



KINGSTON BUSINESS AGAINST CRIME

Working in Partnership

kingston**first**

action against ~~business~~ crime
by business - for business



KINGSTON BUSINESS AGAINST CRIME

PARTNERSHIP PROTOCOLS AND DOCUMENTATION PACK

KINGSTON BUSINESS AGAINST CRIME

INTRODUCTION

This partnership documentation is based on the Home Office 'COMMUNITY CRIME REDUCTION PARTNERSHIPS' guide. It is designed to enable local business crime reduction partnerships to be formally constituted to ensure legal requirements are satisfied, specifically in the area of handling personal data under the Data Protection Act, 1998.

The protocols and procedures contained in this guide have been extensively researched with the Office of the Information Commissioner and the Association of Chief Police Officers and have their agreement.

KINGSTON BUSINESS AGAINST CRIME

CONSTITUTION

CONSTITUTION

Contents

Subject	Reference
Partnership Title	1.0
Management of the Partnership	2.0
Aims & Objectives	3.0
Membership	4.0
Meetings	5.0
Voting	6.0
Administration	7.0
Funding, Financial Records & Auditing of Accounts	8.0
Banking Procedure	9.0
Process	10.0
Benefits	11.0
Liabilities	12.0

CONSTITUTION

1.0 Partnership Title

- 1.1 The partnership will be known as Kingston Business Against Crime. All references to 'the partnership' in this document refer to this partnership.

2.0 Management of the Partnership

- 2.1 The partnership will be representative of the participants and other interested parties, formally constituted and managed.
- 2.2 A steering committee will be appointed from the membership. The Royal Borough of Kingston upon Thames, Kingston police and representatives of other interested parties will be co-opted members of the Steering Group, as appropriate.
- 2.3 *The committee may include representatives from police, Crime and Disorder Partnership, local authority, town centre management, shopping centre management, local press (editor), chamber of trade/commerce, the business community (day and evening economy representatives), leisure sector and other relevant bodies or individuals, as required.*
- 2.4 The steering committee will oversee the aims and objectives of the partnership (see 3.0 below) and be responsible for compliance with its purpose and aims and objectives.

The role of the steering group will be to:

- Resolve misunderstandings and difficulties
 - Effect improvements
 - Assist generally with the smooth and efficient operation of the scheme
 - Decide the level and type of management information that is shared among participating members.
 - Decide on the method in which this management information is shared.
 - Set funding policy
 - Deal with matters relating to security and general management queries.
- 2.5 From within the membership of the steering committee, a board of management (BoM) will be appointed to guide, manage and advise on the day-to-day operation of the partnership which will report back to the steering group as necessary. The BoM will be made up of 4 members and will include a chairperson, vice chairperson, secretary and

treasurer. They will act as the first point of contact on issues relating to the scheme.

The BoM shall be elected at the annual general meeting from nominations received from the membership. Their period of office will be twelve months.

- 2.6 The BoM is the data controller for the partnership – see *Section 5 Data Integrity Agreement*
- 2.7 The BoM reports to and is accountable to the steering committee.
- 2.8 The BoM will be responsible for the financial, procedural, operational and disciplinary regulation of the partnership. Any alterations recommended by the BoM will be subject to approval by a majority vote of the steering committee.
- 2.9 The BoM will agree the annual charges for membership. This will be confirmed by the steering committee.
- 2.10 Voting for resolutions or appointments within the partnership shall be by majority vote. In the event of a tie, any resolution shall fail.
- 2.11 Representatives of the police and other organisations involved in the partnership will be entitled to attend the steering committee and BoM meetings in an advisory capacity and/or at the invitation of the committee members.
- 2.12 The BoM are empowered to ensure that all policies and procedures are fully complied with by each member.

3.0 Aims & Objectives

- 3.1 The legitimate (in accordance with the 8 principles of the Data Protection Act 1998) and lawful gathering, collation, processing, exchange and management of all relevant information relating to business crime and anti social behaviour between retail/business members of the partnership. The police contribution will be the legitimate and lawful provision and management of relevant photographs or other information as agreed.
- 3.2 To reduce and prevent criminality and anti-social behaviour by reducing the opportunity to commit crime.
- 3.3 To assist in the apprehension and prosecution of offenders and suspected offenders.
- 3.4 To reduce fear of crime and the effects of fear of crime.

- 3.5 To reduce members' losses caused by crime and anti social behaviour.
- 3.6 To create a "safe and secure" environment for customers, staff and visitors and to contribute to the economic viability and prosperity of the area.
- 3.7 To expand the partnership to encompass as wide a range of business sectors as possible.
- 3.8 To strengthen partnership working with the business community, police, local authority and other key agencies and organisations.
- 3.9 To establish the partnership as an integral part of the local community safety and crime reduction strategy and work in partnership with the police, local authority, and other agencies and organisations responsible for delivering the community safety action plan.

4.0 Membership

- 4.1 A member is defined as a business that has signed the agreements to abide by the operating protocols and data integrity agreements of the partnership to confirm that they have been made aware of their statutory obligations and responsibilities and has paid the relevant (initial and or annual renewal) membership subscription to the scheme.
- 4.2 Membership will be drawn from businesses, which trade in or in close proximity to the Kingston town centre and representatives of other interested parties, as appropriate.
- 4.3 Members must agree to comply with the protocols, aims and objectives of the partnership before membership is granted. Applications for membership will be agreed by the steering committee.
- 4.4 Payment will be in advance to the scheme account.
- 4.5 Refunds will not be permitted (unless in exceptional circumstances agreed by the BoM).
- 4.6 Members who are in breach of any code of conduct or other rules governing activities of the partnership shall be liable to disciplinary action by the BoM. This may take the form of warning, suspension or expulsion from the partnership.
- 4.7 All members who have access to personal data recorded by the partnership require to be made aware of the requirements of the 1998 Data Protection Act. The responsibility and potential liability for inappropriate disclosure rests with the individual.
- 4.8 Kingston Business Against Crime Board of Management reserves the right to refuse membership if it is deemed appropriate and reasonable

to do so. If the applicant does not fit the criteria for membership, the Board of Management has the right to decide not to disclose reasons for their decision.

See also Section 3, Codes of Practice

5.0 Meetings

- 5.1 An annual general meeting will be held at a date to be agreed. Other meetings held during the year as and when required. *See 2.2 above.*

6.0 Voting

- 6.1 Each member will have one vote at members' meetings. In the event of a tie, the chairman will have the casting vote.
- 6.2 A quorum for a meeting shall be not less than 10 members.

7.0 Administration

- 7.1 The secretary should prepare the agenda meetings after consultation. The members may propose items for inclusion on the agenda, which should be notified to the secretary in advance of the next meeting. Minutes of meetings will be taken and circulated.

