Cover note (must be read before completion):

This Data Sharing Agreement (DSA) has been created by: The National Business Crime Centre, in partnership with The Metropolitan Police Service Business Crime Hub and Information Sharing Support Unit. This was previously referred to as an information sharing agreement (ISA). It will assist officers to share data with business communities engaged in crime reduction partnerships, including, but not limited to: Business Crime Reduction Partnerships (BCRPs), Business Improvement Districts (BIDs), Town Centres. It is hoped that in time all business communities within a borough will join an accredited BCRP in partnership with the police, their local authority and any other authority in their area, allowing the use of one, all-encompassing DSA, which will replace the need for multiple agreements with businesses in the area.

This document must be completed. Please edit the relevant sections coloured:

- Blue - highlighting a specific area to be edited based on the individual circumstances and resources of the business communities and organisations involved.
- Red - highlighting a specific area, such as organisational names, that require inclusion/altering by persons completing this template.

IMPORTANT: Please note that changes to this document outside of the sections coloured Blue or Red, as described above, may invalidate the terms and conditions of this DSA/Memorandum of Understanding and therefore must be brought to the attention of your force's Business Crime Unit or Information Sharing Unit.

All DSA's should be completed in collaboration with partners required to be signatories to the agreement. Partners should only agree to the DSA if they are satisfied that the details contained within provide sufficient protections and assurance to the acquisition, storage and processing of information that they will receive and provide to police.

Definitions are provided in Appendix 1.

Title & Version	A purpose specific Data Sharing Agreement between the [Insert Your Police Force Here] and [Insert name of Business Crime Reduction Partnership/ Business Improvement District]
Author	[Insert name of author within Force]
Organisation	[Insert Your Police Force Here]
Summary/Purpose	An agreement to formalise Data Sharing Arrangements between [Insert Your Police Force Here] and [Insert name of Business Crime Reduction Partnership/ Business Improvement District] for the purpose of data sharing

DSA Ref:

Purpose Specific
Information Sharing Arrangement
Between
The [Insert Police Force Here]
And the
Business Crime Reduction Partnership/ Business improvement District

Index

Section 1. Purpose of the Agreement

This agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Describe the roles and structures that will support the exchange of information between agencies.
- Set out the legal gateway through which the information is shared, including reference to, Data Protection legislation, the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure compliance with responsibilities under Data Protection legislation and agency specific security requirements.
- Describe how this arrangement will be monitored and reviewed.

The signatories to this agreement will represent the following agencies/bodies:

[Insert Your Police Force Here] (“*The Police Force*”)

and

[Insert BCRP/BID Name and acronym] (“*The Partnership Organisation*”)

Section 2. Specific Purpose for Sharing Information

This Data Sharing Agreement between **[Insert BCU/Division Name, e.g; SW-CU],** within ***The Police Force*** and ***The Partnership Organisation*** is for the regular sharing of information, including personal data; sensitive personal data; and images of persons for the crime prevention and policing purposes defined in section 2.2.

Prior to entering into a new Information Sharing arrangement, the joint controllers identified above must carry out a Data Protection Impact Assessment. This must:

a) Describe the nature, scope, context and purposes of the processing;
b) assess necessity, proportionality and compliance measures;
c) identify and assess risks to individuals; and
d) identify any additional measures to mitigate those risks.

2.1 *The partnership organisation*

The Partnership Organisation covers the area of **[Insert geographical area of responsibility, i.e. borough, ward, street or complex]**. The current membership is diverse and includes: retail outlets, eateries, entertainment venues, licensed premises, property companies, museums, theatres, security companies, hotels, government buildings, tourist attractions and educational establishments. There are also numerous transport links within this area **[Delete or add establishments where necessary]**.

This partnership brings together a number of businesses that in isolation are having a minimal effect on crime reduction, but in partnership are capable of pooling sufficient resource and information to have a significant effect on crime reduction within their area. As a collective group, they are willing to coordinate with police and the local authority in order to address crime at a local level that will benefit businesses and the local community.

2.2 Purpose of information sharing through this agreement

The purpose of this agreement is to allow information to be shared for the purpose of the prevention, reduction and detection crime and policing purposes within the area managed by ***The Partnership Organisation****.*

College of policing Authorised Professional Practice (APP) on information management defines **policing purposes** as, “protecting life and property, preserving order, preventing and detecting offences, bringing offenders to justice, any duty or responsibility arising from common or statute law”.

Additionally, Information sharing must be in furtherance of the National Police Chiefs' Council mission for policing, which is, "To make communities safer by upholding the law fairly and firmly; preventing crime and antisocial behaviour; keeping the peace; protecting and reassuring communities; investigating crime and bringing offenders to justice."

The Crime and Disorder Act 1998 provides that responsible authorities must create a strategy for the reduction of crime and disorder in their area. This agreement forms part of that strategy.

