under the Data Protection Act 2018, and The Law Enforcement Directive (EU/2016/680), effective from May 2018, including being consistent with the original purpose of the data creation / collection.

3 Powers and legal purpose

The principal legislative instruments that should be considered when sharing information under this agreement are:

- The Crime and Disorder Act (1998)
- The Data Protection Act (2018)
- EU Directive 2016/680 - The Law Enforcement Directive
- The Freedom of Information Act (2000)
- Human Rights Act (1998)
- The Rehabilitation of Offenders Act (1974)
- Common Law Powers of disclosure

There are other pieces of legislation that place powers or duties to share information on public authorities – this list is not meant to be exhaustive. All information sharing must be conducted in accordance with one or more of the legal powers / duties.

3.1 Data Protection Principles

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the UK GDPR requires that personal data shall be:

#	Principle Description	Example(s) ¹	Evidence/Rationale
1 st principle	a) Processed lawfully, fairly and in a transparent manner in relation to individuals;	The lawful basis for collecting the data: PUBLIC TASK	To support research into disproportionality to improve policing in Staffordshire
2 nd principle	b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;	Data to be collected for the purpose of academic research on disproportionality of service to BAME communities; data to be processed by Keele University and not transmitted further	The data will assist in identifying where disproportionality of service takes place, which communities are impacted, which crime types are relevant – Data will be shared in Excel format, password Protected and sent to secure email address
3 rd principle	c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	Names, Dates of Birth, addresses will be redacted.	Ethnicity will be collated along with crime locations Stop & Search Arrests Use of Force Complaints Drugs Incidents Crime Types (Burglary, Robbery, Violence, Drugs) Customer Satisfaction Crime Survey England & Wales (Staffordshire figures) May also provide Resource data in the future
4 th principle	d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	Updates to the data set will be communicated by SP to Keele University who will update details accordingly	describe how the data will be maintained as accurate and up to date These will be one off datasets

¹ This example text to be removed during completion of the template

5 th principle	e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ²	All data will be disposed of after 2 years and no copies will be kept	describe how and when the data will be disposed of OR describe the rationale for keeping the data longer and why it is in the public interest Two years is in line with standard retention policy.
6 th principle	f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	Data to be protected by digital encryption, etc.	The datasets will be password protected and sent to Keele University secure email address

Article 5(2) requires that: “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

For each principle, insert the relevant details into the table above in the ‘Evidence/Rationale’ Column. There is further guidance in sections 3.2 – 3.3 below.

3.2 Special Category Data

Special category data is defined as more sensitive within UK GDPR, and so needs more protection. For example, information about an individual’s:

- Race or Ethnic Origin
- Political opinions
- Religious or philosophical beliefs
- Trades union membership
- Genetic data
- Biometrics (where used for the purposes of identifying a natural person)
- Health
- Sex life
- Sexual orientation

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 (See 3.1 of this document) and a separate condition for processing special category data under Article 9(2) and Article 10 for Criminal Convictions. These do not have to be linked.

The Conditions for processing Special Category Data within UK GDPR (Article 9) are listed in Appendix B. Articles 9 and 10 of the UK GDPR prohibit the processing of such data unless the special conditions, set out in Articles 9(2) and 10 respectively, are met.

The special conditions which allow processing of special category personal data include:

² personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

- Article 9(2) (b) – for employment, social security and social protection purposes.
- Article 9(2) (g) – for substantial public interest purposes.
- Article 9(2) (h) – for health and social care purposes.
- Article 9(2) (i) – for public health purposes.
- **Article 9(2) (j) – for archiving, research and statistics purposes.**

Article 10 requires that the processing of criminal convictions data is prohibited unless it is carried out under the control of official authority or if it is authorized by UK law. Member states may authorize the processing of criminal convictions personal data in specific circumstances and subject to appropriate safeguards.

Is Special Category Data included? Yes, the special condition being

- **Article 9(2) (j) – for archiving, research and statistics purposes.**

4 The Agreement

This ISA applies to any personal or confidential information, irrespective of the medium in which it is held e.g. paper based, electronic, images. 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.

Under no circumstances should information shared by Staffordshire Police be retained by the partner agency for longer than is necessary to achieve the purpose specified in this agreement. To gain an exemption to this, a specific request must be sent to Staffordshire Police, who then, following a review, determine if the information can be retained. Files containing information from partner sources will be reviewed in line with force policy.