8.0 Funding, Financial Records and Auditing of Accounts

- 8.1 There will be an administrative charge. The partnership should be self-financing and will be non-profit making.
- 8.2 Surpluses after payment of all costs will be carried forward and must only be used to achieve the objectives of the partnership.
- 8.3 The finances and financial records of the partnership will be audited and submitted to members at the AGM.
- 8.4. The BoM will be responsible for all monies, accounts and property of the partnership and will provide a financial statement of accounts to coincide with the meetings of the steering committee or as otherwise requested.

9.0 Banking Procedure

- 9.1 The partnership will operate a separate bank account. Members of the steering group and other authorised individuals can make credits to the account. Only the chairperson, vice chairperson, secretary and treasurer and those appointed members of the steering group will be signatories and authorised to make withdrawals. There must be two signatories for each withdrawal.

10.0 Process

- 10.1 The partnership office is located at: 3rd Floor, Neville House, 55 Eden Street. Kingston upon Thames, Surrey. KT1 1BW.
- 10.2 The partnership shall be managed by a person approved by the steering committee. His/her job title is Business Crime Co-ordinator
- 10.3 Additional staff may be appointed to assist with the management of the partnership, subject to prior agreement of the BoM and approval by the steering committee.
- 10.4 The partnership may be amended, extended or terminated by majority agreement of the members.
- 10.5 If the partnership is terminated, any monies should be reimbursed to members after all outstanding items have been taken into account.

11.0 Benefits

- 11.1 Members will be entitled to receive reports, photographs or other information concerning the activities of offenders whose activities affect their trading environment. The requirement being that the processed data must be relevant for the purpose (that is the prevention and detection of crime, disorder and anti social behaviour, to reduce the opportunity to commit crime, disorder and anti social behaviour and the apprehension and prosecution of offenders) and be lawful and legitimate.
- 11.2 Disclosure of partnership data must only be provided for under the Data Protection Act 1998 and only following assessment by the data controller. The decision to disclose will necessarily have to be on a case-by-case basis and should not be regarded as being available under an automatic authority. There is never an absolute entitlement to receive personal data, as each disclosure must have to be for the purpose (that is the prevention and detection of crime, disorder and anti social behaviour, to reduce the opportunity to commit crime, disorder and anti social behaviour and the apprehension and prosecution of offenders) and will be given only after consideration by the data controller in possession of the information.
- 11.3 Members must ensure that they put internal systems in place to enable them to identify target thieves and, where appropriate, to pass that information to the scheme.
- 11.4 The police will have proper access to data for the purposes of crime prevention or detection. Other third party disclosure will be within the terms of the data notification and the act itself.

- 11.5 De-personalised, anonymous or other information, which is not subject to the Data Protection Act 1998, may be released, where appropriate, from time to time to assist other crime reduction initiatives/agencies.

12.0 Liabilities

- 12.1 The partnership may withdraw the services it provides by giving 3 months notice of its intention.
- 12.2 Members may withdraw from the partnership subject to 3 months notice.

KINGSTON BUSINESS AGAINST CRIME

CODES OF PRACTICE

CODES OF PRACTICE

Contents

Subject	Reference
Introduction	1.0
Description of Partnership	2.0
Statement of Purpose	3.0
Partnership Discipline	4.0
Training	5.0
Staffing	6.0
Third Party Employees	7.0
Information Control/Compliance	8.0
Security/Audit	9.0
Disclosure of Information	10.0
Indemnity Insurance	11.0
Media Relations	12.0
Data Protection Principles	13.0
Data Protection Requirements	14.0
Subject Access	15.0
Complaints	16.0
Links to Other Partnerships	17.0
Acceptance Document	18.0

1.0 Introduction

- 1.1 This code of practice is to control the management, operation, compliance and use of data within the partnership.
- 1.2 This partnership document has been prepared following some advice from the Information Commissioner, police and other contributors to the legal process. It operates strictly within the provisions of the Data Protection Act, 1998.
- 1.3 The document will be subject to periodic reviews following consultation with all interested parties, to ensure it continues to reflect its stated purpose and remains in the public and participants interests.

2.0 Description of Partnership

- 2.1 The partnership is a pro-active crime reduction scheme between businesses, police, the local authority and other agencies and is directed at preventing and reducing criminal activity and anti social behaviour within Kingston town centre.
- 2.2 The members, whose representatives (signatories) have each signed a confidentiality agreement to agree to abide by the operating protocols of the partnership, are involved in the collation, analysis and the dissemination of information within the membership.

3.0 Statement of Purpose

- 3.1 The partnership will be operated fairly and in compliance with current legislation only for the stated aims and objectives for which it was established.
- 3.2 Each member of the partnership is and remains bound by the code of practice and other operating protocols and any subsequent amendments to them.
- 3.3 Persons considered for employment by the partnership must demonstrate an adequate knowledge of relevant legislation such as the Data Protection Act and the Police and Criminal Evidence Act.

4.0 Partnership Discipline

- 4.1 The partnership has specific responsibilities, which must be understood by all partners and their representatives.
- 4.2 The BoM is responsible for the approval of all members and the representatives of these members.

- 4.3 All rules on confidentiality and data protection must be subject to written agreement and must be strictly adhered to by the data controller, employees of the partnership and all members. Non-compliance of the Data Protection Act 1998 may lead to criminal prosecution and/or civil actions for damages.
- 4.4 Lesser infringements of procedure will nonetheless be subject to sanction by the steering group. This may be in the form of further training, verbal and written warnings or removal from the scheme.
- 4.5 Partnership employees will receive training to ensure that a good standard of knowledge is maintained.
- 4.6 Any persons employed or considered for employment by the partnership will be required to disclose prior convictions, if any, (and, if appointed, notify future convictions) in order that a judgement may be made relating to likely impact upon the integrity of partnership information. The steering committee will assess whether the offence has a bearing on the nature of the appointment or continued employment.
- 4.7 All persons employed or selected for employment may be required to satisfy the same conditions as would be imposed for employment by the police, and therefore a proper vetting process is required. This process must be fair and not excessive.
- 4.8 Information processed by the partnership which may prove relevant to pending or possible prosecution will be passed to the police in accordance with local reporting procedures or any conditions laid down by the Crown Prosecution Service.
- 4.9 The partnership manager or his nominated representative will be required to give witness statements to an agreed format, showing their involvement in the acquisition of such evidence. They may subsequently be required to attend court to give evidence in accordance with their involvement and the witness statement submitted.
- 4.10 When information is passed to a police officer the level and nature of response to the information will be decided by that officer. Where possible, the officer should have been advised of the terms of operation of the partnership and the agreed procedures relating to it.
- 4.11 Police will only disclose information to the local partnership where there is a clear legal basis to do so. Information provided under partnership arrangements by police is for the prevention and detection of crime and prosecution of offenders and must not be used for any other purpose.

- 4.12 The partnership Business Crime Co-ordinator is responsible for the day to day operation of the partnership and he/she must ensure that access to the partnership office and files/records is only permitted for authorised purposes and by authorised individuals. Police officers may attend in order to evaluate data and to add information or intelligence.

