Appendix 1 – Safer City Partnership Information Sharing Agreement

THE CITY OF LONDON

PROTOCOL AND PROCEDURE FOR THE EXCHANGE OF INFORMATION

IN RESPECT OF THE CITY OF LONDON SAFER CITY PARTNERSHIP

Document Review Date: May 2022

AS AGREED BETWEEN:

Responsible Authorities

City of London Corporation
City of London Police
City and Hackney Clinical Commissioning Group
London Fire Brigade
London Probation Service

Co-operating Bodies

The Guinness Partnership – Social Housing Provider
East London Foundation Trust
London Ambulance Service
London Community Rehabilitation Company

Participating Authorities

Turning Point - City of London and Hackney Integrated Drug & Alcohol Service
Thames Reach – Outreach
St Mungo's - Outreach
Toynbee Hall - City Advice
Ascent Project
Victim Support
Youth Offending Service
Southwark Mediation
Beyond the Streets
TAMAR Westminster
Transport for London
Network Rail
British Transport Police

Relevant Authorities

Metropolitan Police

City of Westminster
London Borough of Camden
London Borough of Hackney
London Borough of Islington
London Borough of Southwark
London Borough of Tower Hamlets
NHS England

1. INTRODUCTION

1.1 The purpose of this Protocol is to facilitate the lawful exchange of information, whether it be personal, special category, depersonalised or anonymised with the aim of reducing crime and disorder, and the misuse of drugs, in the City of London.

1.2 In particular, this Protocol is concerned with the disclosure of information pursuant to sections 17A and 115 of the Crime and Disorder Act 1998 and otherwise for the purpose of formulating and implementing the Safer City Partnership Strategy.

1.3 The information exchanged between signatories will be used for the formulation, implementation, assessment and monitoring of the City of London's Safer City Partnership Strategy.

1.4 The intention is that a single, joint approach to exchanging information is a highly efficient mechanism for reducing crime and disorder which is a common objective of all of the parties to this Protocol.

1.5 This Protocol clarifies each party's understanding of their responsibilities and duties towards each other, and, as far as is possible, the circumstances under which information can be exchanged.

1.6 By signing this Protocol, the signatories (listed at Appendix 1) declare their commitment to the procedures it sets out. Compliance with such procedures will ensure that data sharing arrangements between them take account of relevant legal requirements and that signatories properly comply with their legal obligations in the collection, use and disclosure of information about individuals.

1.7 This Protocol will be supplemented by Subject Specific Information Sharing Arrangements ("**SSISAs**") addressing specific objectives which involve the sharing of information, such as managing prolific offenders or addressing domestic violence.

1.8 All technical terms and abbreviations are defined in the extensive Glossary section set out in Appendix 2. Descriptions of all relevant legislation and other material are set-out in detail in the Appendices. The terms "signatory", "partner", "partner agency" and "party" are used interchangeably throughout this Protocol. References to "personal data" in the Protocol will, unless the context suggests otherwise, include reference to "special category data".

1.9 This Protocol should be published and made available to the general public, for clarity of purpose.

1.10 This Protocol is due to be next reviewed in <insert date> and any comments should be sent to the <insert team> Department of Communities and Children's Services, City of London.

2. GENERALCOMMITMENTS -

2.1 As signatories to this Protocol, the parties recognise the importance of sharing information with each other in accordance with the aims and requirements of the Crime and Disorder Act 1998 for the purpose of reducing crime and disorder, including the misuse of drugs.

2.2 Each signatory undertakes to co-operate fully with each other within the parameters of the Human Rights Act 1998, the UK GDPR, Data Protection Act 2018 and the Crime and Disorder Act 1998, and in accordance with the regulations and Home Office guidance associated with these Acts.

2.3 Each partner recognises that this Protocol is not intended to apply to information sharing for criminal law enforcement purposes which falls under the regime set out in Part 3 of the Data Protection Act 2018.

2.4 Each party undertakes to ensure that it complies with all other relevant legal requirements (including those set out in Appendix 3)), Government guidance and standards, the requirements of this Protocol, and its own internal policies on disclosure and information sharing. Parties are recommended to seek their own legal advice, wherever necessary.

2.5 Each party undertakes to follow the Pan-London Child Protection Procedures, City and Hackney Child Protection Procedures and the City of London's local Child Protection Procedures and all parties recognise the requirements that Caldicott imposes on NHS organisations and Social and Children's Services departments and will ensure that requests for information from NHS organisations and Social and Children's Services departments are dealt with in a manner that complies with these requirements.

2.6 Each partner agrees to disclose information to those parties who are Relevant Authorities or who are acting on behalf of a Relevant Authority for the purposes of the Crime and Disorder Act 1998 (as amended). Where the recipient is acting on behalf of a Relevant Authority, this means in their capacity as persons selected by the Relevant Authority to formulate or implement the Safer City Partnership Strategy.[1]

2.7 Information disclosed will be processed in accordance with the provisions of the Crime and Disorder Act 1998 for the formulation, implementation, assessment and monitoring of the Safer City Partnership Strategy. Further detail about the information partners may disclose is included in Appendix 4.

2.8 Each signatory to this Protocol will be a Data Controller (as defined under the UK GDPR), being that body, which is responsible for determining both the purposes for which and the manner in which personal data are processed.

2.9 All the Parties recognise that the initial legal responsibility for personal information resides with the organisation that first created or received it. But if personal information is shared, the responsibility extends to the recipient regardless of how transitory that storage of the personal information by the receiving party might be i.e. the requesting party becomes a data controller of that personal information.

2.10 Each party agrees to only request personal information on a "Need to Know" basis i.e. where it is necessary to comply with the legal obligations of the requesting party relating to the prevention, detection and reduction of crime and disorder in the City of London.

2.11 Where a receiving party is asked to further disclose this personal information for any of its other functions or to a third party, there must be a clear legal basis for doing so.

[1] For example: education establishments carrying out research and analysis on behalf of the partner members; and evaluation and monitoring of initiatives, i.e. burglary reduction.

Where the further disclosure is to a signatory, the requirements of this protocol must be followed. Where the further disclosure is to a non-signatory a written record must be kept setting out the reasons why the further disclosure was necessary and the legal basis for the disclosure.

2.12 Each party undertakes to ensure that it is appropriately registered with the Office of the Information Commissioner for sharing and receiving personal information for the purposes of crime detection, prevention and reduction.

2.13 Each party also undertakes to ensure that the data it holds is as accurate and up to date as possible.

2.14 Each partner agrees to periodically consult with each other upon matters of policy and strategy.

2.15 Each signatory undertakes that, where possible and appropriate, information requested in the correct manner is given within a time limit of 10 working days; this may vary depending on the nature, volume of requests and operational need.

2.16 Each partner agrees when handling the Media:

(a) to be fair to our fellow partners, and maintain their integrity;
(b) when providing information to the public, to do so honestly and fairly;
(c) statements must reflect the multi-agency decision process;
(d) consent of the data owner will be sought prior to release to the media;
(e) where practical, individual data subjects will be consulted if the media coverage was such that it may identify the individual.[2]

3. DATA COMMITMENTS

Non-Personal Data

3.1 Signatories understand that Non-Personal Data constitutes data that has never referred to individuals. Non-personal data is, more often than not, Aggregate Data. It is non-personal data (which has never referred to an individual) or aggregated data (derived from Personal, Non-Personal and Depersonalised Data), that is normally used for Crime Mapping. Partners can use this non-personal Data for Crime Mapping purposes, within the remit of the Crime & Disorder Act 1998.

3.2 Signatories agree that non-personal data held by each of them may be subject to the provisions of the Freedom of Information Act 2000. Partners may therefore have a legal duty to provide non-personal data to a third party, if a formal request is made.

3.3 Partners will disclose non-personal data for the purpose of profiling local areas for crime activity, and to calculate the cost, scope and scale of proposed crime reduction interventions by the Safer City Partnership.

Depersonalised Data

[2] Circumstances may exist that make this impractical, such as where the current whereabouts of the data subject is unknown, or the purpose of the media coverage is to identify the individual data subject.

3.4 Each party accepts that depersonalised data is used in the vast majority of Crime Audit activity, as management teams and consultants do not require personal data. De-personalised data is excellent for profiling local areas, and in calculating the scale, scope and cost of proposed crime reduction interventions.

3.5 Signatories understand that depersonalised data encompasses any information that does not and cannot be used to establish the identity of a living individual and has had all personal identifiers removed. Partners note that the Information Commissioner's Office has stated that even a post-code or address can give away the identity of an individual, if there is only one person living there.

3.6 All signatories accept there are no legal restrictions on the exchange within this Protocol of depersonalised data, but a duty of confidence may apply in certain situations, or a copyright, contractual or other legal restriction may prevent the information being disclosed to partners even when it is depersonalised.

3.7 Each partner appreciates that if several sets of depersonalised data were merged or compared to each-other, there is a risk that an individual could be identified. All signatories will always hold depersonalised data securely and destroy it securely, when no longer required.

3.8 It is good practice where possible to give individuals information about how anonymised data about them may be used.[3]

Personal Data

3.9 It is understood that personal data is information which relates to a living individual who can be identified from the data.

3.10 Personal Data will be clearly marked and kept securely within a password protected computer system or otherwise physically secure with appropriate levels of staff access.

3.11 All signatories undertake to destroy all personal information when no longer required for the purpose for which it was provided.

3.12 Each partner undertakes to formally record all grounds for disclosure of personal information and to process information fairly and objectively for each case.

3.13 All signatories agree to only disclose sufficient information to enable partners to carry out the relevant purpose for which the data is intended. This will be determined on a case-by-case basis.

3.14 Signatories undertake that one of the lawful basis set out in Article 6 of the UK GDPR will apply where it is necessary to process personal data. (Refer to Appendix 3).

3.15 Signatories undertake to carry out a Data Protection Impact Assessment where it is necessary in respect of any proposed processing of personal data under this Protocol.

Special Category Data

3.16 Parties to the Protocol must always consider whether exchange of information involves the disclosure of special category data, which is data that falls into the following categories:

[3] Particularly for prolific and priority offenders.

(a) personal data revealing racial or ethnic origin;
(b) personal data revealing political opinions;
(c) personal data revealing religious or philosophical beliefs;
(d) personal data revealing trade union membership;
(e) genetic data;
(f) biometric data (where used for identification purposes);
(g) data concerning health;
(h) data concerning a person's sex life; and
(i) data concerning a person's sexual orientation.