This agreement does not give agencies an automatic right to receive information or a mandate to provide information, but is a process for information sharing in cases in where it is suitable to do so. By signing up to this agreement, signatories are committed to a positive approach to information sharing, and agree to meet the outlined commitments and processes.

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, and that their organisation abides by this document
- Information is shared responsibly and in accordance with professional and ethical standards
- All information is shared, received, stored, and disposed of securely
- Users consider adding the Government Security Classification to documents being shared with partners, including relevant handling instructions where appropriate

- Users adhere to baseline controls for handling police information (Appendix E) in addition to any stipulated handling instructions
- 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 exchanges and refusals are recorded in such a way as to provide an auditable record
- Any electronic information exchange is fully secure to UK Government standards (e.g. those email addresses with .pnn, .cjsm, .gsi, .gsx, .nhs, .gcsx, or .mod 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 disclosing partner, including requests from the public
- Arrangements are in place for data subjects to access to Personal Data if requested

5 Data-Sharing Protocol

Any information exchange should meet one or more of the following policing purposes: protecting life & property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law.

Where information to be shared relates to an ongoing investigation, or is awaiting a court outcome, the Officer in Charge of the case will be consulted prior to information sharing taking place in order to manage risk, harm, and the integrity of the judicial system. Information does not need to be exclusively shared with Staffordshire Police but can be shared directly between partners within this agreement. Any information that is shared between partners, consent must be obtained from partner who provides information prior to sharing with any other organisation.

5.1 Specific Procedures

Data List *(please list all the data fields required):*

Ref Number	
Type of Data (Eg Stop & Search, Complaint, Crime Type)	
Beat / Beat Name or NPT Location	
Location Post Code	
Time of Event	
Date of Event	
Officer Collar Nos (for any future analysis)	
If the offender is in IOM	
Outcome	
Satisfaction Questions / Results	

Crime Survey England & [REDACTED] Questions / Results	
Person characteristics (offender/suspect/victim/person stopped): Age Gender Ethnicity	

Access to the data shall be restricted to the following people:

Name	DoB	Vetting
[REDACTED]	[REDACTED]	Level 3
[REDACTED]	[REDACTED]	Level 2
[REDACTED]	[REDACTED]	Level 3
[REDACTED]	[REDACTED]	Level 3

Should any additional people need access to the data, please notify SP to seek approval prior to access to the data being granted

The Confidentiality Agreement contained in Appendix E will require the signatures of all the listed people receiving access to the data. The confidentiality obligations set out in this agreement shall continue in full force and effect after the expiry or termination of this agreement.

People nominated in the above list should be made aware of the terms of this Information Sharing Agreement.

How Data will be Gathered and how it will be transferred: <i>(Delete as appropriate)</i>	SP to gather data and transfer to partner SP to gather data, sanitise and transfer to partner Partner to gather data and transfer using SP systems – Partner to gather data, sanitise and transfer using SP systems. Email to non-secure email using 7-ZIP and password encryption Email to secure email using 7-ZIP and password encryption 7-ZIP and password encrypted data on disc 7-ZIP and password encrypted data on password encrypted memory stick
--	--

Systems To Be Accessed by researcher if applicable	
---	--

Information accessed on SP systems by partners will only be data relevant to the research purpose detailed in this agreement. SP understands that partners may inadvertently see additional information, however, it is expected that this information is kept confidential, not included in the data extraction and treated with due care. Suitable times/dates to access systems in SP premises needs to be arranged with a member of the Evidence Based Practice Team in advance. Please note that research can only be conducted between 08:00 – 17:00.

Data extracted from SP systems will be dip sampled by a member of the Evidence Based Practice Team prior to removal/transfer from SP premises. Any requirements to be met by partners will be discussed accordingly prior to removal/transfer (for example, where the data has not be de-identified completely.)