This agreement will provide a mechanism for T***he Police Force*** and ***The Partnership Organisation*** to share personal and special category data, as well as specific crime statistic*s,* about persons convicted or suspected of involvement in business related crime in the local area. This information will comprise of extracts of data from ***The Police Force*** intelligence, crime recording and custody imaging systems. It will also include conviction information and non-conviction information regarding arrests, charges and cautions. This information will only be passed on to members of ***The Partnership Organisation***. Other non-conviction information and images may be shared to achieve this purpose on a case-by-case basis, if it is deemed to be proportionate, lawful and necessary.

This agreement, on a case-by-case basis and subject to local risk assessment, will allow ***The Police Force*** to share information with ***The Partnership Organisation*** members about offenders that have received an Order under relevant Anti-Social Behaviour legislation, which prohibits them from entering or manifesting certain behaviours within the vicinity of ***The Partnership Organisation*** area. Members will be able to assist ***The Police Force*** in identifying persons in breach of these Orders. Such information circulated to specific partners will consist of a conviction photograph, Name of subject and Relevant ASBO/CBO conditions.

It is also intended that relevant information related to crime and the prevention of crime, held by the partnership, for such purposes as implementation of exclusion order schemes, will be passed to ***The Police Force*** if there is a belief that the information is not already in ***The Police Force's*** possession and would assist with the purpose of this agreement.

Any personal data shared must be considered necessary for the identified purpose. Necessary means that if you can reasonably achieve the same purpose without sharing the data or all of the data, then you will not have a lawful basis. This means that data should only be shared with organisations to whom it is relevant and that the minimal amount of data should be shared for the purposes set out in this agreement.

2.3 Roles and structures that will support the exchange of information between agencies

Individual members of the partnership will report information about incidents of crime and anti-social behaviour that impacts on their premises, staff or customers to the partnership's administrator. The administrator stores and processes this information (onto a secure encrypted database; a secure encrypted intranet) that members must use private access codes and passwords to enter. The administrator decides if the quality of the data submitted by members is compliant with the member's codes of practice and may disseminate information to members by means of newsletters or bulletins displayed on the system. The secure intranet site is an Information Sharing website that allows businesses and ***The Police Force*** to share CCTV images, crime statistics, photographs and personal details of convicted persons and persons with Anti-Social Behaviour Orders or Criminal Behaviour Orders (ASBO/CBO) and persons subject to orders or restrictions imposed under relevant Anti-Social Behaviour legislation.

The Partnership Organisation administrator or their authorised representative / Safer Neighbourhood Team, will post the information shared through this agreement to the secure site. The site is split into separate areas depending on crime type and time of day. Therefore, members will only be able to see sections of the intranet site, which are relevant to them. Access to the secure intranet is by invitation only by the Business Crime Partnership administrator or their authorised representative and is reserved only for members of ***The Partnership Organisation***.

Primarily the members will use the information provided to familiarise themselves, security and other staff likely to fulfil that role, of the appearance of likely offenders, banned persons or suspects at large. This will best prepare them to deter crime and make informed decisions when safety risks for staff and members of the public are apparent. The information is used for business premises that are members of the partnership and is not to be removed from those premises. Printing and copying rights have been removed from the system. The information is only accessible to members who have signed Data Integrity forms and read, and confirmed they have read the 'must read' documents on the secure intranet site. These documents must echo this agreement and fully comply with Data Protection Law.

Partnership members, local authority CCTV operators and police will make use of a private, two way, radio network. This allows members to broadcast intelligence and updates on real-time incidents and to request assistance when required. Linking in with CCTV suites will allow image and evidence capture and police officers will have opportunity for early intervention to prevent crime, or apprehend offenders before they can make good their escape.

Members who use radios will receive training by police or the scheme administrator. Personal data, special category data and criminal offence data

will only be transmitted when deemed necessary in the immediate circumstances. When conducted by police, details of:

a) What personal data is disclosed and
b) The reason for its disclosure.

will be recorded on ***The Police Force*** systems and all police officers will be reminded of the requirements of MoPI and the Data Protection Principles in relation to transmissions.

2.4 Benefits to *the police force*

This agreement supports the activities of such partnerships as recommended in the Crime and Disorder Act 1998, which places a responsibility on police to work in partnership with other agencies, organisations and individuals in the furtherance of the reduction of crime and anti-social behaviour and the reduction of the fear of crime and anti-social behaviour in the community.

The Police Force benefits will be: the reduction of crime and anti-social behaviour within ***The Partnership Organisation*** area; improved opportunities for the apprehension of offenders and reduction in the fear of crime. This will be measured in crime statistics and outcomes obtained from crime reporting systems and qualitative feedback from the community provided in ward panel meetings and Customer Satisfaction Surveys.

This Information Sharing process will increase opportunities for better partnership working within the business community. It will also assist the local Crime Reduction strategy. Statistically, levels of detections in areas participating in a crime reduction scheme improve, on a national level, from 26% to 82% (Action Against Business Crime AABC 2008). The primary reason for this is the improved intelligence from the sharing of information.

2.5 Benefits to *the partnership organisation*

The establishing of BCRP/BID helps to focus partnership awareness of local crime and improve the quality of shared intelligence with police and other agencies. All businesses will benefit from the reduction of crime and anti-social behaviour within the business district. This in turn encourages better co-ordination of police and partnership resources to deter and prevent crime.