5.0 Training

- 5.1 In order to maintain high standards, a training programme for managers, employees and agents of participating businesses should be maintained to ensure that members are aware of the partnership procedures and their personal roles and responsibilities.
- 5.2 A nominated signatory within each business will liaise with the partnership manager as and when new employees are introduced.

6.0 Staffing

- 6.1 Numbers of staff employed by the partnership will be determined by the steering committee to meet operating requirements.
- 6.2 Matters relating to an employee's –
welfare, safety at work, performance/appraisal, general conditions of employment and working relationships will be the responsibility of the Board of Management.

7.0 Third Party Employees

- 7.1 Participating businesses may be represented by third party organisations such as guarding, store detectives or other out-sourced security services.
- 7.2 Disclosure of partnership data to such third party employees must only be as provided for under the Data Protection Act 1998 and only following assessment by the data controller. The decision to disclose will necessarily have to be on a case-by-case basis and should not be regarded as being available under an automatic authority.
- 7.3 The steering committee will retain the power of veto on third party organisations in appropriate circumstances.
- 7.4 Third party staffs, who are employed/contracted by members, must abide by the same constitution, codes of practice, operating guidelines and data protection agreements as members.

8.0 Information Control/Compliance

- 8.1 The information and intelligence held by the partnership is confidential. No disclosure of information will take place that is not in accordance

with the relevant statutory provisions. The data held may only be accessed and shared by scheme members which have signed the necessary agreements.

- 8.2 The partnership must be notified to the Information Commissioner as required under the Data Protection Act identifying the board of management as the data controller. *See also 14.0 below*

9.0 Security/Audit

- 9.1 All information received from participants will be assessed in terms of its intelligence value and will, if found to be of value, be held on the partnership database.
- 9.2 The partnership will maintain appropriate levels of security, in accordance with good practice and the requirements of legislation.
- 9.3 Members will maintain like standards of security in respect of all information in their care.
- 9.4 A secure cabinet/office must be used for the storage of all information. Upon application for membership, the Business Crime Co-ordinator or other nominated member of the steering committee will carry out an initial visit to the business premises to ascertain suitability for compliance with security and other relevant matters before partnership data is made available to that member.
- 9.5 Each member will appoint a representative/signatory to be responsible for the security of data disclosed and exchanged by the partnership, for ensuring that all security rules are applied and to facilitate any audits. However, the overall responsibility for compliance with the act by the partnership rests with the data controller.
- 9.6 The partnership and its individual members will submit to an annual inspection with a detailed audit report against the requirements and principles of Data Protection Act and partnership operation protocols. The results will be made available. The steering committee or other nominated representatives authorised on their behalf will be responsible for the audit process to ensure individual members maintain the appropriate standards of security and confidentiality.

No member will be allowed to conduct an audit of his or her own operation.

10.0 Disclosure of Information

- 10.1 Only staff, agents of members or other authorised persons will receive relevant information, providing that they do so where it is relevant for purpose.

11.0 Indemnity Insurance

- 11.1 The steering group must provide professional indemnity insurance for employees and officers of the partnership and public liability insurance as appropriate.
- 11.2 Members of the partnership should ensure that adequate insurance exists within their own organisations.

12.0 Media Relations

- 12.1 All media enquiries should be referred to a nominated person who will decide upon an appropriate response. Members should not seek to represent the partnership without consultation.

13.0 Data Protection Principles

- 13.1 Members must be aware of and comply with the data protection principles in the 1998 Data Protection Act. These principles state that:
 - 1. Personal data shall be processed fairly and lawfully.
 - 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
 - 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
 - 4. Personal data shall be accurate and, where necessary, kept up to date.
 - 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
 - 6. Personal data shall be processed in accordance with the rights of data subjects under this act.
 - 7. Data shall be kept secure. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
 - 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of

personal data.

- 13.2 Members of the partnership must be aware of these principles. Data controllers and processors should have a working knowledge of the relevant parts of the act.

14.0 Data Protection Requirements

- 14.1 The partnership must be notified to the Information Commissioner under the relevant provision of the Data Protection Act 1998. See 8.0 above

- 14.2 All staff who have access to personal data recorded by the partnership must be made aware of the following:

1. The information held within files or other documentation is confidential and must be used only for the purpose for which it was generated.
2. Any such information must not be disclosed to any third party who has not signed the necessary agreements.
3. The responsibility and potential liability for inappropriate disclosure rests with the data controller, signatories to the partnership agreements and/or individual participants.
4. Breaches of confidentiality by members or their representatives may also be subject to sanctions by the BoM.
5. Staff allowed access to the data must sign the data and information disclosure declaration to indicate that they have been advised of their statutory obligations and responsibilities.
6. All partnership information will be stored under secure conditions.
7. Target files will not be photocopied or otherwise reproduced unless expressly authorised by the manager.
8. Target files must only be destroyed at the partnership office.
9. If an individual makes a request to a member regarding data held on that individual that person should be referred to the manager.

- 14.3 The partnership procedures must be monitored periodically to ensure its efficient operation:

1. The steering group and/or any representatives authorised on their behalf will audit individual members at least once a year to ensure security and confidentiality. A record will be kept by the manager or nominated person of the audit, eg. date carried out and by whom. (See 9.0 above).
2. Any shortcomings identified must be rectified.

- 14.4 Any changes to nominated contacts/signatories within individual members' businesses must be communicated to the manager.

15.0 Subject Access

- 15.1 Complying with a request for access must be carried out in accordance with the Data Protection Act 1998. Data subject access rights must be protected and this responsibility lies with the data controller.
- 15.2 Where data subject access is requested, a fee may be charged in accordance with that permitted by law.
- 15.3 The data controller may not supply information unless a request in writing has been received and the identity of the person making the request has been established as the data subject.
- 15.4 If a data subject requests access to data held about them from any member, that member must refer the applicant to the data controller/manager. No data must be disclosed other than through the data controller.
- 15.5 The aim is to ensure that the request is complied with in accordance with the Act. The manager will consult disclosing members in order to assess what information it would be proper to disclose, taking into account the extent to which the application for data would likely prejudice either the prevention or detection of crime and the apprehension or prosecution of offenders. This will give the disclosing partner an opportunity to consider claiming an exemption under Section 29 of the Data Protection Act 1998.
- 15.6 The data controller must comply with a request promptly, before the prescribed period. The act defines the prescribed period to mean forty days from the day on which the data controller received the request for subject access.

16.0 Complaints

- 16.1 Complaints should be brought to the attention of the data controller. Any formal complaint by a data subject regarding any stage in the partnership process of disclosure of personal data should be notified in writing to the relevant partnership members and a decision made as to who will lead in responding to the complaint given the specific circumstances.

17.0 Links to Other Partnerships

- 17.1 If the partnership shares data with other partnerships, these partnerships must comply with the requirements of current data protection legislation.
- 17.2 The Safer Shopping Award (SSA) accreditation scheme confirms that a partnership has achieved a standard of operation and management of the partnership that meets the requirements of the Data Protection Act.

