CODE OF PRACTICE

Contents

1.0 Introduction

1.1 This code of practice is to control the management, operation, compliance and use of data within City Safe, which operates strictly within the provisions of the Data Protection Act, 2018 and GDPR 2018.

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 City Safe

2.1 City Safe is a proactive crime reduction scheme (a part of Retail Birmingham Ltd) and is a partnership between businesses, police, the local authority and other relevant agencies and is directed at preventing and reducing criminal activity and anti- social behaviour within Birmingham.

2.2 The members have each signed a confidentiality agreement to agree to abide by the operating protocols of City Safe and are involved in the collation, analysis and the dissemination of information within the membership through the end user agreement with SentrySIS as the data distributor.

3.0 Statement of Purpose

3.1.1 City Safe 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 City Safe is and remains bound by the code of practice and other operating protocols and any subsequent amendments to them.

4.0 City Safe Discipline

4.1 City Safe has specific responsibilities, which must be understood by all partners and their representatives.

4.2 City Safe is responsible for the approval of all City Safe members.

4.3 All rules on confidentiality and data protection are be subject to written agreement and must be strictly adhered to by the data controller, employees of City Safe and all members. Non-compliance of the Data Protection Act 2018 and GDPR 2018 may lead to criminal prosecution and/or civil actions for damages.

4.4 Lesser infringements by members of procedures will nonetheless be subject to sanction by City Safe. This may be in the form of further training, verbal and written warnings or removal from the scheme.

4.5 City Safe employees will receive training to ensure that a good standard of knowledge is maintained.

4.6 Any persons employed or considered for employment by City Safe 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 information. The BID manager and the steering group will assess whether the offence has a bearing on the nature of the appointment or continued employment.

4.7 Information processed by City Safe 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.

4.8 City Safe operatives may 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.

4.9 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 City Safe and the agreed procedures relating to it.

4.11 Police will only disclose information to City Safe where there is a clear legal basis to do so. Information provided under City Safe and ISA 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 City Safe is responsible for the operation of City Safe and must ensure that access to the City Safe office and files/records is only permitted for authorised purposes and by authorised individuals. Police officers and other legislative agencies 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 will be maintained to ensure that members are aware of the City Safe procedures and their personal roles and responsibilities.

5.2 Each business must liaise with City Safe as and when new employees or its membership representative(s) are required to change.

6.0 Staffing

6.1 Numbers of staff employed by the City Safe will be determined by the Retail BID board and the steering committee informed in order 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 BID and Line managers

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 current Data Protection Acts and only following assessment by the City Safe. 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 City Safe 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 City Safe must be notified to the Information Commissioner as required under the Data Protection legislation

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 City Safe database.

9.2 City Safe 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 is be used for the storage of written/paper information. Upon application for membership, the City Safe representative will carry out an initial visit to the business premises to ascertain suitability for compliance with security and other relevant matters before City Safe data is made available to that member.

9.4 Each member will be validated at sign up and will have responsibility for the data disclosed and exchanged by City Safe and for ensuring that all security rules are applied.

9.5 City Safe will submit to an annual inspection with a detailed audit report against the requirements and principles of current Data Protection legislation and City Safe operation protocols. The results will be made available. The Business Manager 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.

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 Professional indemnity insurance is provided for employees and officers of City Safe and public liability insurance as appropriate.

11.2 Members of City Safe should ensure that adequate insurance exists within their own organisations.

12.0 Media Relations

12.1 All media enquiries should be referred to City Safe in the first instance or t who will decide upon an appropriate response. Members should not seek to represent City Safe without consultation.

13.0 Data Protection Principles

13.1 Members must be aware of and comply with the data protection principles in the 2018 Data Protection Act and GDPR 2018. These principles state that data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

13.2 Members of City Safe 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 City Safe must be notified to the Information Commissioner under the relevant provision of the Data Protection Act 2018 and GDPR 2018. *(See 8.0 above)*

14.2 All staff who have access to personal data recorded by City Safe 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 person/authority/organisation that has not signed the necessary agreements.
3. The responsibility and potential liability for inappropriate disclosure rests with the data controller, signatories to the City Safe agreements and/or individual participants.
4. Breaches of confidentiality by members or their representatives may also be subject to sanctions by the Business Manager.
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 City Safe information will be stored under secure conditions.
7. Files will not be photocopied or otherwise reproduced unless expressly authorised by the manager.
8. 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 City Safe procedures must be monitored periodically to ensure efficient operation:

1. The Business Manager 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.
2. Any shortcomings identified must be rectified.

14.2.1 Any changes to nominated contacts/signatories within individual members' businesses must be communicated to City Safe

15.0 Subject Access

15.1 Complying with a request for access must be carried out in accordance with the Data Protection Act and GDPR 2018. Data subject access rights must be protected and this responsibility lies with the data controller.

15.2 Where data subject access is requested, if applicable a response will be delivered within 1 month from receipt of the request.

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 or disorder 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. (Updated DP 2018 and GDPR)

15.6 The data controller must comply with a request promptly, before the prescribed period. The act defines the prescribed period to mean one month from the day on which the data controller received the request for subject access.

16.0 Complaints

16.1 Any formal complaint by a data subject regarding any stage in the City Safe process of disclosure of personal data should be notified in writing to the BUSINESS MANAGER.

17.0 Links to Other partnerships

17.1 City Safe will only share data with other partnerships, which are either accredited organisations or competent authorities compliant with the requirements of current data protection legislation.

17.2 City safe is following a programme of accreditation to achieve and maintain national standards with required protocols

18.0 Acceptance Document

18.1 It is a condition of membership that each member (on behalf of his/her business) must agree the City Safe acceptance documentation which will be presented at sign up. Membership will only then be obtained on evidence of this and passwords issued to the member allowing access to the SentrySIS data dissemination software platform.