Sharing relevant information improves the safety of employees within the area. It also assists in protecting the assets of the businesses trading within the area. The increased levels of detection will improve profitability and maintain a healthy consumer market, which is currently maintained by a combination of residents, commuters and tourists. Protecting these sections of the community improves the sustainability and continuity of the local business partners.

In addition, members will be alert to the fact that persistent offenders who may already be subject to their exclusion schemes may also be subject to orders or restrictions imposed under relevant ASB legislation and thus will identify occasions when police may be best suited to deal with certain issues rather than placing employees at risk.

2.6 Community Benefits

Local communities will benefit from being able to enjoy safer environments in which to shop, live, work and commute. This in turn increases employment opportunities and stimulates local economic growth.

Section 3. Legal basis for sharing and what specifically will be Shared

Data Protection legislation as a framework for how to process (including share) personal, special category and criminal offence data. Article 6 of the GPDR sets out the lawful bases for processing personal data. Article 9 of the GDPR sets out the lawful bases for processing special category personal data and Schedule 1 of the DPA 2018 sets out the lawful bases for processing criminal offence data. The six Data Protection Principles set out in Article 5 of the GDPR must also be complied with when sharing data.

Part 3 of the Data Protection Act 2018 implements the Law Enforcement Directive 2016/680 into the UK. This regulates the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

A competent authority is:

(a) a person specified or described in Schedule 7, and
(b) any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes.

[Insert Your Police Force Here] is a competent authority under schedule 7 of the DPA 2018.

For other bodies who are not competent authorities but who are processing personal data it is the GDPR and other parts of the DPA that regulates their processing activities.

[Insert name of Business Crime Reduction Partnership/Business Improvement District] is not a competent authority.

The law applying to both will, as outlined in this agreement, allow [Insert Your Police Force Here] and [Insert partnership name] to be joint data controllers in relation to the data shared under this agreement.

3.1. First Principle

Competent Authorities
The first data protection principle in Part 3 of the DPA states that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

Other Bodies

The first data protection principle in the GDPR states that data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

3.1.1. Lawfully

Competent Authorities
A public authority must comply with the law when sharing personal data and must be able to rely on a lawful basis as set out in Data Protection Law.

The purpose of this agreement is to allow personal data to be shared for policing purposes within the defined area through working with commercial businesses. Section 6 of the Crime and Disorder Act 1998 provides that responsible authorities must create a strategy for the reduction of crime and disorder in their area. This agreement forms part of that strategy allowing the data sharing powers implied in law to be exercised.

The Police Force also has common law duties and functions as defined in APP in section 2 of this agreement.

Other Bodies
Part 1 of Schedule 2 of the DPA does not provide a power to disclose information containing personal data but it allows personal data to be disclosed if the controller is satisfied that not disclosing the information would prejudice the prevention/detection of crime and/or the apprehension/prosecution of offenders.

Under this agreement, if members of ***The Partnership Organisation*** were satisfied that not disclosing information would prejudice these reasons, they are then exempt from the usual non-disclosure provisions and may provide information required either as a result of a request or proactively disclose information for this purpose. The data controller must also be able to rely on a lawful basis for disclosing personal data/special category personal data/criminal offence data – see paragraph 3.1.6 below. The lawfulness of sharing information by ***The Partnership Organisation*** will be decided on a case-by-case basis.

3.1.2. Duty of Confidence

If an organisation has received any information in confidence, you almost certainly have a Duty of Confidence towards the data subject.

The information to be shared within the context of this agreement will not contain any information that has been received in confidence by any member of ***The Police Force****.*

The common law duty of confidence that ***The Police Force*** has for information it holds about convicted offenders is not an absolute obligation. The information shared under this agreement will override the duty of confidence by its disclosure being in the substantive public interest. The public interest factors for this agreement will be for the purpose of preventing the commission of criminal offences and/or bringing offenders to justice.

The Police will provide information, which is subject to a duty of confidence, such as images and names, to members. The Police will also provide where relevant: addresses; description; ethnic origin; PNCID numbers; vehicle registration(s); associates and any other personal or sensitive data where there is a need and in the interest of public safety. Provision of information by police will be measured on a case-by-case basis. Any other information exchanged such as crime statistics or conviction information will already be in the public domain and not be subject to any duty of confidence.

3.1.3. Fair Processing Requirements

The images to be shared are photographs taken when individuals have been detained at a police station for one of the offences listed at Principle 3, or have been captured on CCTV or Body Worn Camera footage and are suspected of committing one of the offences listed at Principle 3. S.64A(4) of the Police and Criminal Evidence Act 1984 (PACE) outlines the purposes for which the image may subsequently be used. This includes: *'"may be used by, or disclosed to any person for any purpose related to the prevention or detection of crime"…'.*

At the time the image is taken, it is ***The Police Force*** policy and procedure to inform individuals that their image may be used, disclosed or retained. This is in accordance with PACE 1984 – Code of Practice D, Part 5 and satisfies the requirements of fair processing.