3.17 Signatories undertake that, in addition to the identification of a lawful basis for processing, one of the conditions in Article 9 of the UK GDPR will be satisfied where it is necessary to process special category data. (Refer to Appendix 3).

3.18 Signatories acknowledge they are aware that the Data Protection Act 2018 provides additional conditions which must be satisfied to allow the processing of special category data under certain Articles 9 conditions for processing.

3.19 Any disclosure of special category by a signatory should be restricted to the minimum necessary to achieve the purpose intended.

4. THE LEGAL FRAMEWORK FOR INFORMATION SHARING UNDER THE CRIME AND DISORDER ACT 1998

4.1 The Crime and Disorder Act 1998 and associated regulations require or enable data sharing between various public authorities to support the aims of the Crime and Disorder Act 1998. It does not override existing legal safeguards on personal information and there may be other legal bases for the exchange of information between agencies which are party to this Protocol.

4.2 This Protocol has been prepared in accordance with section 6(3)(f) of the 1998 Act, the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007 (as amended) and the Crime and Disorder (Prescribed Information) Regulations 2007 (as amended) and relates to sharing of information under sections 17A and 115 of the 1998 Act and otherwise for the purpose of formulating and implementing the Safer City Partnership Strategy.

4.3 Section 17A provides that Relevant Authorities are under a duty to disclose to all other Relevant Authorities any information held by the authority which is of a prescribed description which is relevant to the reduction of crime and disorder, including anti-social behaviour, in any area of England and Wales. Information is of a prescribed description if it is Depersonalised Information and of a type listed in the Schedule to the Crime and Disorder (Prescribed Information) Regulations 2007 (as amended) and included at Appendix 5.

4.4 Where certain conditions are satisfied, section 115 enables any person to disclose information for the purposes of any provision of the Crime and Disorder Act 1998 to a Relevant Authority, or to a person acting on behalf of such an Authority.

4.5 Co-operating Bodies have a duty to co-operate with the Responsible Authorities in respect of the formulation and implementation of the Safer City Partnership under section 5(2) of the 1998 Act.

5. THE LEGAL FRAMEWORK FOR SHARING PERSONAL DATA[4]

General

4.1 Some of the information shared under this Protocol will be Personal Data. Personal information should only be shared in a particular case when a disclosing partner is satisfied that:

(a) it is legally empowered to do so e.g. under section 115 of the Crime and Disorder Act 1998;
(b) the proposed disclosure of personal information can be made in accordance with the Data Protection Principles;
(c) there is a lawful basis for sharing the personal information;
(d) the disclosure can be made in accordance with all other requirements of the applicable Data Protection Legislation;
(e) the proposed disclosure of personal information is in accordance with the principles of Article 8 of the European Convention of Human Rights;
(f) the disclosure reflects the common law obligations of confidentiality; and
(g) where appropriate, the proposed disclosure is consistent with any other relevant legal requirements, Government guidance or standards.

4.2 Section 115 of the Crime and Disorder Act 1998 provides a specific power for sharing or disclosure of information to Relevant Authorities where this is necessary or expedient to do so for the purpose of implementing the provisions of the Act.[5]

4.3 The UK GDPR and Data Protection Act 2018 are the key legislation governing the protection and use of identifiable information about an individual ("personal data"). The UK GDPR and Data Protection Act 2018 setout a number of key principles which must be followed as well as providing individuals with certain rights.

4.4 The Human Rights Act 1998 (HRA) incorporates into English law certain elements of the European Convention of Human Rights and maps out a number of rights and freedoms that individuals can expect to enjoy in a democratic society. Its primary purpose is to curtail the power of the state from 'interfering' with, or unfairly controlling the lives of its citizens.

4.5 Of particular relevance to this Protocol is Article 8 of the Convention which states that everyone has the right to respect for his private and family life, home, and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

(a) national security;
(b) public safety;
(c) economic well being of the country;
(d) the prevention of crime and disorder;
(e) the protection of health or morals;
(f) the protection of the rights or freedoms of others.

[4] Refer to Appendix 3 for more detail regarding these legal requirements.
[5] For clarity, s17A of the 1998 Act relates to Depersonalised Data and so this section does not provide a legal power for sharing Personal Data.

4.6 When disclosure of information is required, all partners agree to ensure that:

(a) the information is being processed lawfully and fairly;
(b) the public interest is of sufficient weight to over-ride the presumption of confidentiality and to justify any interference with the right to privacy, etc. in Article 8 of the European Convention of Human Rights;
(c) a disclosure is necessary to support the aims of the Crime and Disorder Act 1998;
(d) any disclosure must have regard to specific statutory restrictions on disclosure.

4.7 All partners understand the Public Interest criteria to include:

(a) the administration of justice;
(b) maintaining public safety;
(c) the apprehension of offenders;
(d) the prevention of crime and disorder;
(e) the detection of crime;
(f) the protection of vulnerable members of the community.

Common Law Duty of Confidence

4.8 The common law protects from disclosure information (whether personal or not) that is given in circumstances giving rise to an obligation of confidence on the part of the individual to whom the information has been given. This confidential information will have some sensitivity, will not already be in the public domain and will not be readily available from another public source.

4.9 There are three grounds on which such confidential information may be used by the confidant for a purpose other than that for which it was imparted or disclosed to another party. These are:

(a) consent of the individual;
(b) compulsion of law;
(c) public interest.

4.10 Where data has been obtained in circumstances giving rise to a duty of confidence and a request for its disclosure has been received, the disclosing partner must make a judgment as to whether the public interest supports disclosure. The disclosing party must consider, in weighing the public interest, whether the proposed sharing is a proportionate response to the need to protect the public interest in question. The more sensitive and damaging the information, the stronger the public interest in disclosure will need to be.

4.11 Though information about a deceased person is not caught by the UK GDPR and Data Protection Act 2018, confidential information about a deceased person will remain subject to the duty of confidence. Therefore, careful consideration will be given to the disclosure of such confidential information concerning a deceased person and, if necessary, legal advice will be sought on individual cases.

Consent

4.12 It should not be assumed that consent is essential in order for signatories to share information in support of the Safer City Partnership Strategy. For example, consent is only one of the lawful bases under Article 6 of the UK GDPR which would permit the

processing of personal information and explicit consent is only one of the Article 9 processing conditions permitting the processing of special category data.

4.13 Obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from the data subject. This consent must be freely given, after the consequences are made clear to the person from whom permission is being sought.

4.14 However, in many cases there may be circumstances where it is not practicable or desirable to obtain consent to share information because, for example:

(a) to do so would place a person at serious risk of harm;
(b) to do so would prejudice the prevention or detection of a serious crime;
(c) there is a statutory duty to share the information;
(d) there is a court order in place.

In these instances, another Article 6 lawful basis or Article 9 processing condition must be identified.

5. DECIDING TO SHARE PERSONAL DATA

Specific Legal Powers

5.1 All parties to this Protocol recognise that section 115 of the Crime and Disorder Act 1998 is only one possible legal gateway which will permit information sharing between signatories for the purposes of preventing, detecting and reducing crime and disorder in the City of London - there may also be other legal powers which would permit sharing.

5.2 Section 115 of the Crime and Disorder Act 1998 provides a lawful power (or gateway) for sharing or disclosure of information to Relevant Authorities where this is necessary or expedient to do so for the purpose of implementing the provisions of the Act. However, section 115 does not override other legal requirements preventing disclosure, and although the Act creates a situation where the disclosure of information may be lawful, the presumption of confidentiality will still apply and the personal information will only be shared in a particular case when the disclosing partner is satisfied that the conditions set out at paragraph 5.1 are met.

5.3 Under section 115 of the Crime and Disorder Act 1998, anyone can disclose information to Relevant Authorities (which includes the Police, a Local Authority, Police authority, Probation Committee, Health Authority) or to persons acting on their behalf, where disclosure is necessary or expedient for the purposes of reducing crime and disorder in their area.

5.4 Where disclosure of information is not to a Relevant Authority, section 115 of the Crime and Disorder Act 1998 cannot be relied upon as the legal basis to support the disclosure. However, as long as there is no legal restriction on disclosure, information can normally be exchanged between signatories to support their work to prevent, detect and reduce crime under the Crime & Disorder Act 1998 - provided that this meets with a clear crime reduction objective outlined in the local Safer City Partnership Strategy.

5.5 Where this is the case, this would normally constitute a lawful basis for processing personal information under the UK GDPR and Data Protection Act 2018 BUT it would

necessary to demonstrate that any physical exchange of information was not contrary to:

(a) a common law duty of confidentiality owed to the individual, who is subject to the information (subject to any overriding public interest);
(b) the requirements of the Data Protection Legislation;
(c) the Human Rights Act 1998;
(d) any other statutory provision (e.g. the Rehabilitation of Offenders Act 1975).

5.6 In determining whether personal information or special category information can be exchanged in pursuit of the aims of Crime & Disorder Act 1998, the attached checklist provides a short summary of the main considerations. **It is important to note that it may still be permissible to share information with any body if there is a legal basis for doing so, beyond that set out in the Crime and Disorder Act 1998.**

Purpose of the Exchange	**The Organisation**	**Permissible Yes/No**
To pursue a specific objective in accordance with the Safer City Partnership Strategy	Responsible Authority[6] (Police, Police Authority, Local Authority, London Fire and Emergency Planning Authority, Primary Care Trust)	Yes
To pursue a specific objective in accordance with the Safer City Partnership Strategy	Co-operating Body[7] (local Probation Board, governing body of a maintained school, proprietor of an independent school, governing body of a further education institution etc.)	Yes
To pursue a specific objective in accordance with the Safer City Partnership Strategy	Participating Body[8] (social landlord; Drug and Alcohol Action Team; Homeless outreach teams; Training and Enterprise Council; voluntary organisation operating within the City of London; Crown Prosecution Service; member of a Victim Support Scheme; public transport operator in the City; Transport for London; organisation operating in the City which promotes the interests of, or serves: women, young people and children, the elderly, the physically and mentally disabled, those persons of different racial groups, homosexuals, residents; religious body; trade union; registered medical practitioner; chief officer of a fire brigade in the City; governing body of a higher	Yes, if they have signed this Protocol. Otherwise, only if the party has been able to provide a legal basis for the disclosure.

[6] Refer section 5(1) of the Crime and Disorder Act 1998.

[7] Refer section 5(2) of the Crime and Disorder Act 1998, and Crime and Disorder Strategies (Prescribed Descriptions) (England) (Order) 2004 SI 118/2004.