18.0 Acceptance Document

- 18.1 It is a condition of membership that each member (on behalf of his/her business) must sign the partnership acceptance document. *See also Constitution Section 4.0 above.*

KINGSTON BUSINESS AGAINST CRIME

OPERATING GUIDELINES

OPERATING GUIDELINES

Contents

Subject	Reference
Introduction	1.0
Target Photo File	2.0
Incident Details	3.0
Data Input/Analysis Procedure	4.0
Rationalisation of Files	5.0
Target Tracking	6.0
Management Information/Key Performance Indicators	7.0
Additional Security	8.0

1.0 Introduction

- 1.1 The aim of this operating guide is to provide a set of working procedures for the members of the partnership. It will be reviewed and updated as and when necessary following consultation.
- 1.2 The partnership office is located at the following postal address:

**Kingston Town Centre Management
3rd Floor
Neville House
55 Eden Street
Kingston upon Thames
Surrey
KT1 1BW**

TELEPHONE NUMBER: **020 8 547 2440**

EMAIL: **kbac@btconnect.com**

2.0 Target Photo File

2.1 Definition

The definition of a target is agreed locally and must comply with the data protection principles for storing and processing personal data.
(See Section 3, Codes of Practice and Section 5, Data Integrity Agreement).

2.2 Creation of the Target Photo File

Each member will survey their historical data to identify their most prolific offenders. This information will be submitted to the partnership business crime co-ordinator who will prioritise and determine how many offenders will be included in the target file. This will enable the first target file to be produced for circulation to the members for newly formed partnerships. Consultation with the police is important in this process.

Thereafter, as incidents occur and are submitted, the business crime co-ordinator will prioritise and focus on the most prolific offenders, again liaising with the police. This file will be updated and circulated accordingly.

2.3 Delivery of Target Photo File

The target photo file will be hand delivered to, or collected by, each participating member. A receipt signed by the nominated liaison contact will be necessary when the file is handed over.

2.4 Updating of Target Photo File

When existing targets are withdrawn for whatever reason the respective pages from the target file must be collected and returned to the business crime co-ordinator.

2.5 Use of Target Photo File :

- (i) The photo file must only be used for the purpose of preventing and detecting crime.
- (ii) The contents of the photo file must be treated as confidential by members and only to viewed by management, CCTV operators, store detectives, guards and other authorised staff who have signed the agreements contained in the partnership operating protocols.
- (iii) The photographs are for reference only and not for public or private display.

2.6 File Security

The target photo file is to be stored in a locked/secure office when not being viewed and at all times must remain away from the shop/sales floor.

In addition, members who are permitted to view photographs/data held centrally (in the partnership office) must sign a register stating purpose, business, name, day, date and time in/out (recording sheets will be circulated with files). The reproduction of target photo files is strictly prohibited unless authorised by the manager.

2.7 Destruction of Target Photo File

Target photo files will be securely destroyed by the manager or by members on his/her instructions. Police may also destroy target photos within agreed partnership protocols.

2.8 Audit Trail

Measures must be put in place to ensure that photograph distribution, use, and removal (including destruction) is recorded and held centrally in the partnership office. Signatures must be obtained at each stage:

- When police issue a photograph to the partnership (police sign out)
- When the partnership receive a photograph (partnership sign in)
- When the member receives a photograph (partnership signs out to a numbered file, member signs in)

- When a photograph is removed or destroyed (from person responsible depending on local procedure)

3.0 Incident Details

3.1 Definition of an Incident to be Reported

- Any crime or attempted crime against any member that falls within the scope of the partnership remit.
- Sightings of person(s) known or believed to be involved in offending behaviour.
- Any other relevant and appropriate information from within or near the area of operation as defined by the partnership.

3.2 Recording of Incidents

The partnership will complement member's current security practices. Therefore, all incidents involving targets or other incidents will be reported.

It is the responsibility of each member to report all incidents to the partnership in order to build the database, increase knowledge and be able to respond effectively. It is therefore important that incidents are reported as soon as possible to enable the partnership to respond appropriately.

3.3 Incident Reporting

Members **must** send information to the crime manager on the following incidents –

a) Theft and Attempted Theft

Person(s) arrested for theft or attempted theft

This includes:

- Incidents where the suspect escapes with merchandise without being apprehended.
- Person(s) involved in theft where property is subsequently abandoned in or outside the business premises.

b) Deception

Deception - e.g.

- Where a theft takes place and a suspect obtains or attempts to obtain a refund or exchange on those goods.
- Where the price of goods has been altered to reflect a lower price.
- The use of a counterfeit receipt to obtain a refund on stolen property.
- Counterfeit money used for the purchase of goods.

c) Cheque Card/Cheque Fraud

Person(s) involved in obtaining or attempting to obtain goods by the use of stolen or counterfeit cheques/credit cards.

d) Criminal Damage/Attempted Criminal Damage

Where a person is involved in causing or attempting to cause damage to goods, property or buildings.

e) Street Crime

Person(s) involved in theft, theft from person, robbery, violence and anti-social behaviour within the partnership area. These offences may take place inside or outside members' premises.

f) Sightings

Of person(s) known or believed to be involved in crime. They may not commit an offence but may be acting suspiciously.

g) Assaults or Insulting or Threatening Behaviour

Where a person:

Physically assaults a member of the public or staff

Verbally threatens a member of the public or staff

Intimidates a member of the public or staff.

h) Breach of an Exclusion Notice

Where an person has previously been served with a partnership exclusion notice or court order.

i) Breach of an Anti Social Behaviour Order (ASBO) or Acceptable Behaviour contract (ABC).

j) Breach of Bail Conditions

k) Any other appropriate incident

3.4 Arrest Procedure

If the target commits an offence and is arrested, he/she should be processed in accordance with the normal company procedures and the police contacted. In the case where the suspect is a target this information should be indicated to the reporting police officer. A

summary sheet outlining the incidents that the suspect has been involved can be supplied to the arresting police officer. The member will be required to prepare an incident report form to forward incident/offender details to the partnership business crime co-ordinator's office.

3.5 Communication

A regularly updated members' contact/signatory list must be maintained by the partnership business crime co-ordinator. It is the responsibility of each member to provide this information. Any changes to nominated contacts/signatories within individual members' businesses must be communicated to the business crime co-ordinator.

3.6 Video Evidence

Tapes should be retained in compliance with PACE codes of practice and the disclosure rules.

3.7 Data Accuracy

Incident details will be audited to ensure that all information remains current and accurate in order to satisfy the requirements of the Data Protection Act.

4.0 Data Input / Analysis Procedures

4.1 Data Definitions

- Data means information in a form that can be processed.
- Data equipment means equipment for processing.
- Data material means any document or other material used in connection with, or produced by, data equipment.
- Disclosure, in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data (but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties;) and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed. (Ref: 1998 Data Protection Act)

4.2 Storage of Data

All data/information received by the partnership will be stored on the Business Information Crime System (BICS) database in a secure office. Access to data/information will be logged in accordance with procedures. The management of data applies to both electronically held and manual data.