In addition to the procedure outlined above, ***The Police Force*** displays a Fair Processing Notice in police station front offices and in custody suites. It is also available to view through the Freedom of Information Publication Scheme pages on ***The Police Force*** website: i.e. http://www.met.police.uk/foi/pdfs/other_information/corporate/fair_processing_notice_2013.pdf **[Insert relevant web address here].**

The Notice states that personal information will be used for the purposes of 'Policing' and also states that ***The Police Force*** may share this information with a variety of other agencies for the purposes of Policing.

The Partnership Organisation also have a Fair Processing Notice detailing how it processes personal information. This is available **[Please state where this can be found]**. They will also be registered with the Information Commissioners Office for processing personal data.

3.1.4. Legitimate Expectation

An individual's expectation as to how information given to a public body will be used will be relevant in determining whether the first data protection principle has been complied with.

There is a legitimate expectation that the police will do what they can to maximise fairness and protection under the law. The sharing of information within the terms of this agreement satisfies the expectation that police information will be used for the purposes of crime reduction and prevention as well as the maintenance of public safety.

It is reasonable to assume that people previously convicted of one of the offences detailed at Principle 3 in this document would have a legitimate expectation that the police would share personal information appropriately with other agencies if it would be relevant to the type and location of the offence(s) committed.

Details of this and most other non-sensitive Data Sharing Agreements will be published in line with the requirements of the Freedom of Information Act 2000, on ***The Police Force*** Publication Scheme. This will also allow members of the public to understand how ***The Police Force*** may use their personal information. This is in addition to the information provided to them in the Fair Processing Notice mentioned above.

3.1.5. Human Rights - Article 8: The Right To Respect For Private And Family Life, Home And Correspondence

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests 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.

In pursuit of a legitimate aim:
The aim of this agreement is to permit the policing purposes defined in this agreement within the designated area managed by ***The Partnership Organisation,*** which is in the public interest.

Proportionate:
The information to be supplied is proportionate for the needs of this agreement. The information is shared on a case-by-case basis, with only the minimum amount of information necessary, for the purposes of identifying and monitoring individuals within ***The Partnership Organisation*** area.

Appropriate and necessary to a democratic society:

Supporting law and order and working to improve its effectiveness and the public confidence in it, is an activity necessary to a democratic society.

3.1.6. Lawful Basis for Sharing Personal Data

In addition to the legal criteria set out above, the information sharing arrangement must satisfy at least one condition in Part 3 of the Data Protection Act 2018 (DPA) and in Article 6 of the General Data Protection Regulation (GDPR) in relation to personal data.

Competent Authorities

Part 3 of the DPA 2018 states that, lawful processing by a competent authority must either be carried out with consent of the data subject or where the processing is necessary for the performance of a task carried out by a competent authority.

This supports the implied power to share data for the function set out in section 6 of the Crime and Disorder Act 1998, the common law duties and core functions of the police, which are to prevent and detect crime and disorder.

Other Bodies

Article 6(f) of the GDPR states that the processing is lawful if the:

> *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

The legitimate interest being pursued by ***The Partnership Organisation*** is to run successful businesses in a safe environment for both staff and customers and there is no other reasonable means of achieving this. The sharing of information will not override the rights and freedoms of the data subjects and will not cause any unjustified harm.

3.1.7. Lawful Basis for Sharing Criminal Offence Data

Competent Authorities

Under Part 3 of the DPA criminal offence data is categorised in the same way as personal data. The legal basis outlined in paragraph 3.1.8 will apply.

This will include the following category of information:

- The commission or alleged commission of any offence.
- As the photographs to be circulated are images of individuals who have been convicted, detained or suspected of any of the offences listed in

Principle 3 (below), by implication sensitive personal information is being shared.

Other Bodies

Section 10, subsection (5) of the DPA 2018 permits the processing of personal data relating to criminal convictions and offences or related security measures is only authorised if it meets a condition in Part 1, 2 or 3 of Schedule 1 of the DPA.

In Schedule 1 Part 2 processing, including disclosure, of criminal offence data can take place for purposes of preventing or detecting unlawful acts or for the apprehension or prosecution of offenders. As long as the processing is necessary for the purpose, consent of the data subject is not required if this would be prejudice the prevention or detection of the unlawful act.

If ***The Partnership Organisation*** is disclosing criminal offence data to a competent authority then there is no need to have an appropriate policy document in place. However under Article 30 of the GDPR a record must be maintained by ***The Partnership Organisation,*** which identifies the processing condition that is being relied on under the DPA 2018 and which lawful basis is being relied upon under Article 6 of the GDPR.

In circumstances other than disclosure to a competent authority, for any other processing of criminal offence data, the controller requires to have an appropriate policy document in place which:

(a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and
(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained.

The controller must retain the policy document and review it from time to time. It must be made available to the ICO on request. This must be in place for the time that the processing takes place and for six months afterwards.

