Privacy Notice: For the detection& prevention of crime within the Northfield BID area

This document describes the Northfield Business Crime Prevention Operation (the Operation) and explains why the Operation processes the personal data of specific individuals (Offenders) and what the lawful basis is for that processing. It describes the kind of information about Offenders that the Operation processes and what it does with that information.

1. **Contact details**

   Northfield Town Centre BID Ltd, c/o 693 Bristol Road South, Northfield, Birmingham B31 2JL Email address: bid@northfieldbid.com

2. The Operation's Data Representative is responsible for ensuring its compliance with current Data Protection law and can be contacted at the above address or email address. Northfield BID is registered with the Information Commissioners Office as *Northfield Town Centre BID Ltd*.

Purpose of processing personal data

3. Members of the Operation have the right to protect their property, staff and customers from crime and anti-social behaviour and to exclude from their premises any individuals who are proven threats to their property, staff or customers or disrupt the peaceful enjoyment that their customers expect from the goods and/or services that our Members offer. The Operation processes Offenders' personal data for the management as part of its "Protecting Northfield"BID2 priority on behalf of its Members, to inform Members of an offender's modus operandi, to collate intelligence on criminal activity within the area of the Operation's operation and to contribute to legal proceedings against Offenders where appropriate.

4. The Operation's area of operation and its Public Space Protection Order (Northfield Victoria Common) is within the boundaries of Northfield Town Centre BID area.

Types of processing

5. The Operation undertakes the following types of processing of personal data of Offenders:

   a) Data collection; see Sources of personal data below;
   b) Data storage; storage of Offenders' data in a facility independently certified as secure to a high standard;
   c) Data retention; see Data Retention period below;
   d) Data collation; associating individual Offenders with multiple incidents, and with other Offenders;
   e) Data sharing; as defined in Recipients, or categories of recipients, of personal data below;
   f) Data deletion; see Data Retention period below;
   g) Data analysis; of de-personalised data for historical comparisons etc.

Lawful basis of processing

6. The Operation's Members' 'legitimate interests' provides the lawful basis on which it may process specific items of Offenders' personal data for specific purposes without Offenders' consent.

7. The Operation has assessed the impact of its processing on Offenders' rights and freedoms, has balanced these with its Members' own rights, and has concluded that its Members' rights prevail over Offenders' rights in this specific matter. Therefore, for the purposes of the management of the public space protection order , the retail radio scheme and WhatsApp Group schemes on behalf of its Members, to inform Members of an offender's modus operandi(someone's habits of working, particularly in the context of business or criminal investigations), to collate intelligence on criminal activity within the area of the Operation's operation and to contribute to legal proceedings against Offenders where appropriate, Members' legitimate interests constitute the Operation's lawful basis for processing Offenders' personal data without requiring consent.

8. Categories and types of personal data processed

a) Offender's distinguishing marks and facial image and any relevant information about the nature of his/her activities; the purpose of this processing is to enable Members to identify Offenders in order to submit reports about them, to include them in a list or gallery of excluded persons (if appropriate and in line with the Operation's Rules & Protocols), and to provide information about them which may be necessary to protect the property and personal safety of Members and their staff, customers etc. This data may be shared among Members and other agencies that have a legitimate interest.

b) Only West Midlands Police personnel can officially request the Offenders' name, date of birth, postal and email addresses, telephone number(s) and other contact details; the purpose of this processing is to enable the Operation to communicate with Offenders from time to time, for example to send warning letters, confirmation of exclusions, rules of the exclusion scheme, or confirmation that exclusions have expired. Such data will not be shared with Members except for the purposes of civil recovery or any legal proceedings.

c) Information and evidence about incidents in which an Offender has been involved; the purpose of this processing is to enable the Operation to authorise the issuing of Exclusion Notices, to inform Members of an offender's modus operandi, to collate intelligence on criminal activity within the area of the Operation's operation and to defend its legal rights against any claim or suit by an Offender or other party. Such data may be shared with Members.

9. For the purposes of identification, some sensitive or 'special category' personal data e.g. ethnicity may be processed by the Operation and for the safety and protection of our members, some medical conditions where the condition has symptoms that would render the Offender a danger to our Members. The dissemination of this information to our Members will not be widespread or general in nature but rather targeted to those most likely to be affected.

Sources of personal data

10. Offenders' personal data may be collected or provided to the Operation from:

a) Offenders who may voluntarily offer information about themselves;

b) Members who may submit reports about incidents in which Offenders have been involved. They may also send relevant 'intelligence' about Offenders, for example they may provide a name when asked to identify an unidentified image;

c) West Midlands Police or other public agencies may provide Offenders' personal data under a formal Information Sharing Agreement.

d) Social media platforms where such information is in the public realm by virtue of being displayed, without privacy controls, on a publicly accessible platform.

Recipients, or categories of recipients, of personal data

11. The following types of individuals may have access to the Operation's data, including the personal data of Offenders:

    a) Members who are property owners, agents or their employees working within the operational area of the Northfield BID area who share the same legitimate interests;

    b) Employees and officers of public agencies involved in the prevention and detection of crime, such as West Midlands Police, whose lawful basis for processing your data is their public task;

    c) Data Controllers of other organisations, similar to the Operation, in neighbouring areas if there is evidence that an Offender has participated, or is likely to participate, in any threat or damage to property, staff and customers in areas outside the Operation's area of operation.

12. The Operation will not transfer Offenders' data outside the UK.

Data retention period

13. When an Offender is reported by a Member for participating in any threat or damage to any Member's property, staff or customers, his/her name, date of birth and facial image together with any relevant information of offences or offending behaviour may be shared among Members for 12 months. If no further report is submitted during that period, the Offender's data will be withdrawn from Members at the expiry of that period. It will be retained for a further 12 months in the Operation's database (which can only be accessed by the Data Controller and authorised personnel) after which time, if no further incidents are reported, it will be irrevocably deleted.

14. If during the 12 months when an Offender's data is circulated among Members, he/she is reported for another incident involving a threat or damage to any Member's property, staff or customers, his/her name, date of birth and facial image will be circulated among Members for a further 12 months from the date of the second report. Additionally, the Offender may be excluded from all the properties of all or some Members for 12 months, and this fact will be shared with Members. If no further report is submitted by a Member during that period, the Offender's data will be withdrawn from Members at the expiry of that period. It will be retained for a further 12 months in the Operation's database (which can only be accessed by the Data Representative and authorised personnel) after which, if no further incidents are reported, it will be irrevocably deleted in the case of people under 16 years of age the above rules will apply but a period of six months will be used.

Offenders' rights

15. Every Offender has the right to obtain a copy of all the personal data which the Operation holds about him/her; to do so the Offender must contact the Data Controller (see contact details above). You may be required to provide proof of your identity to make sure we aren't giving your details

to someone else without your permission. The Operation will respond to the request within 30 days and provide full documentation in compliance with Data Protection law.

16. If, when an Offender accesses his/her personal data, any of it is deemed by the Offender to be incorrect, unnecessary or disproportionate, the Offender can require the Operation to correct it. Offenders do not have the right to require the Operation to delete correct, necessary or proportionate information.

17. Offenders have the right to complain about the Operation to the Information Commissioners Office; Offenders can submit a complaint on the ICO's website at https://ico.org.uk/concerns/handling/