CAMBRIDGE BUSINESS AGAINST CRIME

CODES OF PRACTICE

1.0 Introduction

1.1 This code of practice is to control the management, operation, compliance and use of data within the partnership.
It should be read in conjunction with the Additional Reference Material available from Action Against Business Crime, specifically Section 2, Data Protection.

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 review 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 proactive 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 the City of Cambridge.

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 group 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 manager is responsible for the 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.

5.1 A nominated signatory within each business will liase 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 group 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 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 group will retain the power of veto on third party organisations in appropriate circumstances.

7.4 Third party staff, 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 must be used for the storage of all information. Upon application for membership, the Business Crime Manager 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 group 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 premises.

(An example of an Audit document is shown in Appendix B).

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. *(See Additional Reference Material, Section 3, Indemnity Insurance).*

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)*
The partnership must ensure that the Information Commissioner is notified of the correct purposes under which it will be processing and holding personal data and that these purposes are included in the registered entry report which will be received from the Information Commissioner to confirm notification.

The partnership should register (at least) the following three core purposes:

1. *Crime prevention and prosecution of offenders*
2. *Accounts and records*
3. *Administration of membership records*

It is important to ensure that the partnership does not hold data, which it is not registered to hold. The partnership may add additional purposes in its registration, depending on what additional information is held. Guidance should be sought from the Information Commissioner if necessary to clarify individual needs.

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 *(see Section 4, Operating Guidelines -Appendix C)* 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. *(See Section 15.0 Subject Access below).*

14.3 The partnership procedures must be monitored periodically to ensure 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 to 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 Business Award (SBA) accreditation scheme confirms that a partnership has achieved a standard of operation and management of the partnership, which meets the requirements of the Data Protection Act.

Partnerships are strongly advised that they should only consider exchanging data with approved SSA or SBA accredited schemes. Details of accredited schemes may be obtained from Action Against Business Crime – Tel: 020 7854 8956.

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).*
(see appendix A).

APPENDIX A

CAMBRIDGE 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.

Any breach of this agreement will be dealt within accordance to the disciplinary procedures outlined in the partnership protocols and documentation.

Making an unauthorised disclosure of data may lead to criminal prosecution.

Signed ……...

(PRINT NAME) ……..

On behalf of ……...

……...

. ……..

Date ……

Signed . ……..

(PRINT NAME) . ……

On behalf of . ……..

. ……..

. ……..

Date . ……..

APPENDIX B

CAMBAC DATA PROTECTION AUDIT REPORT

Name of Business:…… **Date of report:**…….

Audit carried out by: (signature)……
(print)……

Subject	Requirement	Comments/recommendations
Is the partnership data held manually, electronically on a computer or both?		
Is the partnership data held in a secure room with a lockable entry door to the office?		
Are the hard copy files and other documents that may include personal sensitive data stored in lockable cabinets?		
Are the files clearly labelled?		
Any photographic stills on display?		
If photographic stills are on display can they be covered, if any unauthorised person is in the office?		
Is there a system for visitors to sign in when they enter the partnership		

office where the data is held? Is there documented evidence of this?		
Are the files/data up to date and in order? Is there a procedure for reviewing data to ensure it is up to date and relevant? Are there any files/data that have been recalled? If so, give reasons.		
Is the signatories list up to date? Are the signatories and other key staff aware of their Data Protection responsibilities		

General Observations	Comments