[8] Refer section 5(3) of the Crime and Disorder Act 1998, and Crime and Disorder Strategies (Prescribed Descriptions) (England) (Order) 2004 SI 118/2004.

Purpose of the Exchange	The Organisation	Permissible Yes/No
	education institution; British Transport Police; etc.)	

Disclosing Special Category Information

5.7 Special Category information may be disclosed lawfully to Relevant Authorities using section 115 of the Crime and Disorder Act 1998. However, it is still necessary to be aware of other legal obligations a disclosing agency may have, such as the common law duty of confidence.

5.8 If special category data held under a duty of confidence must be disclosed the disclosing partner must consider whether it is possible to obtain the data subject's consent. If we cannot, then the disclosing partner must consider the other legal justifications which would support the disclosure – e.g. a legal duty to disclose the information, satisfying one of the other conditions set out in the UK GDPR, or an overriding public interest.

5.9 Personal data relating to a victim, informant or witness will normally only be disclosed with their consent, unless there is a legal requirement to disclose the information or there is an overriding public interest in disclosure.

5.10 Where consent to disclose information to a partner agency has been refused or withheld, if there is an over-riding public interest to justify the disclosure. We agree to consider the following:

(a) Is the intended disclosure proportionate to the intended aim?
(b) What is the vulnerability of those who are at risk?
(c) What is the impact of disclosure likely to be on the offender?
(d) Is there another equally effective means of achieving the same aim?
(e) Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
(f) Is it necessary to disclose the information, to protect other vulnerable people?

5.11 Any disclosure of special category information by the partner, should be restricted to the minimum necessary to achieve the purpose and be as generalised as possible.

Cautions, Convictions and Criminal Offence Data

5.12 All signatories agree that details of criminal cautions (or reprimands/warnings) which relate to an adult will not generally be disclosed as the cautioning procedure creates an expectation that the offence has been dealt with and that no further action will be taken. Normally, the only exception will be the vetting of applicants for posts that involve contact with children and young persons, where the vetting is required to meet the legal obligations of the partner agency or is part of implementing a strategy for the reduction of crime and disorder pursuant to section 6 of the Crime and Disorder Act 1998.

5.13 All partners understand that the exchange of personal information post conviction will be subject to the same presumption of confidentiality as that relating to cautions. However, the prevention of crime and administration of justice, as provided for in the

Crime and Disorder Act 1998, are obviously in the public interest and may provide the grounds upon which a disclosure of an individual's criminal convictions can be justified.

5.14 Details of convictions recorded on the Police National Computer, or retained on file by a signatory, can be released to another signatory where this is justified in the public interest to support proceedings under the Crime and Disorder Act 1998. Great care must be taken to ensure conviction data is accurate, up-to-date and relevant to an enquiry before it is released.

5.15 All partners understand that in the absence of official authority, criminal offence data may only be processed if a specific condition for processing in Schedule 1 of the Data Protection Act 2018 applies.

Youth Offending Teams

5.16 It is permissible for information to be disclosed to the members of a Youth Offending Team (or local Youth Justice Team) for the purpose of any provision of the Crime and Disorder Act 1998.

5.17 Following the initial referral, Designated Officers attached to the Team will be responsible for the further disclosure of relevant personal information and conviction data.

5.18 There may be occasions when it is necessary for members of the Youth Offending Team to disclose personal information to another agency. In such circumstances the following guidelines must be followed:

(a) a secondary disclosure of personal information must generally be authorised by the original Data Controller;
(b) the disclosure must support action under the Crime and Disorder Act 1998;
(c) the public interest must outweigh any duty of confidentiality and must justify any interference with the right to privacy under Article 8 of the European Convention of Human Rights 1998;
(d) the information must be processed fairly under the UK GDPR and Data Protection Act 2018.

5.19 The Youth Offending Team Manager will be responsible for ensuring that personal information provided to the Team is stored in a secure place and destroyed when it is no longer required.

Management of Risk in respect of Violent Persons

5.20 The Parties recognise that they need to share information about individuals who they suspect have been subject to, or may be at risk of, abuse and individuals who may be responsible for perpetrating abuse.

5.21 The Parties will share personal information known to each of them about such individuals as openly as possible with other Parties' Personnel who Need to Know, albeit in a manner which is compliant with their statutory responsibilities, the Protocol and a SSISA. Examples of circumstances where sharing of personal information may be required because a service user or some other person is at risk include:

(a) to raise grounds for concern about a person believed to be at risk of abuse,
(b) to notify agencies who have a responsibility to take action in respect of a person who may be at risk of abuse,

(c) to notify the Parties of a risk posed by an individual whether this be a risk to Personnel or a member of the public,
(d) to make a referral to agencies for the purposes of requesting or amending services both for persons at risk of abuse and for those suspected of perpetrating abuse, or
(e) to deal effectively with complaints, grievances and professional and administrative malpractice.

6. DATA CONTROLLER RESPONSBILITIES

Designated Officers

6.1 Each partner must appoint a Primary Designated Officer (PDO), who will be a Manager of sufficient standing and have a co-ordinating and authorising role. Partners must also appoint at least one deputy Designated Officer (DO) to support the PDO. These staff names are listed in Appendix 6.

6.2 Designated Officers assume responsibility for data protection (including notification where appropriate), security and confidentiality, and compliance with all relevant legislation, guidance and standards relating to information sharing under this Protcol.

6.3 Designated Officers under this Protocol are listed in Appendix 6. Changes to the Primary Designated Officers, or Designated Officers, of each signatory, or their contact details, shall be notified in writing to each of the other signatory agencies by updating the Appendix and circulating it to the Primary Designated Officers of all other signatories. Such changes shall not constitute a formal variation to this Protocol.

6.4 Designated Officers will have the following responsibilities:

(a) ensuring their agency abides by this Protocol;
(b) ensuring that all Designated Officers and other staff are fully aware of their responsibilities;
(c) appointing other Designated Offices to act as deputy in their absence;
(d) authorising their agency's involvement and co-operation in the information sharing process, at every stage;
(e) internal information governance and/or operational procedures and process relating to this Protocol;
(f) the dissemination, implementation, monitoring and evaluation of the Protocol, including any Subject Specific Information Sharing Arrangements;
(g) keeping a Protocol Co-ordination Folder which holds all the partner's information sharing documents relating to this Protocol;
(h) ensuring their organisation's Data Protection Notification entry is accurate, up to date and adequate in respect of processing of personal data as relevant to the agency's functions, duties and obligations.

6.5 Only DO's and PDO's can make the formal requests and SSISAs for the sharing of personal information under this Protocol. Parties can decide (on a case by case basis) why a disclosure is necessary to support action under the Crime and Disorder Act 1998. We will also decide why and when the public interest overrides the presumption of confidentiality.

6.6 PDO's and DO's are responsible for ensuring that processing of personal data under this Protocol is in accordance with the Data Protection Principles, namely that it is:

(a) used fairly, lawfully and transparently
(b) used for specified, explicit purposes
(c) used in a way that is adequate, relevant and limited to only what is necessary
(d) accurate and, where necessary, kept up to date
(e) kept for no longer than is necessary
(f) handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

6.7 PDO's and DO's must also ensure ease of administration in their agency's compliance with the terms of this Protocol, including documentation of the information sharing process. This may be achieved by creation of a project folder or file which must be kept up-to-date and include:

(a) record of data disclosed;
(b) project chronology;
(c) project Access List;
(d) notes of meetings with our partners, and recent correspondence and phone calls.

6.8 Designated Officers must also ensure that the information held is reviewed with all signatory agencies at least annually. This will ensure, amongst other things, that information held is accurate and up to date and will enable exchanges of information under the protocol to be audited.

7. PROCESS

7.1 Signatory agencies will locally define the requirements of disclosure procedures, as well as outlining the nature of any risks. This is fundamental to the drawing up of this Protocol and may involve meetings.

7.2 The process must be documented in writing using the Request for Information Form at Appendix 7 and the Information Disclosure Form at Appendix 8, so as to ensure a paper trail for any audit and for clarity purposes.

Disclosure of Depersonalised Information under s17A of the 1998 Act

7.3 Where practicable Relevant Authorities under a duty to disclose to all other Relevant Authorities information held by that authority which is Depersonalised Information and of the type set out at Appendix 5 in accordance with section 17A of the 1998 Act, will share that information using the "SafeStats" data platform, on quarterly basis. Information will otherwise be disclosed in accordance with the requirements of section 17A of the 1998 Act and the Crime and Disorder (Prescribed Information) Regulations 2007 (as amended) electronically on a quarterly basis by agreement between the Relevant Authorities.

Disclosure Requests

7.4 Agreed procedures will generally require making a request in writing.

7.5 Access to information obtained through this protocol other than by Primary Designated Officers and Designated Officers should be limited to employees whose work is directly

related to the aim for which the data was obtained and those working within the crime reduction programme or field.

Subject Access Requests

7.6 The data subject is legally entitled to request their records from the receiving agency under the UK GDPR unless an exemption applies. If a data subject requests access to their records, the receiving agency should contact the disclosing agency to determine whether the latter wishes to claim exemption. The procedure should be fully documented in writing and stored on file.

Weeding and Retention of data

7.7 Signatories to the protocol must agree the criteria for the review and weeding of data exchanged under this protocol, in accordance with existing policies and codes of practice. This is to ensure that an agency does not retain data for longer than is necessary for that agency to undertake its functions. Partners accept that an agency may continue to hold information beyond a normal retention period where the agency continues to require it to undertake their functions.

It must be noted that the above represents the recommended approach to data sharing arrangements to ensure compliance with data protection legislation.

Publication

7.8 Where possible, this Protocol should be published and made available to the general public for clarity of purpose.

Media Handling

7.9 Signatories agree when handling the media to ensure there is a consistent approach to media enquiries, and that staff do not express personal views and respect the requirement for confidentiality and discretion. Signatory agencies agree:

(a) to be fair to our fellow signatory agencies, and maintain their integrity;
(b) when providing information to the public, to do so honestly and fairly;
(c) statements must reflect the multi-agency decision process;
(d) consent of the disclosing agency will be sought prior to release to the media; and
(e) where practical, individual data subjects will be consulted if the media coverage was such that it may identify the individual.

7.10 This might be best achieved through development of a media strategy on a case by case basis, co-ordinated by the disclosing agency.

8. SECURITY AND DATA MANAGEMENT

8.1 Signatories to this protocol must ensure they have adequate security arrangements in place to protect the integrity and confidentiality of the information held.