The data will generally be processed within:	Anonymised transcripts and field notes may both be stored on the secure server at Keele University or on password protected personal laptops during data analysis phases. No personal data will be stored on personal laptops
Security measures in place whilst processing data: <i>Some examples-</i> <i>Emails securely deleted if data transferred to server</i> <i>Processed in a room that has restricted card swipe access</i> <i>Stored on a secure server</i> <i>Password access to data on server</i> <i>Devices used – Type/level of encryption</i>	Keele University secure server and on a password protected, identity card-accessed, secure computer within

Proposed Research Start Date	Jan 2021
Proposed Research End Date	Jan 2024

Contact List:

SP Evidence Based Practice Team	██████████	████████████████████
SP Project Lead	Ch Supt	██████████
Project Manager/Lead Researcher	Head of Knowledge Hub	██████████

6 Publication

Personal data used for research will not be published in identifiable form unless the persons concerned have given their consent and in conjunction with other safeguards set out in domestic law.

Staffordshire Police will review any articles, including dissertations, or other materials, prior to publication. Staffordshire Police may request the deletion of any material that it considers inaccurate. If any material is considered, in the opinion of Staffordshire Police, to be harmful to the reputation of Staffordshire Police, a discussion as to how the material can

be reported will be held between you and Staffordshire Police. This may include steps such as fully anonymising any involvement of Staffordshire Police in subsequent publications

Staffordshire Police will have an interest in the outcome of the research as well as the finished product. **Upon completion of your research, a copy of your finalised research paper must be sent to the SP Evidence Based Practice Team.** This will be kept on record with the force, published onto our force internal intranet research page, and potentially referenced to or utilised in the future.

You may also be asked to present your findings or recommendations to the Staffordshire Police Executive Team or at a force meeting or event.

7 Security

Keele University agrees to apply appropriate security measures commensurate with the requirements of principle 7 of the Data Protection Act (1998),. In particular, they will ensure that measures are in place to do everything reasonable to mitigate against risks including accidental or unauthorised access, destruction or loss, use, modification, or disclosure of personal data.

Keele University will ensure that appropriate security measures shall be applied at all times. Whilst certification to ISO/IEC 27001:2013 may not be possible for some partners, all signatories should seek to comply with the principles contained in the ISO/IEC 27000 series.

Appendix E details the Minimum Protective Measures which must be in place under the Government's General Security Classification for OFFICIAL and OFFICIAL-SENSITIVE categories. Partners should ensure they have appropriate security arrangements in place.

8 Liability

Staffordshire Police cannot be held responsible for breaches of this protocol by the partner agency or complaints arising from these breaches. The partner agency is not responsible for breaches of this protocol by Staffordshire Police, or complaints arising from these breaches.

All information that is disclosed under this agreement remains the property of the original data owner (Data Controller), and partners must obtain expressed permission 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 partner to ensure it is compliant 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.

Complaints and breaches must be dealt with by utilising each signatories' established policies and procedures for breaches and complaints. Breaches and any immediate action taken to mitigate the risk caused by that breach must be notified to the originating partner as soon as is practicable, and in any case, within 72 hours.

9 Management and Operation of the Protocol

This ISA will be active from 25th Jan 2021. Where an organisation is an existing signatory to the protocol, but the signing Chief Executive or Director has left, the organisation will remain as a signatory; it is not expected that they re-sign and pursue the ISA, unless they wish to do so.

The review of this protocol will be completed 6-months after commencement, and annually from the date of commencement thereafter. This will be undertaken by both partners and coordinated by Staffordshire Police. 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.

Staffordshire Police may want to request a copy of the partner's information security policy (where it exists) when sensitive personal data is to be shared.

Signatories to this agreement shall grant Staffordshire Police Information Management and Information Security Teams all reasonable access to enable an audit to take place to ensure compliance with the information management, and security requirements and other obligations detailed in this agreement. Signatories shall provide all reasonable assistance to enable the audit to be completed. The signatory can exercise its right under this agreement to audit compliance in relation to its own information shared with Staffordshire Police.

Failure to supply sufficient guarantees in respect of security arrangements, or to comply with monitoring processes is likely to result in the termination of the agreement. Staffordshire Police may terminate this agreement at any time, and without notice, by providing written notice to Keele University, if Keele University is in material breach of any obligation in this agreement.

10 Signatures

All agencies that are part of the information sharing process will be, upon signing this agreement, bound to comply with its terms.



Within Staffordshire Police, the signatory is signing on behalf of the Chief Constable of Staffordshire Police.

