Information Sharing Agreement

City of London Safer City Partnership

Govt Security Classification	Official
Publication scheme	No
Title	Information sharing agreement City of London Safer City Partnership
Version	**V1.1**
Author	RS
Review Date	May 2019
Date Issued	In draft 21 May 2018

Responsible Authorities

City of London Corporation

City of London Police

City and Hackney Clinical Commissioning Group

London Fire Service

London Probation Service

Relevant Authorities

British Transport Police

City of Westminster

Driver Vehicle and Standards Agency (DVSA)

Guinness Trust

London Borough of Camden

London Borough of Hackney

London Borough of Islington

London Borough of Southwark

London Borough of Tower Hamlets

Metropolitan Police

NHS England

Transport for London

Co-operating Authorities

Ascent Project

East London and City Mental Health Trust

East London Foundation Trust

London Ambulance Service

Network Rail

Square Mile Health, Westminster Drugs Project

St Mungo's Outreach

Toynbee Hall (City Advice)

Victim Support

Youth Offending Service

Purpose;

Identify the core legislation supported by effective information sharing.

Clarify GDPR principles when information sharing.

Identify why and how data should be shared and protected by those with a need to know.

Highlight considerations around information sharing.

To remind partners of the importance of the information sharing process for the purposes of safeguarding people, property and the environment, whilst working together.

Support joint understanding of risk and develop shared situational awareness.

Legislation supporting safeguarding. (with hyperlinks)

- *Crime and Disorder Act 1989.* Manage ASB, manage offenders, apply for orders.
- *Care Act 2014*. Protect adults at risk of abuse or neglect.
- *The Children's Act 1989* and *Children's Act 2004.* Protecting children.
- *Domestic Violence, Violent Crime and Victims Act 2004.*
- *Sexual Offences Act 2003*
- *Misuse of Drugs Act 1971* and *Drugs Act 2005*
- *Violence Against Women and Girls (VAWG) Strategy 2016-2020.*
- *Safer City Partnership Strategic Plan 2017-18*

The list is an example of core legislation and strategy that needs effective information sharing.

Government Data Protection Regulation compliance;

GDPR compliance is a legal duty. All agencies must conform to the data gathering, sharing and retention principles, which include being;

Lawful, transparent and fair

Limited to its purpose

Minimal in content to achieve its aim

Accurate

Retained for no longer than is necessary

Respect confidentiality and show professional integrity

Defining personal information;

Privacy notices are required when collecting data to comply with GDPR which explain why data is collected and upon which legal basis. Each agency is responsible for its own organisational privacy notice refresh. *CoL Privacy notice.*

Personal information is anything that directly or indirectly identifies and relates to a living person, such as a name, address, telephone number, date of birth, unique identification number, photographs, video recordings (including CCTV) etc.

Some personal information is 'special category data' and needs more protection due to its sensitivity. This includes any information about an identifiable individual that can reveal their sexuality and sexual health, religious or philosophical beliefs, racial origin, ethnicity, physical or mental health, trade union membership, political opinion, genetic/biometric data. Personal information relating to criminal offences and convictions, although not 'special category data', is still sensitive in nature and merits higher protection.

Why do we need and share personal information?

We may need to use information about a person in order to:

- Deliver our services required by law and other services which extend beyond our statutory duties;
- Safeguard people and managing offenders;
- Coordinate and manage high risk cases between agencies;
- Protect property and the environment;
- Conduct effective investigation and detection of crime;
- achieve the objectives set out in our Corporate Plans or organisational priorities;
- contact people about our services to get their views;
- investigate any concerns or complaints;
- track service expenditure;
- check the quality of services and improve them where required;
- research and plan new services or to comply with legal requirements;
- support and promote the City of London, London and the UK;

How the law allows us to use personal information

There are legal reasons why we may collect and use personal information in different circumstances.

Generally, we collect and use personal information where:

- a person or their legal representative, have given consent
- a person has entered into a contract with us
- it is necessary to perform our statutory duties or other legitimate purposes
- it is necessary to protect someone in an emergency
- it is required by law
- it is necessary for employment purposes
- it is necessary to deliver health or social care services
- you have made your information publicly available
- it is necessary for legal cases

- it is to the benefit of society as a whole
- it is necessary to protect public health
- it is necessary for archiving, research, or statistical purposes

Sharing information between agencies;

The security and transfer of data between agencies is the responsibility of all those involved in the process. Safeguards must be used to protect, transfer and store the data in whatever format it is used. Access to that data must also be protected as well as the application of the correct Government Security Classifications. When using data with a high risk to individuals or for a new initiative it may be useful to carry out a Privacy Impact Assessment (*UK Govt PIA*) or if there are intentions to use data already held.

Common daily methods of data sharing might include;

E-mail, using addresses that are more secure than open addresses, for example the use of; .pnn .gsi .cjsm

If using a non-secure e-mail address, a password encrypted document can be attached with the password being shared separately, for example via the telephone.

Personal home e-mail addresses should not be used to share information for work purposes.

Data or documents should be retained within a password protected folder or a folder with restricted staff access.

Telephone conversations should be made and received in appropriate environments.

Hard copy information must be stored in accordance with its protective marking requirements, which may include using secure cabinets or a safe. Access should be restricted to people with a legitimate 'need to know.

Documents for meetings can be held on an encrypted laptop for viewing on the screen in situ. If a hard copy is needed it can be e-mailed to the venue in advance of the meeting, printed for use and shredded prior to leaving.

Documents, electronic devices and any other form of data storage must be stored in an appropriate location and never unattended in vehicles.

Considerations when deciding to share data;

When deciding whether to share personal data (either as a provider, a recipient or both) you must identify the objective to be achieved. Consider the benefits and risks of sharing the data as well as assessing the risk of not sharing the data.

- **What is the sharing meant to achieve?** You should have a clear objective or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document what you have shared and why.

- **What information needs to be shared?** You shouldn't share all the personal data you hold about someone if only certain data items are needed to achieve your objectives. For example, you might need to share somebody's current name and address but no other information you hold about them. Another example may be

sharing the risk profile of a situation without needing to share the full documented information.

- **Who requires access to the shared personal data?** You should employ 'need to know' principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- **When should it be shared? I**t is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular situations. For the purposes of this agreement it is to achieve the objectives of the legislation and safeguarding policies that are being applied.

- **How should it be shared?** This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- **How can we check the sharing is achieving its objectives?** You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- **What risk does the data sharing pose?** For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

- **Could the objective be achieved without sharing the data or by anonymising it?** It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

Joint understanding of risk and shared situational awareness.

Accurate, concise and clear information sharing, using plain language without jargon is essential to achieving joint understanding of risk and shared situational awareness. Explaining your own organisational roles, responsibilities and capability will avoid operational ambiguity and minimise misunderstanding.

It is important to review and re-assess a situation on an ongoing basis as circumstances evolve, enabling partners to adjust to changing circumstances, apply coordinated mitigation and recognise the limitations of their service.

APPENDIX 1 – MEMORANDUM OF PARTICIPATION

By signing this information sharing agreement on behalf of their organisation signatories acknowledge their responsibilities related to information sharing to achieve the objectives of the Safer City Partnership.

Signatory;

……..

name, title and organisation

……

date