8.2 Signatory agencies agree that personal information disclosed must:

(a) not be emailed over internet links without appropriate protection, where this is practical.
(b) be protected by back-up rules.

(c) when stored on a computer system, it must be password protected with provisions to ensure system security.
(d) paper copies must be stored securely.
(e) be located in a geographically secure environment.
(f) not be inputted/accessed without industry standard security devices as defined by BS7666.

8.3 Each partner agrees that where practicable information shared under this Protocol will be processed using the Empowering-Communities Inclusion & Neighbourhood management System ("E-CINS").

8.4 Each partner will be responsible for agreeing and implementing their own organisation's retention policy to ensure the secure disposal of information in accordance with best practice and statutory obligations as referred to in paragraph 7.6 above.

8.5 Signatory agencies understand that all these measures need to be taken to ensure the security of our partners and to protect the general public.

8.6 The parties undertake to regularly, but at least annually, audit their processes under this Protocol to ensure that its requirements are being met.

9. COMPLAINTS AND BREACHES

Complaints

9.1 Initial complaints must be referred to the appropriate Primary Designated Officer or Designated Officer. It is agreed in this Protocol that the procedure to be followed in the event of a complaint being received is as follows:

(a) details of the complaint need to be clearly and accurately recorded at that time.
(b) the complainant should be referred to the organisation's relevant complaints procedure if the matter cannot be resolved informally.
(c) any formal complaint by a data subject regarding any stage of the process will be notified in writing to all signatories.
(d) all agencies will do all they can within the guidelines of the UK GDPR and Data Protection Act 2018 to assist with a complaint.

9.2 Signatories recognise that individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

Breaches

9.3 Signatories agree that any breach of confidentiality will seriously undermine and affect the credibility of the Crime and Disorder Reduction Strategy objectives and render us liable for breach of the law.

9.4 All agencies undertake at all times to comply with the data protection law and other legal requirements relating to confidentiality.

10. SUBJECT SPECIFIC INFORMATION SHARING ARRANGEMENTS ("SSISAs")

10.1 This Protocol will be supplemented by Subject Specific Information Sharing Arrangements ("**SSISAs**") addressing specific objectives which involve the sharing of information. These include, Domestic Abuse, Anti-Social Behaviour, Prevent/Channel, Modern Slavery, Human Trafficking, Hate Crime and Serious and Organised Crime.

10.2 SSISAs will set out the detailed arrangements relevant to the particular information sharing purposes. SSISAs will be focused on the operational elements and guidance associated with achieving these specific objectives and the principles agreed and adopted by signatories under this Protocol will also apply to them. The Parties to this Protocol will ensure that all SSISAs will be fully compliant and consistent with this Protocol. Each SSISA shall, as a minimum, contain the elements set out in paragraph 10.3 and be prepared in the form as set down in Appendix 9.

10.3 In drawing up individual protocols for sharing information, partners will agree the "rules" for disclosure under the SSISA by going through the following steps in respect of the relevant crime and disorder reduction objective:

(a) identify where there is a legitimate interest in sharing information.
(b) define the specific elements of information required.
(c) identify the reasons the information is required.
(d) identify the specific designated officers under the SSISA for each signatory.
(e) identify the role and functions of designated officers in respect of that SSISA; and
(f) create a matrix showing the elements of information, who "needs to know" and therefore has access to them and the reasons why.

10.4 A SSISA is required when:

(a) personal information is required to be shared across different organisations to meet the objectives of the Safer City Partnership Strategy; and
(b) the frequency of personal individual information requests across different organisations exceeds agreed levels which have been defined between the parties (usually following the mapping of information flows between them).

10.5 Each SSISA shall require the parties to it to implement and maintain procedures for recording and alerting those acting on its behalf of any request or requirement imposed by an individual that personal information about him or her shall not be shared with any particular person or class or classes of person. As mentioned at paragraph 4.12 above, this lack of consent will not always prevent disclosure of the information if there is an overriding public interest or a legal basis requiring disclosure.

10.6 It is suggested that each SSISA should also include a summary of the information about "consent", "Need to Know" and the various "exemptions" as well as flow charts.

11. NOTICES

11.1 Any partner may withdraw from this Protocol upon giving written notice to the other signatories. Data which is no longer relevant should be destroyed or returned. The partner must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory.

12. REVIEW

12.1 The parties undertake to conduct regular reviews of the operation of this Protocol at 12 monthly fixed periods, in order to amend it and ensure it remains fully effective.

13. SIGNATORIES

13.1 Signatory agencies will ensure that the protocol is signed at Appendix 1 by the appropriate person within their agency who has the authority to commit the agency to the terms of the Protocol.

13.2 The signatory agencies formally agree to the following:

(a) to subscribe to the principles contained in the Protocol;
(b) to work to the procedures identified within the Protocol;
(c) to fully implement the protocol within their own agency, ensuring all staff know of its existence to support the Safer City Partnership Strategy, and to support their attendance at any training event required;
(d) to supply information within the bounds of this protocol at no financial cost to any of the other signatory agencies;
(e) to contribute to the development of trust and confidence between the signatory agencies by working within the framework of the protocol to disclose, retain and dispose of data for the purpose of supporting the Safer City Partnership Strategy.

APPENDIX 1

SIGNATORIES TO PROTOCOL AT [INSERT DATE]

AGENCY	REPRESENTATIVE	SIGNATURE	DATE
City of London, Department of Communities and Children's Services			
City of London Police			
City and Hackney Clinical Commissioning Group			
London Fire Brigade			
London Probation Service			
The Guinness Partnership			
East London Foundation Trust			
London Ambulance Service			
Turning Point – City of London and Hackney Integrated Drug and Alcohol Service			
Thames Reach			

AGENCY	REPRESENTATIVE	SIGNATURE	DATE
St Mungo's			
Toynbee Hall – City Advice			
Ascent Project			
Victim Support			
Youth Offending Service			
Southwark Mediation			
Beyond the Streets			
TAMAR Westminster			
Transport for London			
Network Rail			
British Transport Police			
Metropolitan Police			
City of Westminster			
London Borough of Camden			
London Borough of Hackney			
London Borough of Islington			

AGENCY	REPRESENTATIVE	SIGNATURE	DATE
London Borough of Southwark			
London Borough of Tower Hamlets			
NHS England			

APPENDIX 2

GLOSSARY TO THE PROTOCOL

ACCESS LIST:	A register specific to a project where personal information is shared logging the authorised access to the information.
AGENCIES/PARTNERS ("SIGNATORIES"):	Those signatories party to this Protocol which are under a duty to formulate and implement crime and disorder strategies in compliance with the Crime and Disorder Act 1998 and any other participating parties invited to co-operate.
AGGREGATE DATA:	Data that consists of statistics of events forming a trend or pattern but from which it is not possible to identify individuals.
AUDIT TRAIL:	A process of collating data for the purpose of identifying and refining internal procedures of partner agencies, by means of examination of all documentation kept on the information exchange.
BULK DISCLOSURES/TRANSFERS:	The disclosure of a quantity/set of identifiable personal data, for the purpose of a criminal investigation/ crime and disorder initiative.
CALDICOTT GUARDIANS	Caldicott Guardians are senior staff in the NHS and Social Services appointed to protect client confidentiality.
CADICOTT PRINCIPLES	The Caldicott Report set out a number of general principles that health and social care organisations should rely upon in the proper use and management of client information which have been reviewed and updated and which are set out in Appendix 10.
COMMON LAW DUTY OF CONFIDENTIALITY:	The principle underlying all criminal-related work is the common law duty of confidentiality owed to the public. This requires that personal information given for one purpose cannot be used for another, and places restrictions on the disclosure of that information. This duty can only be broken if the public interest or another legal obligation requires it.
CONSENT:	Agreement, either expressed or implied, to an action based on knowledge of what that action involves, its likely consequences and the option of saying no.
CO-OPERATING BODIES:	Those parties which are under a duty to co-operate with Responsible Authorities in formulating and implementing crime and disorder strategies in compliance with the Crime and Disorder Act 1998 as defined in s5(2) of the Crime and Disorder Act 1998.
CRIME:	Any act, default, or conduct prejudicial to the community, the commission of which by law, renders the person responsible liable to punishment by fine, imprisonment or other penalty.

CRIME AND DISORDER ACT 1998:	The purpose of the Act is to tackle crime and disorder and help create safer communities. It requires the police and local authorities in partnership with the community, to establish a local partnership to cut crime and disorder. This partnership must conduct an audit to identify the types of crime in the area and develop a strategy for tackling them.
CRIME AUDIT:	A process of collating statistical data from lawful sources to identify trends or patterns in crime and disorder in order to formulate strategies and projects to disrupt and negate criminal and anti-social behaviour.
CRIME MAPPING:	This is the process of combining data resources and the use of different types of data, to create a more accurate or clear picture of what is going on in the area.
CRIMINAL OFFENCE DATA	Personal data relating to criminal convictions and offences or related security measures.
DATA/INFORMATION:	Essentially the same as "information," but tends to be information recorded in a form, which can be processed by equipment automatically (usually electronically), in response to specific instructions.
DATA IN THE PUBLIC DOMAIN:	Any information which is publicly available, whether it relates to a living individual or not. For example, Information found on the internet, television or local authority records.
DATA CONTROLLER/HOLDER/ OWNER:	Has the same definition as Article 4 UK GDPR.
DATA PROCESSING:	This term is used to describe the collecting, handling, using, sanitising, sharing, transferring and storing of all types of data.
DATA PROTECTION ACT 2018:	This legislation sets out the framework for data protection law in the UK. It sits alongside and supplements the UK GDPR.
DATA PROTECTION LEGISLATION	The UK GDPR, Data Protection Act 2018, and regulations made under the Data Protection Act 2018, as may be amended from time to time.
DATA PROTECTION PRINCIPLES	The principles defined by Article 5 of the UK GDPR.
DATA SHARING (EXCHANGE):	The physical exchange of data between one or more individuals or agencies; this is data recorded in an electronic or processing form. For example, this usually involves the transfer of a data set to a partner agency.
DATA SUBJECT:	Has the same definition as Article 4 UK GDPR.
DEPERSONALISED DATA/INFORMATION:	This is information that does not constitute personal data within the meaning of the UK GDPR.
DESIGNATED OFFICER:	A person nominated by the agency of sufficient standing, to process or initiate requests for personal information and data. [Health Authority representatives may refer to them as "Caldicott Guardians"].
DISORDER:	Refers to the level or pattern of anti-social behaviour within a certain area.