Signed on behalf of SP –	Signed on behalf of Keele University
Print Name: [REDACTED]	Print Name: [REDACTED]
Signed: [REDACTED]	Signed: [REDACTED]
Role/Job Title: Chief Superintendent	Role/Job Title: [REDACTED]
Organisation: Staffordshire Police	Organisation: Keele University
Date: [REDACTED]	Date: [REDACTED]

Appendix A: The Lawful Bases for processing Personal Data within GDPR

	(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
	(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
	(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
	(d) Vital interests: the processing is necessary to protect someone's life.
	(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

	(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)
--	--

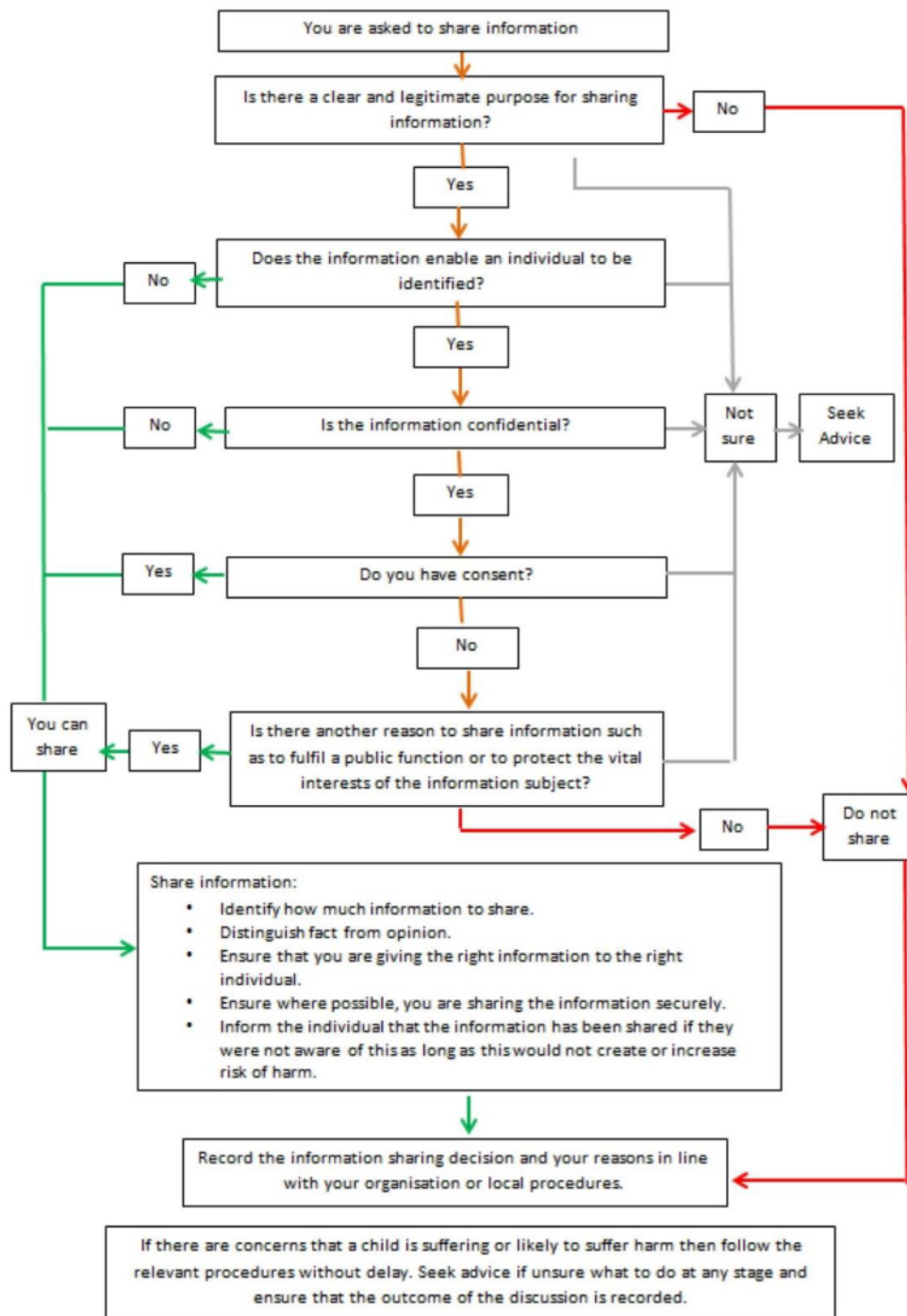


Appendix B: The Conditions for processing Special Category Data within GDPR

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Appendix C: Flowchart of When and How to share

Flowchart of when and how to share information



Source: Information Sharing (HM Government March 2015)

Appendix D: Definitions

Anti-social behaviour

Anti-social behaviour is defined as acting in a manner, which causes or is likely to cause harassment, alarm, or distress to one or more persons who are not of the same household.