If the disclosure is made under this provision ***The Partnership Organisation*** is exempt from providing the information required by Articles 13 and 14 of the GDPR to the data subject to the extent that this would prejudice the purposes of preventing or detecting unlawful acts or for the apprehension or prosecution of offenders.

3.1.8. Lawful Basis for Sharing Sensitive or Special Category Data

If the information is "sensitive" as defined in section 35(8) of the DPA or "special category" as defined in Article 9 GDPR (that is, where it reveals

racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trades union, physical/mental health, or sexual orientation or sex life) then processing is only permitted in certain cases.

Competent Authorities

For Competent Authorities there is a provision in Part 3 of the DPA 2018, which sets out that sensitive data can be processed where:

(a) the processing is strictly necessary for law enforcement purposes;
(b) the processing meets at least one of the conditions in Schedule 8; and
(c) at the time when the processing is carried out, the controller has an appropriate policy document in place.

In schedule 8 processing which is necessary for reasons of substantial public interest can be carried out as long as it is necessary for the exercise of a function conferred on a person by an enactment or rule of law. Section 6 of the Crime and Disorder Act 1998, the common law duties and core functions of the police, to prevent and detect crime and disorder provide the legal basis to share sensitive personal data to the extent that it is necessary for these purposes.

Section 42 of the DPA 2018, states that the competent authority must also have a policy in place which:

(a) explains the controller's procedures for securing compliance with the data protection principles, and
(b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained.

The competent authority must retain the policy document and review it from time to time. It must be made available to the ICO on request. This must be in place for the time that the processing takes place and for six months afterwards.

The competent authority must maintain a record of processing, which includes reference to the condition in Schedule 8 that is being relied on, such as that processing is necessary for a law enforcement function, identifying whether personal data is retained or erased, or if there is a reason for not doing this.

Other Bodies

For other bodies, sharing of special category data will be carried out on the basis of Art 9(2)(g) of the GDPR.

The processing of special category data is prohibited under the GDPR unless one of the conditions set out in Article 9(2) applies and in relation to this agreement subparagraph (g) allows:

"processing, [which] is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to protection and provide for suitable and specific measures to safeguard the fundamental data rights and the interests of the data subject".

The relevant Member State law is the DPA 2018, where section 10 states that the processing of special category data can take place if a condition in Part 2 of Schedule 1 is met. The processing condition referred to above in relation to the processing/sharing of criminal offence data would apply to the sharing of special category data in relation to this agreement. This would require substantial public interest and the same policy documentation would need to be in place.

3.2. Second Principle

Competent Authorities
The Law Enforcement Purpose for which the personal data is collected on any occasion must be specified, explicit and legitimate and it must not be processed in a manner that is incompatible with the purpose for which it was collected.

Other Bodies
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The information to be shared under this agreement will be that which was originally obtained for the prevention/detection of crime and/or the apprehension/prosecution of offenders.

Sharing this information with a third party, in this case ***The Partnership Organisation*** members or the Police, will not result in the information being processed in any manner contradictory to the original purpose.

If ***The Partnership Organisation*** is disclosing personal data to ***The Police Force*** using the legal basis set out in Part 1 of Schedule 2 where it has decided that not sharing the personal data would prejudice the prevention and detection of crime or the apprehension or prosecution of offenders, then ***The Partnership Organisation*** *is* not required to comply with the second principle to the extent that it would prejudice the purpose of the Sharing Agreement.

3.3 Third Principle

Competent Authority

Data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Other Bodies
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

A secure email will be sent to ***The Partnership Organisation*** Business Crime Partnership Manager or their authorised representative regularly. This will contain images extracted from ***The Police Force*** custody imaging system, CCTV or Body Worn Camera footage of individuals who have previous convictions or suspected involvement in any of the following offences within the last two years and are believed to be committing criminal acts again within the area covered by ***The Partnership Organisation***;

- Theft (and kindred offences)
- Deception & fraud
- Public nuisance
- Public order offences
- Racially aggravated offences
- Serious acquisitive crime
- Violence or threat of violence
- Use or threat of weapons
- Alcohol related offences
- Drug related offences
- Sexual offences
- Robbery
- Burglary
- Terrorism
- Violent political activism
- Sexual offences
- Any other offences that the partnership organisation is able to take steps to prevent or to reduce the risk of harm to people or damage or destruction of property within the partnership area

These offences will have taken place in ***The Partnership Organisation*** area, surrounding or similar areas where the need to share with local businesses is justifiable, proportionate and necessary.

Each image will be numbered and annotated with the name of the individual along with basic information about the type of offence committed and only other information deemed lawful and necessary will be included. No other information will be attached to the image, or supplied to ***The Partnership Organisation***.

This is the minimum information necessary to allow members and their employees to identify and subsequently monitor an individual for suspicious behaviour or activity if they enter the designated area.

Any personal data shared must be considered necessary for the identified purpose. Necessary means that if you can reasonably achieve the same purpose without sharing the data or all of the data, then you will not have a lawful basis. This means that data should only be shared with organisations to whom it is relevant and that the minimal amount of data should be shared for the purposes set out in this agreement.