DOMESTIC VIOLENCE:	Any incident of threatening behaviour, violence or abuse (psychological, physical, sexual, financial or emotional) between adults who are or have been intimate partners or family members, regardless of gender or sexuality.' (includes familial violence, forced marriage & harmful cultural practices)
EDUCATION ACTION ZONE:	Geographical area identified as being beneficiary of government funding, providing local businesses contribute a set amount for precise education needs
EXPRESS CONSENT:	Consent which is expressed orally, or in writing, (except where patients cannot write or speak, when other forms of communication may be sufficient.)
FORMAL REQUEST:	A written request by the Designated Officer for information made to the information holder.
HEALTH ACTION ZONE:	Geographic area identified as being beneficiaries of government funding to address significant health inequalities.
HOT SPOT AREAS:	These are geographic areas of focus, where there is a disproportionately above average incidence of criminal activity.
HUMAN RIGHTS ACT 1998:	This Act requires the compliance to Article 8 of the European Convention on Human Rights. This allows interference with the right to respect for private and family life only when it is in accordance with the law, and pursues a legitimate public interest in a proportionate manner.
INDEMNITY:	Parties may seek to indemnify themselves against eventual legal action or litigation for compensation for damage or distress under the relevant legislation.
INFORMATION OBTAINED FOR NATIONAL STATISTICS:	Refers to administrative and survey data. Used within the NS framework.
INFORMATION SHARING (EXCHANGE):	Involves a physical exchange of data between one or more individuals or agencies.
INTELLIGENCE:	This is the end product of a process by which that information is checked and compared with other information and is then used to inform decision-making.
LOCAL POLICING UNIT:	An area covered by one police station.
MAINSTREAMING:	To provide services as part of the usual business of an organisation, rather than as a short-term project or initiative.
MEMORANDUM OF UNDERSTANDING:	Essentially, another term for Protocol.
META-DATA:	This is essentially data about data. This is a process of making the finding of a resource more efficient, by providing a structure of defined elements that describe or catalogue the resource. It should also provide details as to how the elements are used.
'NEED TO KNOW'	This means that parties will only have access to personal information if it is lawful for them, or those acting on their behalf, to have access to such personal information for the relevant purpose and the function they are required to fulfill at that particular time, in relation to a particular individual, cannot be achieved without access to the personal information specified.

NON-DOMESTIC BURGLARY:	All burglary that does not occur in a residential property. Includes burglary against sheds and garages, public buildings, commercial property.
NON-PERSONAL DATA/INFORMATION:	Any information which does not or cannot be used to establish the identity of a living individual.
PARTICIPATING BODIES:	Those persons defined under s5(3) of the Crime and Disorder Act 1998, invited by Responsible Authorities to participate in the formulation and implementation of crime and disorder strategies in the City of London.
PERFORMANCE INDICATOR:	Tool to measure the success/failure of an objective
PERSONAL DATA/ INFORMATION:	Information which relates to a living individual who can be identified from the data or any other information which is in the possession of the data controller. This is the most restricted type of information and should only be used where there is no reasonable alternative.
PERSONAL INFORMATION REQUEST FORM (PIRF):	A form requiring the disclosure of personal information from the information holder.
PRIMARY DESIGNATED OFFICER:	As Designated Officer, only the most senior member of the information sharing party in the partnership.
PROJECT:	A planned and co-operative activity undertaken by agencies and individuals to disrupt and negate criminal and antisocial behaviour according to the precepts of the Crime and Disorder Act 1998. Where information sharing is required to support a Project, parties to this Protocol may enter into a Subject Specific Information Sharing Agreement (SSISA) which will set out particular arrangements and processes agreed by relevant partners.
PROJECT CHRONOLOGY:	A register specific to a project where each agency logs its involvement in the information sharing process and the security arrangements.
PROJECT FILE:	A file to be kept by each partner agency containing all the personal information and documentation relevant to the information sharing process for the project.
PROJECT GROUP:	Individuals and agency representatives formed into a group to manage a specific project that involves data sharing.
PROJECT MEETING:	Meeting of the project group, to discuss the project.
PROTOCOL	A document between a number of parties which are drawn up for the specific purpose of clarifying the process and types of information that may be exchanged between the parties to them. They are not legally binding.
PROTOCOL CO-ORDINATION FOLDER:	To be held by each partner agency giving an overview of its information sharing arrangements and all projects in which it is involved.
PUBLIC DOMAIN:	Information is judged to be in the public domain when it is so generally accessible that it can no longer be regarded as confidential.
RECORDED OBJECTIVES:	The objectives formulated, outlined and agreed in an initiation document by the agencies as the beginning of a project under this Protocol.

RELEVANT AUTHORITIES:	Any of these bodies or persons referred to in Section 115 (2) of the Crime and Disorder Act 1998, including: the City of London Police, the City of London as local authority and police authority, the London Probation Board, the City and Hackney CCG, and any registered social landlord under section 1 of the Housing Act 1996.
RESPONSIBLE AUTHORITIES:	Those persons referred to in section 5(1) of the Crime and Disorder Act 1998 which are under a duty to formulate and implement strategies in compliance with the Crime and Disorder Act 1998.
REVIEW:	Periodic review of data exchanged for the purposes of the project including review of the scope, relevance and accuracy of disclosed data; a review process which shall be defined at the time of the project initiation.
RISK ASSESSMENT:	Carried out to establish whether the subject is likely to commit serious, physical, psychological harm to others.
RISK MANAGEMENT:	A plan to reduce, manage or eliminate the risk. The components may include treatment, supervision, incapacitation, disclosure.
RISK SCREENING:	The initial process of confirming information. The degree of likelihood and gravity of consequences of future behaviour.
SPECIAL CATEGORY DATA/INFORMATION:	Has the same definition as Article 4 UK GDPR.
'SMART' GOALS:	Goals that are: Specific, Measurable, Achievable, Realistic with a Timetable.
SCOPING:	Liaison between partner agencies, before a formal request is made, to define the problem and identify information holders.
SSISA (SUBJECT SPECIFIC INFORMATION SHARING ARRANGEMENTS):	Documents which are agreed by relevant partners to this Protocol which support the co-operative activity of partners in undertaking Projects aimed at targeting a specific crime and disorder objective. These documents set out the specific processes and management requirements relating to sharing of information which is necessary for a Project. SSISAs are subsidiary to this Protocol and the principles agreed by partners under this Protocol will always apply to the arrangements set out in a SSISA.
TRIGGER EVENT:	Information received by an agency that indicates an individual may constitute a risk of harm. Or which viewed together with other information, leads to that view.
TWOC:	Taking a car without the owner's consent.

APPENDIX 3

RELEVANT LEGISLATION

(a) The Crime and Disorder Act 1998 and associated regulations;
(b) The Data Protection Act 1998;
(c) The Human Rights Act 1998.
(d) Common Law Duty of Confidence;
(e) Children Act 1989;
(f) Children Act 2004;
(g) Crime and Victims Act 2004;
(h) Education Act 1996;
(i) Freedom of Information Act 2000;
(j) Health & Social Care Act 2001;
(k) Housing Act 1996;
(l) Mental Health Act 1983;
(m) NHS and Community Care Act 1990;
(n) Serious Organised Crime and Police Act 2005;
(o) Sex Offenders Act 1997;

Human Rights

The Human Rights Act 1998 incorporated into English law certain elements of the European Convention of Human Rights and sets down a number of rights and freedoms that individuals can expect to enjoy in a democratic society. Its primary purpose is to curtail the power of the state from 'interfering' with, or unfairly controlling the lives of its citizens.

The HRA works with the 'primary legislation' of the countries in which it has become law. This means that in making a ruling on a case, a Judge or Magistrate has to ensure that any legislation that is relevant to the case is read and given effect in a way which is compatible with the Convention rights. This also means that a Court or Tribunal must, in determining a question which has arisen in connection with a Convention right, take into account any judgement, decision or ruling of the European Court of Human Rights, any opinion of the Human Rights Commission, or other authoritative precedent material insofar as it is relevant to the proceedings – however while this jurisprudence must be considered, the Courts are not bound to follow it.

If the disclosure of information will in some way restrict the rights of an individual, in order to ensure that a fair balance is achieved between the protection of the individual's rights and the general interests of society, the law requires the disclosing signatory to consider whether a disclosure is proportionate. A record should be kept of the decision to disclose and the matters considered in coming to the decision in case the decision is challenged.

There are a number of rights which have been incorporated into English law through the HRA, but the two most likely to be relevant to the confidentiality and security of personal information for the purposes of preventing, detecting and reducing crime and disorder are set out in Article 6 and Article 8 of the Convention.

Article 8: Right to Respect for Private and Family Life

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

This clearly supports the UK GDPR and Data Protection Act 2018. The HRA requires that any obvious act of curtailment of such rights and freedoms by the State (or any instrument of it) be justified and evidenced. The HRA recognises the issue of 'proportionality', in that the rights of one individual might be at variance with those of another. An example of this in terms of Article 8 would be where a child might be at risk of "significant harm", or indeed, where an individual with a severe mental illness poses a risk to the safety of others. In the case of a child at risk of 'significant harm; the professionals involved will work within the context of the Children Act 1989 and the Children Act 2004, and share information in order to protect that child or children. In this situation therefore, Article 8 is overridden in the child's "best interests".

Article 6: Right to a Fair Trial

1. *In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.*

2. *Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.*

3. *Everyone charged with a criminal offence has the following minimum rights:*
   - *(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;*
   - *(b) to have adequate time and facilities for the preparation of his defence;*
   - *(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;*
   - *(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;*
   - *(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.*

As the provisions of this Article can also be applied to the right to a fair assessment, it is clearly necessary for there to be accurate recording of information and the appropriate use of risk assessment and management processes, when disclosing information without consent. If a risk assessment is found to be without professional rigour and judgement based on the presenting information, then the individual has grounds to say that the assessment was not 'fair' within the context of Article 6. This would in turn constitute a breach of Article 8 and the Data Protection Legislation.

UK GDPR and the Data Protection Act 2018

The key legislation governing the protection and use by public organisations of identifiable information about an individual ("personal data") is the UK GDPR and the Data Protection Act 2018 (DPA). The DPA sets out a number of key principles which must be followed as well as providing individuals with certain rights.

Data Subject's Rights

The UK GDPR gives eight rights to individuals in respect of their own personal data held by others, they are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Data Protection Principles

Anyone processing personal data must comply with the seven Data Protection Principles set out in Article 5 of the UK GDPR, which in summary are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the Data Controller towards the individual, although in some limited circumstances exemptions will apply.