4.3 Input of Data

The business crime co-ordinator and anyone authorised by the steering committee will have responsibility for the inputting of all data onto the database. All data entries will be quality assured.

4.4 Confirmation of Receipt

A register will be kept to record the receipt of data/information. In cases where data/information has been circulated to a contact and no confirmation has been notified within 72 hours then confirmation will be sought by the partnership business crime co-ordinator. This time limit will also apply to recall requests for target photo files.

5.0 Rationalisation of Files

If a target has not been active within the agreed period (see Section 5 - Data Integrity Agreement), data in respect of him/her will be removed to a dormant file for a further limited period before deletion/destruction. This will not apply where a person is known to have been in prison or abroad over the relevant period.

6.0 Target Tracking

Whilst a major activity of the partnership is the use of intelligence-driven pro-activity against persons who engage in business and associated crime on an organised basis, an additional component will be the tracking of persons as they move through the criminal justice system.

7.0 Management Information/Key Performance Indicators

7.1 It will be necessary to establish key performance indicators (KPIs) to measure the operating success of the scheme and provide management information members and statistics for the scheme.

An important function of the partnership will be to identify what management information is required, the frequency it will be produced, and in what format.

The source of this information will, in the main, be from these key areas:

- Recorded crime statistics from the police.
- Information from the members regarding the impact their theft and loss performance. (NB. No individual member's information should be disclosed by name). Agreement should be reached as to how members' data would be disclosed.
- Management information from the BICS database (if installed).

- Other data, such as court results, re offending rates, deter at entry policy, outcomes from exclusion notice scheme and examples of good partnership working are good indicators.
- Visitor surveys, which measure customer satisfaction levels, are a good measure of fear of crime.

8.0 Additional Security

8.1 Procedures will be in place to ensure full compliance with data protection and other legal obligations. The following are examples of forms that can be used: -

- **Visitors Log.** Access to the partnership office will be controlled and all visitors will be logged in and out,. All visitors must sign on entry to the office acknowledging their acceptance of confidentiality of data and the reason for their visit.
- **Data and Information Disclosure Declaration.** This document is to be held by each member and be signed by each individual within that organisation who will receive information from and disclose information to the scheme.
- **File Movement Record.** This document will control the movement of files between the scheme office and each member.

KINGSTON BUSINESS AGAINST CRIME

DATA INTEGRITY AGREEMENT

Data Integrity Agreement
Confidentiality Agreement incorporating
Partnership Protocols.

1.0 The Data Protection Act 1998

- 1.1 The act regulates the use and handling of information (personal data) processed by computers and information held on manual records. It provides a framework by establishing data protection principles. The purpose of the Data Protection Act 1998 is to make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information. All processing must be in compliance with the provisions of the act and in the event of non-compliance the Information Commissioner may take enforcement action.
- 1.2 Particular obligations are placed upon the partnership, its members and the **data controller** and you as a member of the partnership must comply with the data protection principles.

2.0 Definition of Terms

- 2.1 The partnership is an initiative operated by businesses in partnership with police and other agencies and organisations, through an agreement with each of the members, who have agreed to the principles outlined in the protocols document, specifically, the constitution, code of practice, operating procedures, data integrity agreement and other agreed partnership procedures and protocols contained therein.
- 2.2 **Authorised Persons**
For the purpose of this agreement are the **signatories** to the agreement.
- 2.3 **Data Controller**
The board of management of the partnership is the **data controller** and is responsible for all matters concerning the management of the partnership. The BoM will determine the purposes for which, and the manner in which, any personal data are, or are to be, processed.
- 2.4 **Personal Data**
Data consisting of information, which relates to a living individual, who can be identified from that information.

2.5 **Data**

“Data” means information which –

- is being processed by means of equipment operating automatically in response to instructions given for that purpose.
- is recorded with the intention that it should be processed by means of such equipment.
- is recorded as part of a relevant filing system, or with intention that it should form part of a relevant filing system, or
- does not fall within paragraph a), b) or c) but forms part of an accessible record.

2.6 **Data Subject**

A living individual who is subject of **personal data**

2.7 **In or Near**

Is the area within which the partnership operates and is defined as the area within or near the geographic boundary of Kingston town centre.

2.8 **Disclosure of Information**

The **Data controller** will approve **disclosure** of **personal data** and information about **data subjects** to **signatories** of this agreement, where relevant and appropriate, for the purposes of:

- The prevention and detection of crime or:
- The apprehension or prosecution of offenders or suspected offenders

Information should only be passed where it is relevant to do so.

2.9 The **Data controller** will disclose **personal data** to **signatories**, where it is relevant to do so in connection with:

- Person(s) who are identified as legitimate “**targets**” under the partnership protocols or:
- Person(s) who are strongly believed to be in the **operating** area and in respect of whom there is clear evidence of their propensity to commit crime in the area.

2.10 **Data processor** means any person who processes the data on behalf of the data controller.

2.11 **Processing**, in relation to information or data, means obtaining, recording or holding information or data or carrying out any operation in relation to the information or data, including-

- organisation, adaptation or alteration of the information or data.
- retrieval, consultation or use of the information or data.

- disclosure of the information or data by transmission, or otherwise making available
- alignment, combination, blocking, erasure or destruction of the information or data.

3.0 Definition of a Target

- 3.1 For the purpose of this agreement a **target** means and includes:
- A person who is known (from a reliable source) to be currently, persistently and actively involved in committing or attempting to commit crime or disorder, **in or near** the area of operation. This will be the main criteria. In addition, a target will have a criminal record, e.g.
 - A person who has been convicted within the previous twelve months of any offence **in or near** the area of operation which may impact on the business environment. The conviction must be relevant and appropriate to the purpose (that is the prevention and detection of crime, disorder and anti-social behaviour and the apprehension and prosecution of offenders). This would not include parking offences and or other minor incidents which are not relevant.
 - A person who lives **in or near** the area of operation and who has been convicted within the previous twelve months of any crime which may impact on the business environment and whose activities or antecedents indicate that they are currently engaged in crime or are believed to be involved in crime. The conviction must be relevant and appropriate to the purpose (that is the prevention and detection of crime, disorder and anti-social behaviour and the apprehension and prosecution of offenders). This would not include parking offences and or other minor incidents which are not relevant.
 - A person who has been served with an exclusion notice preventing him/her from entering any member premises.
- 3.2 **Personal data** shall be periodically reviewed and shall not be retained for any longer than necessary. In particular **target** photographs and **target** information shall be reviewed every 3 months to ensure that the **data** reflects the **data subject's** current circumstances. **Personal data** shall not normally be retained for any longer than twelve months unless subject to review.

4.0 Data Security

- 4.1 **Data** shall not be **disclosed** to any non-signatory, either directly or indirectly unless required to do so by law or by the order or ruling of a court, tribunal or regulatory body. If required to do so, the member should notify the partnership manager promptly, prior to making such **disclosure**.