Confidential information

Confidential information is covered by the common law duty of confidence. It applies to any information that has been received or accessed in circumstances where it is reasonable to expect that the information will be kept secret or should only be shared with a limited number of specific people.

Consent

Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Crime

- A crime is defined as any act, default, or conduct prejudicial to the community the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

Data in the public domain

- This type of information incorporates any information, which is publicly available, whether it relates to an individual or not.

De-personalised and aggregated information

Where de-personalised or aggregated information is no longer sensitive or identifiable it may be shared outside of the scope of this agreement. However, where de-personalised or aggregated information may still be deemed sensitive (e.g. as a result of complexity, currency, potential for misinterpretation or misuse) it must still be treated with care under the provisions of the ISA.

Disorder

- Disorder is considered to be the level or pattern of anti-social behaviour within a particular area.

Information about someone who has died

The Data Protection Act 1998 does not apply to information about people who have died. However, such information may still be sensitive, confidential or relate to individuals who are still alive. Information about people who have died must still be shared under the provisions of the ISA.

Information sharing

Information Sharing involves a physical exchange of information between one or more individuals or agencies. Any disclosure of personal information must be bound to both common and statute law, as described in this section.

Personal data

Personal data is defined under the Data Protection Act 1998 as anything that relates to a living individual in which the individual can be identified:

- Directly from the information (e.g. name and address), or
 - From the combination of this information with other information that may be readily accessible (e.g. address but not name), and
 - Which affects the privacy of the subject, whether in personal, family, business or professional life.
- 

Processing of Personal Data

Defined in GDPR in relation to personal data means an operation or set of operations which is performed on personal data or sets of personal data such as;-

- a) Collection, recording, organisation, structuring, or storage,
- b) Adaptation or alteration
- c) Retrieval, consultation or use
- d) Disclosure by transmission, dissemination, or otherwise making available
- e) Alignment or combination
- f) Restriction, erasure or destruction

Sensitive personal data

Sensitive personal information is defined under the Data Protection Act 1998 as any 'personal data' relating to: racial or ethnic origin; political opinions; religious or similar beliefs; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence; any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.



Appendix E: Confidentiality Agreement

Undertaking of Confidentiality

I, **[print name]** as an employee of the Data Processor involved in the work as defined in this Agreement to which this Undertaking is appended, hereby acknowledge the responsibilities arising from this Agreement.

I understand that my part in fulfilling the Purpose means that I may have access to the Police Data and that such access shall include:

- a) reading or viewing of information held on computer or displayed by some other electronic means, or
- b) reading or viewing manually held information in written, verbal, printed or photographic form.

I undertake that; -

1. I shall not communicate to, nor discuss with any other person, the contents of the Data except to the Data Controller or an official representative or to another Approved Researcher.
2. I shall not retain, extract, copy or in any way use any Police Data to which I have been afforded access during the course of my duties for any other purpose.
3. I will only operate computer applications or manual systems that I have been trained to use. This training will include the requirements of Data Protection Act 2018, with reference to the General Data Protection Regulations (EU 2016/679) and The Law Enforcement Directive (EU/2016/680), which prescribes the way in which Personal Data may be obtained, stored and processed.
4. I will comply with the appropriate physical and system security procedures made known to me by the Data Controller or a representative.
5. I will act only under instructions from the Data Controller, or other official representative in the processing of any Data.

I understand that the Police Data is subject to the provisions of the Data Protection Act 2018, with reference to the General Data Protection Regulations (EU 2016/679) and The Law Enforcement Directive (EU/2016/680), and that by knowingly or recklessly acting outside the scope of this Agreement I may incur criminal and/or civil liabilities.

I undertake to seek advice and guidance from the Data Controller or other relevant official representative of the Data Controller in the event that I have any doubts or concerns about my responsibilities or the authorised use of the Police Data defined in the Agreement.

I have [redacted] understood and accept the above.

Signed [redacted]

Name [print] ... [redacted]

25th February 2021

Date