To meet the requirements of these Principles, personal information should be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
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;
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; 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;

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).

Lawful bases for processing Personal Data

The First Data Protection Principle requires that for personal data to be processed lawfully, one of the lawful bases set out in Article 6 of the UK GDPR for processing must apply. To lawfully process special category data, you must ALSO identify a separate condition for processing under Article 9 of the UK GDPR.

Article 6: Lawful bases for processing personal data
As stated above, the processing of personal data of any type must fulfil at least one of the following lawful bases:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
2. **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.
3. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **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.
6. **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.)

Health care professionals, local authority officers and the police use some or all of the above conditions on a daily basis in their work with clients/patients, in particular reliance upon consent which may be express or implied. While it may be normal practice to seek consent for processing personal information, consent is only one of the available conditions which would permit the processing (including the disclosure) of personal information. The right of an individual to actively control the processing of their data (i.e. to withhold or refuse consent) may be overridden if the processing is necessary to comply with a legal obligation, it is in the "best interests" of the individual themselves, or in the context of the wider, "public interest".

Article 9: Conditions for Processing Special Category Data
Special Category data is data that falls into the following categories:

(a) personal data revealing **racial or ethnic origin**;
(b) personal data revealing **political opinions**;
(c) personal data revealing **religious or philosophical beliefs**;
(d) personal data revealing **trade union membership**;
(e) **genetic data**;

(f) **biometric data** (where used for identification purposes);
(g) data concerning **health**;
(h) data concerning a person's **sex life**; and
(i) data concerning a person's **sexual orientation**.

Processing of special category data by a Data Controller requires both a Article 6 lawful basis **and** an Article 9condition to be satisfied. The Article 9 conditions are:

1. Explicit consent
2. Employment, social security and social protection (if authorised by law)
3. Vital interests
4. Not-for-profit bodies
5. Made public by the data subject
6. Legal claims or judicial acts
7. Reasons of substantial public interest (with a basis in law)
8. Health or social care (with a basis in law)
9. Public health (with a basis in law)
10. Archiving, research and statistics (with a basis in law)

It should be noted that if you are relying on conditions 2, 8, 9 or 10, you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. If you are relying on the substantial public interest condition (condition 7), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

This range of conditions supports the necessity of statutory interventions and the inevitable need therefore to process special category information. Although these Article 9 conditions are available to enable the processing of special category data where it can be justified, it is good practice to seek the explicit consent of an individual to process their special category information wherever possible.

DPA 2018, Schedule 2, Paragraph 2 – Crime and Taxation; general - exemption

The UK GDPR and DPA 2018 provide a number of exemptions to some of their rights and obligations in certain circumstances. The exemptions include a general crime and taxation, the second part of which applies when another controller obtains personal data processed for the prevention and detection of crime, the apprehension or prosecution of offenders or the assessment or collection of a tax or duty or an imposition of a similar nature;. for the purposes of discharging statutory functions. The controller that obtains the personal data is exempt from the following UK GDPR provisions to the same extent that the original controller was exempt:

- The right to be informed.
- The right of access.
- All the principles, but only so far as they relate to the right to be informed and the right of access.

However, a data controller must still comply with the other UK GDPR and DPA 2018 requirements, including the identification of an Article 6 lawful basis for processing (and, where relevant, one of the conditions in Article 9).

Crime and Disorder Act 1998

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime and disorder partnerships around local authority

boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 17A of the 1998 Act provides that Relevant Authorities are under a duty to disclose to all other Relevant Authorities any information held by the authority which is of a prescribed description which is relevant to the reduction of crime and disorder, including anti-social behaviour, in any area of England and Wales.

Section 115 of the Act provides that any person has the power to lawfully disclose information to 'Relevant Authorities' (the police, local authorities, probation service or health authorities) or persons acting on their behalf where they do not otherwise have the power, but only where it is necessary and expedient for the purpose of the Act. However, whilst all agencies have the power to disclose, section 115 does not impose a requirement on the Relevant Authorities to disclose information. It should also be noted that section 115 does not exempt the disclosing party from complying with the second Data Protection Principle when disclosing personal data.

Co-operating Bodies, as defined in section 5(2) of the 1998 Act have a duty to co-operate with the Responsible Authorities in respect of the formulation and implementation of the Safer City Partnership.

Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) gives the public a statutory right to access the majority of records held by public authorities. In doing so it aims to make public authorities more accountable and bring about a change in the provision of information to the public from a "need to know" to "a right to know".

The FOIA gives any person the right to request information held by public authorities who must either confirm or deny whether or not information of the description sought is held. The authority must also provide applicants with such advice and assistance as may reasonably be expected.

A number of exemptions to the right of access exist. These include confidentiality, the prevention and detection of crime and personal data.

The Freedom of Information Act 2000 only applies to the City of London Corporation in respect of its functions as a local authority, police authority and port health authority. All other parties are subject to the FOIA.

If you require assistance regarding the FOIA, please contact the person in your organisation (or department) who has been given responsibility for compliance with the FOIA. Otherwise, more information may be found at www.informationcommissioner.gov.uk.

APPENDIX 4

TYPES OF INFORMATION

Types of Information held and potentially disclosed in accordance with this Protocol

Source	Type of Data
Police	Crime incidents, recorded crime statistics, NPCC defined disorder incidents Offender information, witness details where consent has been obtained, conviction data Victim information, evidence to support court proceedings e.g. statements, officer attendance Command & control data on non-crime incidents Non sensitive information on current operations Vulnerable Persons Reports Custody Information Anti-social behaviour incidents Geographical information
Police Authority	Public surveys
Local Authority Housing Department	Housing voids, damage to non housing property and land, anti-social behaviours orders, RSLs Criminal damage costs, derelict property, emergency property, entry phones, evictions Neighbourhood complaints, property rooms, re-housed offenders, re-housed homeless Vandalism records, types of locks and fittings, sub-standard housing, re-housed victims Racial/homophobic incidents, emergency out of hours calls, empty property, turnover of tenants Reasons for transfer applications Records of neighbour disputes/complaints Stock turnover, rent arrears and possessions, housing and council tax benefits Evictions, injunctions, relating to anti-social behaviour Information regarding domestic abuse
Local Authority (Technical Services)	Details of commencement of work, new buildings, refurbishments and scaffolding licences issued
Local Authority Social Services Department	Information on vulnerable groups e.g. elderly, people with disabilities, mental ill health, child protection, child abuse, lone parents, families on benefit Children in care/leaving care, child neglect, low family income and deprivation Information on young offenders, nuisance families, needle exchange, welfare referrals Individuals at risk of exploitation or other connections to antisocial behaviour and/or crime
Local Education	Exclusions

Source	Type of Data
Authority	Truancy Disciplinary Reports
Individual Schools	Experience of discipline
Local Authority Environmental Services	Neighbourhood disputes Refuse collections problems, fly tipping, dogs fouling Health & Safety problems, notices and prosecutions, odour, pollution, drainage, food Grants for safety improvements, pollution, licensing, gambling premises, public houses Noise notices Cleansing data Licensing information
Local Authority Highways	Location of traffic accidents
Local Authority Open Spaces	Staff reports on lost property, and anti-social and criminal behaviour
Street Lighting	Requests for lighting
Local Authority Centre (Chief Exec/Policy Unit)	Census data analysis Needs analysis for external grants Records of crime/anti-social behaviour against staff
Local Authority Planning Department	Planning maps Previous area based work Forthcoming developments Work for SRB bids etc Census data Land use, including dereliction, recreational, and business Planning Applications Demographical information
Probation	Offender profiles e.g. age, gender, employment status, substance misuse, reconviction data, percentage of risk cases, effectiveness of programs, types of orders, total case loads, offender needs e.g. drugs. Housing supervision status, release from custody/licence information, risk assessment
Health Authority	A&E records of assault and domestic violence Victims of violence treated in primary care, relevant patient record Mentally disordered offenders Information on substance misuse e.g. drugs and alcohol Behaviour Modification attendee numbers
District Health Authority	Morbidity data
Drug Action Team	Information on drug-taking/alcohol & substance misuse
Fire Service	Incidents of arson, hoax calls, suspicious fires, false alarms, rescue

Source	Type of Data
	incidents Details of individuals involved with ‘Firesafe’
Community Relations Council	Incidents of racial attacks and harassment
All public buildings e.g. schools, hospitals, libraries and leisure facilities	Costs of criminal damage and vandalism
Chamber of Commerce	Costs of damage and vandalism to private companies
Chamber of Trade	Costs of retail crime, damage and vandalism
Employment Service	Adult/youth unemployment data
Voluntary & other support services (victim support, gay/lesbian support groups, medication schemes)	Nature and extent of harassment/incidents Profile of victims and perpetrators
Ambulance Service	Relevant incident details and calls for service (including 999 calls, victim information, incident type) Any records of crime and anti-social behaviour against staff
Public Protection	All night cafes, diseases, households, educational establishments, complaints origin, commercial property types

APPENDIX 5

PRESCRIBED DESCRIPTION OF INFORMATION TO BE DISCLOSED UNDER SECTION 17A OF THE CRIME AND DISORDER ACT 1998 BETWEEN RELEVANT AUTHORITIES

Extract from the Schedule to the Crime and Disorder (Prescribed Information) Regulations 2007 as at 1st April 2021.

"1

Information held by the police force for the area on the category of each—

(a) anti-social behaviour incident,

(b) transport incident, and

(c) public safety/welfare incident,

in the area, as defined in accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales [as at [1st April 2010]], and the time, date and location of each of those incidents.

2

Information held by the police force for the area on the sub-category of each crime classified as—

(a) burglary,

(b) criminal damage,

(c) drug offences,

(d) fraud and forgery,

(e) robbery,

(f) sexual offences,

(g) theft and handling stolen goods,

(h) violence against the person, and

(i) other offences,

in the area, as defined in accordance with the Home Office Notifiable Offences List as at [1st April 2010], and the time, date and location of each of those crimes.

3

Information held by the fire and rescue authority for the area on the time, date and location of each—

(a) deliberate primary fire (excluding deliberate primary fires in vehicles) in the area,

(b) deliberate primary fire in vehicles in the area,

(c) deliberate secondary fire (excluding deliberate secondary fires in vehicles) in the area,

(d) incident of violence against employees of the fire and rescue authority in the area, and

(e) fire in a dwelling in the area where no smoke alarm was fitted attended by the fire and rescue services of the authority,

as defined in accordance with [Incident Recording System—Questions and Lists, published by the Department for Communities and Local Government in May 2009].