- 4.2 **Personal data** shall be transmitted to **authorised persons** through secure channels.
- 4.3 Appropriate security measures will be employed to prevent unauthorised access to, or alteration, disclosure, accidental loss or destruction of **personal data**. Such consequences may be seen as a breach of the **data protection principles** and may lead to further action.
- 4.4 **Personal data** relating to **targets** or other **data subjects** shall immediately be returned or destroyed when requested to do so in writing or otherwise.
- 4.5 **Personal data** relating to **targets** or other **data subjects** will be retained in accordance with the procedures outlined by the partnership protocols and documentation.

5.0 The Commitment

- 5.1 In consideration of the **personal data** being made available between the **data controller** and the **data signatories**, both parties undertake the following:
1. To keep the **data** received confidential at all times
 2. To obtain and process **data** and information fairly and lawfully
 3. **To** collate the **data** solely for the purposes of prevention and detection of crime, or the apprehension or prosecution of offenders
 4. **Data** held will consist solely of descriptions, habits, movement details, and criminal intelligence relating to **target** offenders and person(s) who are strongly suspected of committing crime, nuisance and/or disorder **in or near** the area of operation
 5. Police data will consist of the circulation of photographs or other information as agreed locally.
 6. **Data** held will relate to **target** offenders, current and past and person(s) who are strongly suspected of committing crime, nuisance and/or disorder **in or near** the area of operation.
 7. **Data** may be disclosed to police, prosecutors and courts
 8. **Data** shall be adequate, relevant, and not excessive for the purpose it is intended
 9. **Data** shall only be accessed or disclosed by or to **authorised persons**.

KINGSTON BUSINESS AGAINST CRIME

POLICE AGREEMENT FOR SHARING PHOTOGRAPHS

Photograph file protocol

The photograph file must be used only for the purpose of preventing and detecting crime, not maliciously or for any improper motive.

The folder and photographs/information will at all times when not in use be kept in a locked drawer in an area of the premises not accessible by general members of the public and authorised co-ordinators will be permitted to check the security of the folder and photograph / information.

The folder and photographs/information will be produced to a 'Metropolitan Police Service representative' or the 'Kingston Business Against Crime co-ordinator' on request and can be retained by either of these at any time.

Each participant to this scheme will nominate a specified employee to act as a liaison point and to be responsible for the security of the folder and photograph/information.

The nominated employee/representatives details will be provided to police to be checked against police records.

Any change of nominated employee/representative or manager should be notified to the co-ordinator immediately.

The authorised co-ordinator can without being required to provide reason request the company to change the nominated employee and the company will comply with this request.

Each participant in the scheme will sign and abide by these 'Codes of Practice' at all times.

The folder and photographs/information will only be shown to members of staff who have good reason to view them.

Any unauthorised disclosure of information could be liable to prosecution under the Data Protection Act.

Under no circumstances will any document in the folder be reproduced under any means.

The theft/ loss of a folder, photograph or information will be reported to the co-ordinator immediately.

Signed:

(PRINT NAME).....

Rank.....Date...../...../.....

(For and on behalf of Kingston Police)

Signed:.....

(PRINTNAME).....Date...../...../.....

(For and on behalf of Kingston Business Against Crime.)

KINGSTON BUSINESS AGAINST CRIME

EXCLUSION NOTICE SCHEME

Dear Member,

Welcome to the Kingston Business Against Crime exclusion notice scheme.

Please find attached the exclusion notice package, for your immediate attention. There is a need for a united approach in tackling business crime in the Royal Borough of Kingston upon Thames and this initiative has been established as part of the crime reduction strategy of the Kingston Business Against Crime partnership. This provides assistance to you and your business in the following areas:

- A collective approach in dealing with persistent and prolific offenders by excluding them from the member shops, stores and businesses.
- Protects staff from acts or the threat of physical violence and verbal abuse.
- Reduces the fear of crime in members' premises, for the benefit of staff, customers and the public.
- Frees up resources otherwise spent observing and apprehending prolific offenders.
- Encourages greater economic investment by creating and promoting a safer place to invest and work.

The scheme, which is supported by Kingston Police, is a civil agreement between you and other businesses within Kingston town centre, where you will collectively ban prolific offenders who may not have committed an offence in your premises. In joining, it must be stressed that for the scheme to be successful you must be prepared to eject an excluded person from your premises immediately and on every occasion they enter, despite the fact that the individual may not have committed an offence against your business. There will only be a relatively few offenders receiving the exclusion notice enabling the scheme to be manageable. It is important to note that these individuals will be responsible for a significantly high proportion of offending and anti social behaviour in the area.

By joining the Kingston Business Against Crime partnership you will be part of the exclusion notice scheme and be expected to support and enforce the scheme on the understanding that you will be challenged if you fail to do so.

Should you have any queries or need clarification on any aspect of the exclusion notice scheme, please contact the Kingston Business Against Crime co-ordinator.

1. Introduction

- 1.1 The scheme operates by utilising the business community as one voice thereby sending a strong message to those prolific offenders, who regularly intimidate and harass staff, by telling them that we know who they are and that they are not welcome in Kingston town centre.
- 1.2 Many of the offenders are well known to both businesses and police and cause a considerable drain on resources, with arrests sometimes leading to violence with the potential for injury to staff.
- 1.3 This has a detrimental effect on trade and the impact on peoples' perception of crime and the fear of crime is significant
- 1.4 The scheme will be run on a day-to-day basis by the partnership Co-ordinator and overseen by the board of management (BoM), or their nominated representatives, who are elected in accordance with the partnership constitution.
- 1.5 In addition to administering the scheme, the Co-ordinator and BoM will be responsible for liaising with members and outside agencies and organisations.

Exclusion notice schemes are an effective means of managing offenders, ensuring that they are deterred from committing crime.

We will provide window stickers advertising your commitment and inclusion in the scheme and notes for your information and guidance.

2. Objectives

2.1 These are:

- To exclude persistent and prolific offenders from members' premises.
- To reduce the opportunity for crime and anti social behaviour to take place.
- To protect staff from acts of physical violence and verbal abuse.
- To reduce the incidents of crime and the fear of crime for the benefit of staff, customers and the public.
- To improve the economic and general environment of Kingston town centre, improving prosperity within the area and helping to protect and create employment.
- To encourage greater economic investment by creating and promoting a safer place to invest and work.

3. What is an Exclusion Notice?

- 3.1 There is a presumed invitation by businesses, which allows members of the public to enter their premises and either view or buy merchandise on display.
- 3.2 The issue of an exclusion notice withdraws that invitation to the person issued with the exclusion notice.
- 3.3 This scheme only applies to those businesses that are members of Kingston Business Against Crime and have confirmed their involvement in the scheme and have signed the relevant partnership protocols and agreements.
- 3.4 Some businesses already operate similar notices, but only in relation to their own businesses.
- 3.5 This scheme allows the partnership to issue exclusion notices on behalf of the members, excluding offenders from the premises and of all members of the Kingston Business Against Crime.