3.4 Fourth Principle

Competent Authority
Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

The Police Force must distinguish between personal data based on facts, so far as possible, and personal data based on personal assessments i.e. witness statements.

There should also be a clear distinction drawn, where relevant and as far as possible, between personal data relating to different categories of data subject, such as:

(a) persons suspected of having committed or being about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) persons who are or may be victims of a criminal offence;
(d) witnesses or other persons with information about offences.

All reasonable steps must be taken to ensure that personal data, which is inaccurate, incomplete or no longer up-to-date, is not transmitted or made available for any of the law enforcement purposes. Therefore, the quality of personal data must be verified before it is transmitted or made available and in all transmissions of personal data, the necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included. If, following the data being transmitted it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Other Bodies
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it was processed, is erased or rectified without delay.

This information comes from ***The Police Force*** corporate systems and is subject to normal procedures and validations intended to ensure data quality.

Any inaccuracies should be notified to ***The Police Force*** by the signatory to this agreement representing ***The Partnership Organisation.*** The notification is to be by secure email or in writing for auditing purposes.

Whilst there will be a regular sharing of information, the data itself will be 'historical' in nature. Specifically this means that the data fields exclusively relate to individual actions or events that will have already occurred at the time of sharing. These are not categories of information that will alter substantially or require updating in the future.

In addition there will be **[describe the required time frame]** security meetings, hosted by The Partnership Organisation where feedback can be obtained and recorded as to whether the individuals have been seen entering the area or its retail outlets.

3.5 Fifth Principle

Competent Authority
Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Other Bodies
Personal data shall be 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.

A new electronic file of images will be updated and supplied to ***The Partnership Organisation*** on a regular basis. The update will supersede the previous electronic file.

The process for the destruction or disposal of the previous file can be found in section 4 of this agreement. As stated in the fourth principle above, the images will be regularly weeded via feedback to ***The Partnership Organisation*** manager.

The secure Intranet database will automatically apply time limits to photos and intelligence held online to ensure information is not kept for longer than is necessary.

Printing, sharing and otherwise exporting the data from the system must be restricted as much as technically possible. Policies and written user

agreements must prohibit the exporting of data via any means. This ensures that the administrator can remove data in a timely and effective fashion.

3.6 Sixth Principle

Competent Authorities
Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss destruction or damage).

Other Bodies
Personal data shall be 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.

Measures to satisfy the Sixth Principle are detailed in Section 4 of this agreement.

3.7 Data Subject Rights

Competent Authority
Part 3, sections 43 to 54 of the DPA set out the obligations that the police force has in relation to data subjects.

In relation to personal data provided by ***The Partnership Organisation*** to ***The Police Force***, Part 1 of Schedule 2 of the DPA 2018 provides that ***The Police Force*** will be exempt from the obligations under Articles 13, 14 and 15 of the GDPR to provide the data subject with information collected about them and to provide confirmation of processing or access to the data.

Other Bodies
Chapter III, Articles 12 to 23 of the GDPR sets out the obligations that the partnership organisation has in relation to data subjects.

In relation to data provided by ***The Police Force*** to ***The Partnership Organisation***, part 1 of Schedule 2 of the DPA 2018 provides an exemption to the obligation to comply with data subject rights set out in Articles 13 to 21 of the GDPR. Information can be withheld if it is being processed for the purposes of the prevention or detection of crime or for the apprehension or prosecution of offenders and to comply with the rights would prejudice those purposes.

Otherwise, ***The Police Force*** and ***The Partnership Organisation*** are joint data controllers in relation to the personal data shared under this agreement. If required both Parties shall ensure that their privacy notices comply with the DPA 2018 and the GDPR.

If ***The Partnership Organisation*** receives a Right of Access Request (ROAR) in relation to any of the personal data shared under this agreement, or any other request from a data subject to exercise his or her rights under Data Protection Law, ***The Partnership Organisation*** will seek the views of ***The Police Force*** in relation to disclosure of information under a ROAR within seven calendar days of receiving the application.

If ***The Police Force*** receives a ROAR in relation to any of the personal data shared under this agreement, or any other request from a data subject to exercise his or her rights under Data Protection Law, ***The Police Force*** will seek the views of ***The Partnership Organisation*** in relation to disclosure of information under a ROAR within seven calendar days of receiving the request.

Each Party shall keep a record of Data Subject Requests received by that Party and any information provided to the Data Subject and/or exchanged with the other Party. The Parties agree to provide such reasonable assistance to the Party receiving a Data Subject Request (within seven calendar days of any written requests) as is necessary for the receiving Party to comply with the Request.

The Police Force reserves the right to withdraw right of use of the data at any time.

3.8 Transfer of Personal Data to Third Countries or International Organisations

A transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection or if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The data shared under this agreement is intended solely for use within the area managed by ***The Partnership Organisation*** and would not be transferred to third countries or international organisations. Compliance with the above provisions are a condition of membership.

Section 4. Description of arrangements including security matters.