4

Information held by the fire and rescue authority for the area on the time and date of each call to the fire and rescue services in the area in relation to a malicious false alarm and the purported location of those alarms as defined in accordance with [Incident Recording System—Questions and Lists, published by the Department for Communities and Local Government in May 2009].

5

Information held by the local authority for the area on the time, date and location of each road traffic collision in the area and the number of adults and children killed, seriously injured and slightly injured in each of those collisions.

6

Information held by the local authority for the area on the age and gender of each of the pupils subject to a permanent or fixed term exclusion from state primary and secondary schools in the area, the names and addresses of the schools from which those pupils have been excluded and the reasons for their exclusion.

7

. . .[9]

8

Information held by the local authority for the area on the category, time, date and location of each:—

(a) incident of anti-social behaviour identified by the authority, and

(b) incident of anti-social behaviour reported to the authority by the public,

in the area, as defined in accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales [as at 1st April 2010] or any other system for classifying anti-social behaviour used by that authority as at the date of these Regulations.

9

Information held by each [clinical commissioning group] or Local Health Board the whole or any part of whose area lies within the area[, or by the National Health Service Commissioning Board,] on the general postcode address of persons resident in the area admitted to hospital, the date of such admissions and the sub-categories of each admission within the blocks—

(a) assault (X85–Y09),

(b) mental and behavioural disorders due to psychoactive substance use (F10–F19),

(c) toxic effect of alcohol (T51), and

[9] Revoked

(d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or evidence of alcohol involvement determined by level of intoxication (Y91),

as classified in accordance with the International Classification of Diseases, Tenth Revision (ICD-10) published by the World Health Organisation.

10

Information held by each [clinical commissioning group] or Local Health Board the whole or any part of whose area lies within the area[, or by the National Health Service Commissioning Board,] on the general postcode address of persons resident in the area admitted to hospital in respect of domestic abuse as defined in Section 2.2 of the Responding to domestic abuse: a handbook for health professionals published by the Department of Health in December 2005, and the date of such admissions.

11

Information held by each [clinical commissioning group, Local Health Board or local authority (within the meaning of section 2B of the National Health Service Act 2006) acting in the exercise of public health functions (within the meaning of that Act),] the whole or any part of whose area lies within the area[, or by the National Health Service Commissioning Board,] on the number of—

(a) mental illness outpatient first attendances, and

(b) persons receiving drug treatment,

in the area.

12

Information held by each [clinical commissioning group] or Local Health Board the whole or any part of whose area lies within the area[, or by the National Health Service Commissioning Board,] on the location, time and date of ambulance service calls to incidents relating to crime and disorder and the category of such incidents using any system for classifying crime and disorder used by that authority.

[13

Information held by each provider of probation services operating wholly or partly within the area on—

(a) the demographic profile of offenders including age, gender, ethnicity, first part of postcode and offence description;

(b) the assessment of factors relating to offenders' criminality including thinking and behaviour, attitudes, accommodation, employment, training and education, relationships, lifestyle and associations, drug misuse and alcohol misuse; and

(c) the risk posed by offenders of serious harm to others and of re-offending

in the area.]

APPENDIX 6

PRIMARY DESIGNATED OFFICERS

AGENCY	NAME	POST	CONTACT DETAILS
City of London, Department of Communities and Children's Services			
City of London Police			
London Probation Service			
City and Hackney Clinical Commissioning Group			
London Fire Brigade			
London Ambulance Service			

APPENDIX 7

REQUEST FOR INFORMATION FORM
(to be completed by the requesting party)

Data protection implications must be considered before personal information is disclosed or transferred. All requests for information must be documented. Please refer to the Safer City Partnership Protocol for more information.

Organisation receiving request:	
Organisation making request:	
Details of Information required:	
Purpose of the information request:	
You must consider the following before requesting this information. You should keep a detailed record of the reasons for your request, and provide a summary of them on this form. Please refer to the Protocol for more information.	
Is the objective of the request for information to prevent crime and disorder? (Y/N – state specific objective from the Safer City Partnership Strategy)	
Would failure to disclose the information prejudice the objective? (Y/N – if Yes, state why)	
Is the disclosure of the information "in the public interest?" (Y/N – if Yes, state why)	
What is the lawful basis under which you are acting (refer to specific legislation etc)	
Does processing involve any special category data?	
Are there any specific arrangements for retention / deletion of data?	
If the request relates to personal information, confirm that the DPA Principles have been properly considered. (Y/N)	
Supervisor/Designated Officer Approval:	
Print Name:	Position:
Signed:	Date:
Person requesting information: (this is the individual requesting information who has the responsibility for using information received lawfully; and where personal information is released, for using it in accordance with the UK GDPR and DPA 2018.)	
Print Name:	Position:

Signed:	Date:
Contact Tel No:	

APPENDIX 8

INFORMATION DISCLOSURE FORM
(to be completed by the disclosing party)

Data protection implications must be considered before personal information is disclosed or transferred. All requests for information must be documented.

This information is disclosed after having received an appropriate request and with the understanding that the following points have been considered before releasing this information:

1. The objective of the request for personal information is to prevent or detect crime and disorder.
2. Failure to disclose the information would prejudice the objective.
3. The disclosure of the information is "in the public interest."
4. Where the request relates to personal information, the Data Protection Principles have been properly considered.

Please refer to the Safer City Partnership Protocol for more information.

Organisation receiving information requested:	
Lawful basis for sharing (including additional conditions where applicable in respect of special category data):	
Why is sharing necessary:	
Is a DPIA required, if so what is the outcome:	
Details of Information requested. Please also give reasons for non-disclosure (where appropriate.)	
Disclosed information must be destroyed or returned to the originator, when no longer relevant to the purposes it was obtained for.	
Not all information relating to an individual or incident need be disclosed, only specific details asked for or that which is directly relevant. If you are unsure of what information is required, contact the requestor.	
Supervisor/Designated Officer Approval:	
Print Name:	Position:
Signed:	Date:
Person requesting information: (this is the individual requesting information who has the responsibility for using information received lawfully; and where personal information is released, for using it in accordance with the UK GDPR and DPA 2018.)	
Print Name:	Position:

Signed:	Date:

APPENDIX 9

PRO-FORMA FOR SUBJECT SPECIFIC INFORMATION SHARING ARRANGEMENTS

Subject Specific Information Sharing Arrangements
"SSISA"

Between

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

[NAME THE AGENCIES INVOLVED]
e.g. City of London Police, City of London (relevant department)

for the purpose of
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
e.g. Combating Domestic Violence
e.g. Preparing Mapping Data
e.g. Addressing Prolific Offending
e.g Anti-Social Behaviour Orders

JUSTIFICATION OF PURPOSE

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A JUSTIFICATION FOR THE PURPOSE SHOULD ALSO BE INCLUDED i.e. WHY THERE IS A NEED FOR THIS INFORMATION TO BE SHARED.

e.g. to meet the following priority/ies under the City of London Safer City Partnership Strategy 2019-22: …

1. PARTIES

1.1 The Parties to this SSISA (the "**Parties**") are:

e.g.
- City of London Corporation
- City and Hackney CCG
- City of London Police

whose addresses are as set out in Annex A below.

NB Include above only those organisations that are to be party to this SSISA. Where there are parties to this SSISA who are not already signatories of the Protocol the parties also need to agreed to comply with the relevant provisions of the overarching Protocol refer paragraph 4.2 below.

2. DEFINITIONS

2.1 In this SSISA, the following terms have the following meanings:

"DPA 2018"	the Data Protection Act 2018
"Consent"	Agreement, either expressed or implied, to an action based on knowledge of what that action involves, its likely consequences and the option of saying no.
"Safer City Partnership Priority/ies"	For full details please refer to the City of London Safer City Partnership Strategy 2019-22. In summary these are: • Vulnerable people and communities are protected and safeguarded • People are safe from violent crime and violence against the person • People and businesses are protected from theft and fraud/acquisitive crime • Anti-Social Behaviour is tackled and responded to effectively • People are safe and feel safe in the Night-Time Economy
"Need to Know"	This means that parties will only have access to personal information if it is lawful for them, or those acting on their behalf, to have access to such personal information for the relevant purpose and the function they are required to fulfill at that particular time, in relation to a particular individual, cannot be achieved without access to the personal information specified.
"other SSISA"	any Subject Specific Information Sharing Arrangements to which the Protocol relates and to which some or all of the Parties are party, other than this SSISA
"personal information"	Information which relates to a living individual who can be

	identified from the data or any other information which is in the possession of the data controller. This is the most restricted type of information and should only be used where there is no reasonable alternative.
"Personnel"	the Parties' employees, officers, elected members, directors, voluntary staff, consultants and other contractors and their sub-contractors (whether or not subject to legally binding contracts) and such contractors' and their sub-contractors' Personnel
"the Protocol"	the Safer City Partnership Information Sharing Protocol to which the Parties are signatories
"special category data"	The DPA defines certain categories of personal data as being special category data and therefore subject to even stricter controls than those applying to personal data. Use and disclosure of this type of information must only be undertaken when absolutely necessary, and preferably with consent, unless there is an overriding public interest or legal obligation requiring it's disclosure.
"SSISA"	Subject Specific Information Sharing Agreement

3. THE SUBJECT OF THIS SSISA

Combating Domestic Abuse, Anti-Social Behaviour, Terrorism/Prevent, Modern Slavery, Human Trafficking, Serious and Organised Crime, Hate Crime

3.2 The purpose of this SSISA is to identify:

(a) the procedures for secure and confidential sharing of information between the Parties in the course of meeting the Safer City Partnership Priority/ies,
(b) the specific purposes for which the Parties have agreed to share personal information in connection with delivery of the Safer City Partnership Priority/ies,
(c) the responsibilities assigned to the Parties in relation to the collection of personal information,
(d) the responsibilities of each Party to implement procedures to seek to obtain the consent of service users for the sharing of their personal information, and
(e) how this SSISA will be implemented, monitored and reviewed.

3.3 Each Party confirms that:

(a) it has full power and authority to enter into this SSISA and when signed this SSISA will constitute binding obligations on each Party in accordance with this SSISA's terms, and
(b) its signatory identified below in annex A is duly authorised to sign this SSISA on its behalf.

3.4 Each Party undertakes to the others that it and its Personnel will comply with this SSISA and the law relevant to the information sharing to which this SSISA relates.

4. SCOPE

Application

4.2 The Parties to this SSISA who are also parties to the Protocol agree that as between

themselves:

(a) this SSISA is subject and subservient to the Protocol, and
(b) the provisions of the Protocol apply to and are deemed included in this SSISA.