4. How will it work?

4.1 Criteria for the issue of an exclusion notice

- 4.1.1 Individuals receiving an exclusion notice will normally be known as prolific offenders. Circumstances leading to the issue of an exclusion notice will vary, for example, where an individual commits an offence that requires an immediate and appropriate response or where the number of documented incidents reported to the partnership manager suggests that an individual's behaviour has reached the stage where an exclusion notice is appropriate. Reported incidents will relate to, for example:
 - Theft Act offences,
 - Possession of controlled substances,
 - Public Order offences,
 - Criminal damage,
 - Possession of offensive weapons
 - Assault
 - Anti social behaviour
- 4.1.2 It may also be the case that an individual has a case pending which may lead to a conviction in the near future. In these circumstances the partnership manager will consult with the police and the partnership before a decision is made to proceed. Due consideration must be given to all the circumstances involved to ensure the decision to proceed is fair and appropriate.
- 4.1.3 The issue of an exclusion notice is not dependent on a previous criminal conviction/caution or anti social behaviour order.

4.1.4 Therefore, subject to Human Rights considerations, and having regard for all the circumstances of the offending behaviour/ documented activity, consideration to issue an exclusion notice will be made, for example, as follows:

a) Adults

1. Where an suspect is arrested and subsequently prosecuted or cautioned. A caution may be counted as a conviction as the suspect will have admitted the offence.
2. Where an individual is arrested and bailed by the police to conduct further enquiries into offences against member/s premises and the circumstances of the case/s suggest that the alleged offences were of such a nature that an exclusion notice is appropriate.
3. Where the number of documented incidents or the gravity of the offending reported to the partnership manager suggests that an individual behaviour has reached the stage where an exclusion notice is an appropriate response.
4. A person subject of an exclusion order from the courts under the Licensed Premises (Exclusion of Certain Persons) Act 1980.

or a combination of the above circumstances.

b) Juveniles -

1. Where a decision is made to prosecute an juvenile or deal with by way of a 1st reprimand or final warning the offence committed.
2. Where an individual is arrested and bailed by the police to conduct further enquiries into offences against member/s premises and the circumstances of the case/s suggest that the alleged offences were of such a nature that an exclusion notice is appropriate.
3. Where the number of documented incidents or the gravity of the offending reported to the partnership manager suggests that an individual behaviour has reached the stage where an exclusion notice is an appropriate response.

or a combination of the above circumstances.

4.2 Exclusion Notice procedures

- 4.2.1 The members must complete incident reports, as required, to be submitted to the Business Crime Co-ordinator for inclusion on the database as normal practice. From this information individuals will be identified who meet the criteria as outlined in 4.1 above.
- 4.2.2 A decision will be taken by the partnership crime manager in liaison with the police whether the circumstances satisfy including the person in the exclusion notice scheme. The decision to proceed will be ratified by the BoM who will keep a record of their decision and reasons for that decision.
- 4.2.3 The partnership Co-ordinator will be responsible for serving the exclusion notice:
 - a) by recorded delivery to the person's home address, or
 - b) given personally, directly to the individual concerned and circulating the details to the members.
- 4.2.4 A certified copy of service of the exclusion notice will be retained by the partnership Co-ordinator. A further copy will be forwarded to, and retained by, police.
- 4.2.5 The police officer(s) in the case will liaise with the criminal justice unit (CJU) to monitor the progress of any prosecution. Alternatively, the Co-ordinator will liaise with the magistrate's court office to monitor the progress of the prosecution and to establish the result of the court proceedings.
- 4.2.6 The result of any court proceedings will be notified to the partnership Co-ordinator and at that point the exclusion notice will be re-evaluated to ensure that it is still appropriate.
- 4.2.7 The police will be responsible for updating the relevant PNC record with details of the exclusion notice ensuring that PNC national guidelines are complied with.

4.3 What action should members follow?

- 4.3.1 When a person is known to have previously been served an exclusion notice and is recognised inside a members' premises (and not thought to have committed an offence at that stage), that person should be immediately asked to leave the premises as they are regarded as a trespasser.
- 4.3.2 The person will be informed that all other members of the scheme will be notified of their presence and if they attempt to enter, they will also be requested to leave those premises.

The fact that a person, subject of an exclusion notice, has been ejected from a members premises should then be communicated over the radio link system to all other members informing them that an excluded person (identify him or her by the reference relating to the individual concerned) is in the locality, giving a brief description of clothing and direction of travel.

- 4.3.3 The existence of an exclusion notice does not confer any additional powers for eviction and current procedures for removing unwanted persons as trespassers should continue to be exercised. (The offence is civil trespass and should the member wish to pursue a complaint, they should do this through the civil courts).
- 4.3.4 If an excluded person is suspected of committing any offence within a member's premises, Police should be called. When an offender has been previously issued with an exclusion notice and that person is arrested committing another offence, the fact that they have been previously issued with an exclusion notice will be included in the evidence.
- 4.3.5 If an excluded person is subsequently charged with the offence, the partnership co-ordinator will arrange for a certified copy of the exclusion notice to be included on the prosecution file for the information of the Crown Prosecution Service (CPS).
- 4.3.6 The CPS have agreed that provided the required evidential procedures have been followed, they will inform the court of the existence of the exclusion notice, at the point of conviction, as antecedents.
- 4.3.7 The chair of the justices and the clerk to the magistrates court have been acquainted with the objectives of the scheme. They have indicated that if an excluded person is convicted of another offence against any partnership member, the existence of an exclusion notice will be considered as an aggravating fact and would be reflected in the sentence imposed by the court.
- 4.3.8 The local press will be informed by the partnership of the existence of the exclusion notice and the identity of the excluded person for publication.

5. Possible exceptions to the issue of an exclusion notice

Examples might be:

- a) When the decision is for a store caution. (Unless there is a recent history of repeat offending). The BoM will make the final decision.
- b) When the incident involves elderly or confused persons.
- c) Where, in the case of a juvenile, further police investigations lead to a decision not to prosecute. In this case, police may make a recommendation to the partnership to withdraw the exclusion notice.
- d) For first offences, depending upon the severity of the offences

Where a decision is made not to issue a partnership exclusion notice, the member still maintains the right to issue a ban in respect of their individual premises, which shall not form part of this scheme.

6. Time limits for exclusion notices

Exclusion notices must include a time limit, which will normally be twelve months, but may be extended as set out below.

Immediately prior to any exclusion notice becoming time-lapsed, the partnership will review each notice and determine whether or not the notice should lapse or be extended. Reasons for extending the period rests with the BoM and a record kept and reasons recorded.

Circumstances for extension of an exclusion notice will be either further evidence of re-offending (of relevant offences) within Kingston town centre or a decision by the partnership, after consideration of any further information, which may be provided by partnership members.

Where an exclusion notice has been extended the offender will be notified together with the reasons, and the information circulated to all members.

The partnership may consider the early lifting of the order where exceptional circumstances prevail and the offender requests the lifting of the order in writing, giving reasons for the same.