4.1 Process

The relevant Safer Neighbourhood Team will be responsible for extracting data from ***The Police Force*** systems, which will then be placed on a prepared information page that will explain the information provided and the reason it is relevant to members. The information will be placed in a briefing and passed by secure email to ***The Partnership Organisation*** Business Crime Partnership Manager or their authorised representative on a regular basis / uploaded directly on to the secure intranet site.

The Partnership Organisation Business Crime Partnership Manager will post the information shared through this agreement on the secure internet/intranet site. This site is hosted by **[insert name of intranet site e.g. Littoralis]**, with the platform being **[insert name e.g. *DISC* (Database and Intranet for Safer Communities)**]. Once information is posted, it will form part of a weekly newsletter that is automatically generated and sent to members. The member must log in to be able to view the information.

All requests for ***The Police Force*** information, sharing of information and denied requests will be recorded on ***The Police Force*** intelligence system in line with statutory requirements and The Information Sharing SOP.

Information will not be shared to businesses outside of the secure intranet. Upon becoming a member of the secure intranet site, the signatory will receive a username and password and only that person will have the authorisation to access the information. Once accessed, the distribution of this information to others and matters of security will be the responsibility of that person but it must be done in compliance with Data Protection Law. The member will provide an email address to receive the notifications. Members will be given full instructions on how to handle the information and this will not be incompatible with the instructions in this section.

On occasion there may be the need for the Safer Neighbourhood Team to deliver the information they have provided to the Business Crime Partnership Manager direct to members of the partnership via a briefing. The same selection of information process will occur as with the email briefings.

Members of ***The Partnership Organisation*** will be able to contact ***The Police Force*** on a designated telephone number where if they have a person detained who has committed an offence, and they have already confirmed the identity of the detained person, a Police National Computer (PNC) check can be conducted in order for ***The Police Force*** officer to establish whether that person is wanted for an outstanding offence.

The Officer conducting this check will ask for the members location, offence that the person detained has committed and the reason for needing to

conduct the check. This will be recorded in the normal way on PNC so an audit trail is available through a #TE check. The officer conducting the check will then assess any existing PNC record(s) and disclose if there is an immediate threat of danger to themselves or the public. They will also disclose if the person detained is wanted by the police. The caller is then advised that it is their decision as to how they wish to conclude the incident. ***The Partnership Organisation*** will be updated with a requirement that all members who wish to utilise this service must keep a record, in their store, of the subject's name, the person conducting the check, the circumstances and the final disposal.

Members of ***The Partnership Organisation*** can share information amongst themselves and to police on the secure intranet site. This information will relate to incidents of crime and disorder in and around their premises and individuals suspected of involvement with these incidents. Any information that ***The Police Force*** receive either via the secure intranet site or direct from members will be transferred to the appropriate corporate police system.

4.2 Confidentiality and Vetting

The Partnership Organisation Business Crime Partnership Manager has been vetted by ***The Police Force*** to NPPV level 2. Security officers employed at member venues involved in the partnership have valid licences from the Security Industry Authority (the regulating body for security providers). As part of this, all security guards will have completed a check from the Disclosure and Barring service (DBS).

However, the value of the information they will access is 'Official Sensitive' (formerly 'Restricted') and they will need this information in order to carry out their work. ***The police force*** Code permits staff 'need-to-know' access to Official Sensitive information. The person disclosing the information must give additional consideration and justify why it is necessary to share this additional information with someone that is not vetted based on the circumstances in the particular case.

The partnership manager must ensure that information shared with members is the bare minimum to achieve the purpose and must give due consideration to the fact that members themselves may not be vetted to the same level, if at all. The technical controls in this agreement mitigate some of this risk.

4.3 Movement of Information

Movement of any information under this agreement is conducted electronically.

CJSM is a Home Office supported programme that was developed to facilitate better communications between all those involved in the criminal justice system.

However, the secure email facility provided as part of the programme, is one that can be used for many other purposes such as wider Information Sharing. The CJIT programme supports its wider application.

Sending email between ***The Police Force*** .pnn email addresses and .cjsm email addresses is technically secure. It means that those agencies that are not part of the GCS, for example Local Authorities or regulatory bodies such as the Security Industry Authority, can still have secure email connections with the members of the GCS and other CJSM users.

The Business Crime Partnership Manager at ***The Partnership Organisation*** has a Password Enabled Secure CJSM email address, which allows ***The Police Force*** to send the briefings securely. If briefings are shared under this agreement, each member of partnership is required to have access to individual Password Enabled CJSM email accounts, which then allows the sanitised briefings to be securely distributed.

The Partnership Organisation secure intranet site is protected by technical measures and is password encrypted. The site has met ***The Police Force*** required standard of security and is fully compliant with principles of the Data Protection Act 2018 The site abides with guidance given by the Information Commissioners Office. Correct use and disclosure of information is a condition of membership of ***The Partnership Organisation***.

4.4 Partner's Building & Perimeter Security

Where Official Sensitive information is concerned, the information will be kept within a secure location with a managed and auditable access control system that the general public have no access to.