4.3 If any Party to this SSISA is not already a party to the Protocol or subsequently ceases to be a party to the Protocol, by entering into this SSISA such Party undertakes in favour of all parties to the Protocol to comply (or, as the case may be, continue to comply) with the terms of the Protocol insofar as it is relevant to the information sharing to which this SSISA relates.

4.4 The fact that a Party has ceased to be a party to the Protocol **SHALL NOT OF ITSELF** be a reason for a Party not to share personal information as the sharing may still be necessary in order that the legal duties of the disclosing and/or receiving party met.

Relationship to other SSISAs between the Parties

4.5 If this SSISA applies to subject matter to which any other SSISA applies, nothing in this SSISA shall prejudice such other SSISA, provided that if there shall be any conflict between this SSISA and such other SSISA it shall be resolved by agreement between the Parties and the parties to such other SSISA.

Specific Purposes for Sharing and Roles of Each Party

4.6 Information may only be disclosed under this SSISA as necessary to meet the statutory duties of the disclosing and/or receiving Party as relevant to the Safer City Partnership Priority/ies to which this SSISA relates. These specified purposes are set out in Annex B. It is anticipated that the Parties may also undertake specified roles in order that the Safer City Partnership Priority/ies under this SSISA may be met, as detailed in Annex B.

[Complete the table in Annex B with an entry for each Party, determining the Roles which need to be undertaken by the Parties in order to meet the objectives of this SSISA]

5. PROCEDURES

Internal compliance with this SSISA

5.1 Each Party shall nominate a Designated Officer to oversee compliance with this SSISA.

5.2 Refer to Annex C below for a list of Designated Officers, being those individuals in each party responsible for compliance and information sharing issues to which this SSISA relates.

[Complete the table in Annex C with an entry for each Party]

The Collection of Personal Information

5.3 Personal information relevant to the Safer City Partnership Priority/ies to which this SSISA relate/s will be collected in accordance with the processes set out in Annex B.

[Annex B will set down for staff details of how the information will be collected and a description of relevant processes to ensure proper, secure, and legally compliant, information sharing.]

5.4 Each Party agrees that:

(a) it is responsible for maintaining the personal information that it has collected on its own account, or jointly with another Party, in accordance with the UK GDPR and DPA 2018,

(b) it will retain legal responsibility for correcting personal information where it is factually incorrect, and

(c) it will not amend the record of an opinion or judgement recorded by a health or social care professional or police officer, whether accurate or not, because the recorded opinion or judgement is essential for understanding the decisions that were made and, where relevant, to audit the quality of care.

Dissemination of Personal Information

5.5 Wherever possible, subject to the requirements of the Protocol and applicable law and guidance, personal information collected by one Party that is requested by another Party (or is proposed to be transferred to another Party without a request) for the purposes of meeting the Safer City Partnership Priority/ies, will be transferred to receiving Party as:

(a) part of any referral correspondence, and/or
(b) part of an 'at risk' alert.

[insert/amend as appropriate to meeting relevant Safer City priority.]

5.6 The receiving Party will ensure that any Party which disclosed information to it, as necessary to meet the legal obligation's of the disclosing Party, is provided with:

(a) progress reports on the nature of the care provided by the receiving Party and the outcomes planned, and
(b) discharge correspondence when the care provision has ceased.

[amend or add anything else appropriate to this meeting this particular Safer City priority]
[paragraph 5.6 above only needs to be included where it is relevant to the Safer City priority to which the SSISA relates]

Sharing of Personal Information

5.7 Personal information may be disclosed to a receiving Party only if the personal information is necessary to perform a function or responsibility identified for such receiving Party to perform in Annex B and (if there has been a request) the request for the information has been made in accordance with the information sharing principles and procedures set down in the Protocol and Annex B to this SSISA.

[ANNEX B – should cover the specific information sharing procedures and processes that need to be met to ensure proper management and legal sharing of information (special category data or otherwise) e.g seeking consent to collect and share information, disclosing without consent, tracking information, Audit Trails, security processes]

.

5.8 The persons holding the job titles listed in the table in Annex C, and only those persons, will be permitted access to personal information shared under this SSISA, which is not special category data.

5.9 Alterations from time to time to the above list shall be notified by the Parties to each other in accordance with paragraph 9.4 below.

Sharing of Special Category Data

5.10 Special category data may be disclosed to a receiving Party ONLY IF the special category data is necessary to perform a function or responsibility identified for such receiving Party to perform Annex B above and (if there has been a request) the request for the information has been made in accordance with the information sharing principles and procedures set down in the Protocol and in Annex B, AND EITHER:

(a) the service user or other person to whom such special category data relates has given his or her Explicit Consent for the sharing of such special category data; OR

(b) some other lawful ground for sharing the special category data without Explicit Consent exists as set out in Annex B.

5.11 Each Party's Designated Officer has:

(a) notify the other Parties' Caldicott Guardians, data protection officers or equivalent of the roles of persons in such Party who will be permitted access to special category data held by such Party and any changes to such list from time to time; and

(b) maintain a list of the roles of persons in each of the Parties who will be permitted access to special category data held by the Parties,

and only those persons whose roles are identified on the list kept by the Designated Officers shall have access to special category data. All persons whose roles are identified on such list will be provided with a copy of the list to enable them to be fully aware of the identity of persons with whom they are authorised to share information. The list may be qualified, and access to special category data further protected, by limiting access to information by some persons on the list in relation to specifically named service users.

5.12 The persons holding the job titles listed in the table in Annex D, and only those persons, will be permitted access to special category data shared under this SSISA. Alterations from time to time to such list shall be notified by the Parties to each other in accordance with paragraph 9.4 below.

Audit Trail Procedure

5.13 The Parties shall abide by the audit trail procedure as set out in Annex B.

6. SPECIFIC ARRANGEMENTS

7.1 See Annex B for procedures for transfer of data, updating of data and transfer of data in emergencies or transfer to non signed up organisations.

7. AGREED GUIDANCE FOR STAFF

8.1 The information contained in Annex B is agreed between the Parties as practice that must be complied with to help ensure consistency in the processes adopted in sharing personal information.

[Those making use of this paragraph 7 should take care not to conflict with any commitments made in the Protocol, which overrides this SSISA, or with the general law. Further, any Parties intending to produce and rely upon such an Annex are advised to obtain legal advice on it.]

8. GENERAL

9.1 In this SSISA:

(a) words importing one gender shall (where appropriate) include any other gender and words importing the singular shall (where appropriate) include the plural and vice versa,

(b) references to statutory provisions shall be construed as references to those provisions as amended or re-enacted or as their application is modified by other provisions from time to time (whether before or after the date of this SSISA) and shall include references to any provisions of which they are re-enactments (whether with or without modification) and shall also include statutory instruments or orders from time to time (whether before or after the date of this SSISA) made pursuant to them,

(c) unless the context otherwise requires, references to paragraphs and to appendices are to paragraphs of and appendices to this SSISA

9.2 No variation, waiver or modification of any of the terms of this SSISA shall be valid unless in writing and signed by or on behalf of the authorised representatives of the Parties.

9.3 Nothing in this SSISA shall constitute or be deemed to constitute a legal partnership between any of the Parties or any Party the agent of any other Party and none of them shall have any authority to bind the others in any way by virtue of this SSISA, save as otherwise expressly provided in this SSISA.

9.4 All notices to be given under this SSISA will be in writing and will be sent to the address and contact name for the receiving Party shown in Annex A below or any other address the relevant Party may designate by notice given in accordance with this paragraph 9.4 to all other Parties. Notices may be delivered personally, by first class pre-paid letter or by fax. Notices will be deemed to have been received:

(d) by hand delivery - at the time of delivery,

(e) by first class post - 48 hours after the date of posting,

(f) by fax – immediately on transmission provided a confirmatory copy is sent by first class pre-paid post or delivered by hand by the end of the next business day.

ANNEX A - SIGNATORIES TO SSISA AT [INSERT DATE]

AGENCY	REPRESENTATIVE	SIGNATURE

ANNEX B – SPECIFIC PURPOSES FOR SHARING AND ROLES OF EACH PARTY

- **Domestic Abuse**
- **Anti-social Behaviour**
- **Hate Crime**
- **Modern Slavery**
- **Human Trafficking**
- **Serious and Organised Crime**
- **Prevent/Channel**

[Set out the specific purposes for which information will be shared under this SSISA in order to meet the Safer City Partnership Objectives to which this SSISA relates.

Some Parties to the SSISA may, as a result of their legal duties, have to undertake certain roles in relation to the SSISA – whether in meeting a specific legal obligation or other relevant procedural requirement that is relevant to their functions e.g Common Assessment Framework; or in maintaining certain records e.g. audit trains and reporting information, preparing statutory returns etc.

This section must therefore be written specifically for the SSISA.]

ANNEX C - DESIGNATED OFFICERS

AGENCY	NAME	POST

ANNEX D – PERSONS WITH PERMITTED ACCESS TO SPECIAL CATEGORY DATA

AGENCY	NAME	POST

APPENDIX 10

THE CALDICOTT PRINCIPLES

All organisations which are party to the Information Sharing Protocol and the related Subject Specific Information Sharing Arrangements are committed to the eight Caldicott principles when considering whether confidential social services or health information should be shared.

The Caldicott Principles clearly accord with of the UK GDPR, the Data Protection Act, and Article 8 of the Human Rights Act.

Compliance with these Caldicott Principles also requires that each partner organisation is able to map and track information streams flowing in and out of it and to be aware of where, why and with whom information is being exchanged.

Principle 1 – Justify the purpose(s) for using confidential information
Every proposed use or transfer of personally-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the Caldicott Guardian.

Principle 2 – Don't use personally-identifiable information unless it is absolutely necessary
Information items which can identify an individual should not be used unless there is no alternative.

Principle 3 – Use the minimum that is required
Where use of personally-identifiable information is considered to be essential, each item of information should be justified with the aim of reducing identifiability.

Principle 4 – Access to personally-identifiable information should be on a strict "need-to-know" basis
Only those individuals who need access to personal information should have access to it, and they should only have access to the information items that they need to see.

Principle 5 – Everyone should be aware of their responsibilities
Action should be taken to ensure that those handling personally-identifiable information – both practitioner and non-practitioner staff – are aware of their responsibilities and obligations to respect an individual's confidentiality and privacy.

Principle 6 – Understand and comply with the law
Every use of personally-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8 - Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.