7. Distribution of exclusion notice copies

Exclusion notice documentation should be produced in triplicate (by photocopy, if necessary), signed by the recipient if possible, with copies as follows: -

- | | |
|--------|--|
| Copy 1 | To be forwarded (or handed) to the person receiving the exclusion notice
<i>(If forwarded, this should be sent by recorded delivery to the offender and the receipt slip retained with the indexed copy)</i>

A copy of the partnership exclusion notice window sticker must be shown to the individual when he or she receives their copy of the exclusion notice so that the individual recognises those businesses that are members of the scheme. |
| Copy 2 | To be handed to the police for inclusion in the arrest file. Details of the issue of the exclusion notice require being included in the statement of evidence provided for the offence. |
| Copy 3 | To be held in the Kingston Business Against Crime office by the partnership Co-ordinator, in order that updated lists can be distributed to the membership on a regular basis. |

KINGSTON BUSINESS AGAINST CRIME

CONTENTS

Action 1	KBAC1	Joining Pack – Contents
Action 1	KBAC2	Application For Membership
Action 1	KBAC3	Partnership Acceptance Document
Action 1	KBAC4	Data protection & Telecoms Authorisation
Action 2	KBAC5	Data Protection Audit Report
Action 3	KBAC6	Radio Link System Agreement
Action 3	KBAC7	Data Integrity Agreement
Action 3	KBAC8	Target Files Codes Of Practice
Office	KBAC9	File Movement Record – In File
Office	KBAC10	File Movement Record – Out File
Office	KBAC11	Data Disclosure – Visitors Log
Office	KBAC12	Data & Information Disclosure Declaration
	KBAC13	BoM Exclusion Notice Decision Form
	KBAC14	Schedule of Excluded Premises
	KBAC15	Schedule of Excluded Persons
	KBAC16	Exclusion Notice
	KBAC17	BoM Subjects Appeal Form
	KBAC18	BoM Exclusion Notice Appeal Form
	KBAC19	Management Board
	KBAC20	Radio Training Leaflet
	KBAC22	Incident Reporting Log

KINGSTON BUSINESS AGAINST CRIME

Contents List Of Joining Pack

Application Form – Return

Partnership Protocols and Documentation Pack

Partnership Acceptance Form – Return

Data Integrity Agreement - Return

Data Protection Act and Telecoms Form – Return

Radio System Agreement – Return

SERVICOM Agreement Forms - Return

KBAC1

Application for Membership

KINGSTON BUSINESS AGAINST CRIME

(A) DETAILS OF PROPOSED BUSINESS MEMBER	(B) CORRESPONDENCE DETAILS IF DIFFERENT TO (A)
<u>Name of Organisation</u>	<u>Name of Organisation</u>
<u>Business Description</u>	
Address	Address
Post Code	Post Code
Name of Nominated KBAC Contact at this Address:	Name of Contact at this Address:
Position	Position
Phone/Fax	Phone/Fax
Mobile	Mobile
E-mail	E-mail

Signed	Name	Date
--------	------	------

Kingston Business Against Crime office use:

Approved by:	
Date:	
Signed partnership participation acceptance documentation	
Radio Link member	Yes or No
Full or Associate membership required	Please State

Please return to Business Crime Co-ordinator, Kingston Business Against Crime, Neville House, 55, Eden Street, Kingston upon Thames Surrey KT1 1BW

KINGSTON BUSINESS AGAINST CRIME

PARTNERSHIP ACCEPTANCE DOCUMENT

I have read and understood the Constitution, Codes of Practice, Operating Guidelines, Data Integrity Agreement and all other documentation relating to the operating protocols of the partnership.

I agree to operate within the conditions, policies and procedures contained therein.

I acknowledge my personal responsibility and liability with regard to membership of this partnership.

Signed

(PRINT NAME)

On behalf of

.....

.....

Date

Signed

(PRINT NAME)

On behalf of

.....

.....

Date

KINGSTON BUSINESS AGAINST CRIME

Data Protection and Telecommunications Act Authorisation Form

Please complete the details required below which will also act as a mail/check list of current information held for Crime Reduction Partnership purposes.

BUSINESS NAME.....

MANAGER/PROPRIETOR.....

ADDRESS.....

.

POSTCODE.....**Tel No**.....**Fax No**.....

E-MAIL ADDRESS.....

Authorisation

I, the undersigned, give Kingston Business Against Crime and Kingston Police the authority to place my personal details as stated above on their database. I understand my rights are protected and that this information will not be used for any other purpose other than the Kingston Business Against Crime partnership.

Signed.....**Date**.....

KINGSTON BUSINESS AGAINST CRIME

RADIO SYSTEM AGREEMENT

Agreement made between **KINGSTON BUSINESS AGAINST CRIME** partnership and:

Name:.....
Address:.....
.....
.....Post Code.....

1. Radio link is established for the purpose of improving the quality of communications and co-operation between members, to assist in the safety of persons, the security of property and to facilitate the prevention, intervention and detection of crime and disorder.
2. The radio link system is a partnership using two radio channels made up from members of **KINGSTON BUSINESS AGAINST CRIME, PUB WATCH** and other appropriate agencies, organisations, bodies and individuals.
3. All members must be approved by the board of management.
4. All members must comply with the rules of **KBAC**. Failure to comply may result in a member being removed from the partnership.
5. All members will agree to undertake training in the correct operation of radios.
6. All members will sign for and receive a copy of the membership radio link agreement.
7. **KBAC** reserves the right to amend this agreement. Members will be notified of any change and will be requested to sign a new or amended agreement.
8. All members are to ensure that their staff are made aware of the radio link operating procedures.

Signed.....Print Name.....
Position.....
Address (if different from above).....
.....Post Code.....

KINGSTON BUSINESS AGAINST CRIME

Data Integrity Agreement

Any breach of this agreement will be dealt within accordance with the disciplinary procedures outlined in the Kingston Business Against Crime partnership protocols and documentation. Making an unauthorised disclosure of data may lead to criminal prosecution.

I/we confirm and understand our responsibility to manage personal data according to the 9 Principles of Data Protection and the above protocols.

1. To keep the **data** received confidential at all times
2. To obtain and process **data** and information fairly and lawfully
3. **To** collate the **data** solely for the purposes of prevention and detection of crime, or the apprehension or prosecution of offenders
4. **Data** held will consist solely of descriptions, habits, movement details, and criminal intelligence relating to **target** offenders and person(s) who are strongly suspected of committing crime, nuisance and/or disorder **in or near** the area of operation
5. Police data will consist of the circulation of photographs or other information as agreed locally.
6. **Data** held will relate to **target** offenders, current and past and person(s) who are strongly suspected of committing crime, nuisance and/or disorder **in or near** the area of operation.
7. **Data** may be disclosed to police, prosecutors and courts
8. **Data** shall be adequate, relevant, and not excessive for the purpose it is intended
9. **Data** shall only be accessed or disclosed by or to **authorised persons**

Signed:

(PRINT NAME).....

Company.....(POSITION).....Date.....
(For and on behalf of the member)

Signed:.....

(PRINTNAME).....Date.....

(For and on behalf of)