The information is only accessible via the secure **[intranet/internet, secure email such as CJSM etc…]** to which only the Business Crime Partnership Manager and/or their authorised representative will have access. Only they will have access to the secure system and other relevant information. Their computer has an individual secure password; the office is locked and alarmed within an office block.

4.5 Storage

Information added to the secure intranet will be stored on a secured server, which automatically deletes the information once the time limits for displaying the information runs out. The secure intranet has met ***The Police Force*** required standard of security.

Upon becoming a member of the secure intranet site, the signatory will receive a username and password and only that person will have the authorisation to access this information.

4.6 Security Incidents and Breaches of the Agreement

Non-compliance and/or breaches of security arrangements will be reported to ***The Partnership Organisation*** Business Crime Partnership manager and dealt with in accordance with their existing code of conduct between The Company and the stores within The Partnership.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the members of The Partnership's internal disciplinary procedures. If misuse is found, there should be a mechanism to facilitate an investigation into initiating criminal proceedings. ***The Partnership Organisation*** management agree to fully support this investigation.

Additionally, any security incidents, breaches, or newly identified vulnerabilities will be reported to the Data Protection Officer (DPO) for the police force and the signatory of this agreement. The signatories will ensure that the *DPO* is informed of any security incident(s) or breach(es) to this agreement, including unauthorised disclosure or loss of information, through ***The Police Force*** [include the internal and external contact details of the DPO and all relevant security departments].

All parties to this agreement are aware that non-compliance with the terms of this agreement may result in the agreement being suspended or terminated and the breach will be reported to the Information Commissioners Office who may carry out an investigation and proceed to take enforcement action including the imposition of administrative fines.

4.7 Disposal

In the case of briefings received via secure email, when a new briefing is received by the Business Crime Partnership Manager an email acknowledging receipt of it will be sent along with confirmation that the previous document has been destroyed. The sender will specify the retention period of the briefing giving due consideration to the necessity of retention on a case-by-case basis and only to achieve the defined purpose.

The secure Intranet database will automatically apply time limits to photos and intelligence held online to ensure information is not kept longer than is necessary. The period for automatic deletion will either be specified by the uploader or applied by the scheme administrator, whichever is the shorter period. The data must only be kept for as long as is necessary to achieve the purpose of sharing and will be determined on a case-by-case basis, giving due consideration to the seriousness of the offence and necessity for the data in achieving the purpose of this agreement.

The administrator of the partnership will be responsible for ensuring destruction of data through automated means or manually as required.

4.8 Compliance

The Partnership Organisation Crime Partnership Manager will be responsible for ensuring that all agreed security agreements are complied with. Any issues around compliance with the agreed security measures will form part of the initial review of the agreement.

All partners are responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under Data Protection Law

The Partnership Organisation Business Crime Partnership manager will hold a copy of this agreement, which will be kept in a central location so members of staff can access and familiarise themselves with the exact content and arrangements in place.

Partners agree where necessary to allow peer-to-peer reviews to ensure compliance with the security section of this DSA. Compliance with these security controls will be catered for in the periodic reviews of the DSA.

4.9 Review

This agreement will be reviewed three months after implementation, then at six months and at least annually thereafter.

4.10 Freedom of Information Act and Data Protection Act 2018

Normal practice will be to make all Data Sharing Agreements available on ***The Police Force*** publication scheme. It is recognised that ***The Police Force*** may receive a request for information made under the DPA 2018, that relates to the operation of this agreement. Where applicable, they will observe the Code of Practice made under S.45 of the Freedom of Information Act 2000.

This Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to information held only by the other authority.

Individuals can request a copy of all the information an organisation holds on them, by making a ROAR. This may include information that was disclosed to that organisation under this agreement. Where this is the case, as a matter of good practice, the organisation will liaise with the originating organisation to

ensure that the release of the information to the individual will not prejudice any ongoing investigation/prosecution.

Section 5. Agreement to abide by this arrangement

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of required information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners at least annually.

Date of agreement XX/XX/XXXX

Date of first review (3 months after agreement) XX/XX/XXXX

Date of Second review (6 months after last review) XX/XX/XXXX

Date of first annual review (12 months after last review) XX/XX/XXXX

To be reviewed annually thereafter or immediately following a material change in circumstances.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this Data Sharing Agreement:

Agency	Post Held	Name	Signature	Date
(Business Crime Reduction Partnership)	**Business Crime Partnership Manager**			
(Business Crime Reduction Partnership)	**Board Member**			
(Business Crime Reduction Partnership)	**Board Member**			
Police				

Appendix 1

Definitions

Data Protection Law

This refers to:

- The General Data Protection Regulation 2016/679
- The Data Protection Act 2018
- Any other EU or UK data protection law, which supersedes this legislation.

Personal Data

Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This can include CCTV footage and photographs, which may also be criminal offence data.

Special Category Personal Data

- the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
- the processing of data concerning health;
- the processing of data concerning an individual's sex life or sexual orientation.

Criminal Offence Data

The definition is set out in section 10 of the DPA 2018 and includes personal data relating to:

(a) the alleged commission of offences by the data subject, or
(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.