

# **Data Protection Policy**

Reviewed September 2007

# Data Protection Policy

## SAFETY NET ASSOCIATES LIMITED ("SNA") DATA PROTECTION POLICY (the "Policy")

### PART I

## SNA STATEMENT ON DATA PROTECTION AND EMPLOYEES

SNA is committed to using all reasonable endeavours to ensure compliance with the requirements of the Data Protection Act 1998 (the " **DPA** "). Consequently, SNA requires you to be aware of the purposes for which SNA will process your personal information ( **Part 1 of this Policy** ) and the obligations that both SNA and its employees are under when processing personal data. ( **Part II of this Policy** ).

#### 1. Definitions

For the purpose of understanding this Policy, the following definitions have the following meanings:-

**1.1 "personal data"** is defined in Section 1, Part 1 of the DPA and includes any information from which a living individual can be identified, either on its own or together with other information which is or is likely to come into the possession of SNA. This definition also covers expressions of opinion about individuals and indications of the intentions of SNA or any other person in respect of individuals.

Therefore, personal data includes information such as telephone numbers, names, addresses (including e-mail addresses), sound and image data (for example photographs and voice recordings), indications of status and title as well as remarks about individuals - if the identity of the individual can be ascertained from such information.

**1.2 "sensitive personal data"** is defined in Section 2, Part 1 of the DPA and includes information relating to racial or ethnic origin, political opinions, religious beliefs or

beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, information relating to any proceedings for offences committed or allegedly committed by data subjects.

**1.3 "processing"** is defined in Section 1, Part 1 of the DPA and means obtaining, recording, or holding data or carrying out any operation or set of operations on the data including: organisation, adaptation or alteration of the information or data; or retrieval, consultation or use of the information or data; or disclosure of the information or data by transmission, dissemination or otherwise making available; or alignment, blocking, erasure or destruction of the information or data.

For the purposes of the DPA, personal data will be caught by the DPA, if it is processed in:

i. an automated fashion (for example: by main frame computers, PCs, word-processors, electronic memory typewriters, electronic mail (e-mail) or filing systems, laptops, computer hardware, computer software and Internet accounts); and/or

ii. a manual fashion, which includes a set of information relating to individuals which is structured according to criteria which allows easy access to specific personal data (for example: card indices or manual files of client, employee or supplier data which is stored in a structured fashion).

**1.4 "data subject"** means the individual who is the subject of personal data, which is being processed by SNA (for example: clients, employees, supporters, recruits and suppliers of SNA).

**1.5 "Information Commissioner"** means the UK Information Commissioner responsible for implementing and overseeing the DPA.

## **2. Processing of Employee Data by SNA**

**2.1** As specified in your Statement of Written Particulars SNA may, from time to time, process personal data about you for the following purposes:-

a. **Statement of Written Particulars** - for completing and updating your Statement of Written Particulars in relation to your employment with SNA and your Terms and Conditions of Service and generally for the administration and management of your employment with SNA and/or SNA's business.

b. **Payroll Pension and Accounts** - for calculating and paying employee remuneration and pensions and accounts relating to the activities of SNA.

c. **Back-up** - to ensure the security and accuracy of the data processed by SNA.

d. **Business Development** - this may include the disclosure of certain information contained in your personal data to potential or existing clients, customers, partners, contractors, suppliers and/or fellow employees (including your name, title and office contact details) for the purposes of marketing or other business related activities of SNA and/or ensuring client, customer, supplier and employee satisfaction or otherwise for the promotion and/or development of SNA's business. Such personal data may be disclosed in written, electronic or other form including on an SNA Extranet or a third party Extranet to which SNA has access for the purposes described above.

f. **Employee Administration and Management** - this may include sensitive personal data about you where this is necessary to comply with legislation and/or your Statement of Written Particulars and/or Terms and Conditions of Service and/or SNA employee administration policies. Examples of purposes for which personal data relating to you may be processed in the administration, management and carrying out of your employment include (but are not limited to):-

- Recruitment activities;
- Administration of absence records, including sick leave and sick pay, monitoring sickness absences and attendance and manpower planning;
- Administration and maintenance of personnel records, payroll and other benefits;
- Administration of holiday and other absence records such as maternity leave, parental leave, paternity leave and time off;
- Equal opportunities matters including the operation of the Equal Opportunities Policy;
- Carrying out performance appraisals and development reviews;
- Disclosure to prospective employers;
- The pursuit of disciplinary and grievance matters;
- Recording the commission or alleged commission of any offence;

- The provision of information to any government body or agency for legitimate purposes including social security and income tax.

g. **Prevention and Detection of Crime** - this may include information relating to offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed for the purpose of the prevention and/or detection of crime.

h. **Monitoring and Promotion of Equal Opportunities and Trade Union Membership** - this may involve sensitive data about you, such as religious beliefs or similar beliefs, ethnic origin and trade union membership.

i. **Corporate Finance, Mergers and Acquisitions** - this may include the disclosure of certain personal information about you to other individuals and organisations with whom SNA may consider entering into commercial transactions.

j. **Regulatory and Professional Requirements** - this may include the disclosure of certain information within your personal data to regulatory and professional bodies.

k. **Administration of Membership Records** - to administer your membership with clubs, associations and other organisations for business and/or professional purposes.

l. **Assessment and Collection of Taxes and Other Revenue** - to administer SNA and employee revenue and tax obligations which will require the disclosure of certain information to the Inland Revenue amongst others.

m. **Training and Career Development** - to administer employee training and oversee career development, which may require the disclosure of certain personal data (including contact and qualification details) to training organisations.

n. **Health & Safety** - to comply with prevailing health and safety legislation and SNA policies. This may include the processing of certain sensitive data, such as mental and physical health details about you.

o. **Internal Communications** - to facilitate communications between SNA's employees, certain personal data, such as your photograph, CV, status and office contact details may from time to time be included in any internal communications and/or on an SNA Intranet and/or in internal newsletters, magazines or other similar publications.

**p. Monitoring - please note that SNA may (at any time and without notice) monitor or keep a record of communications sent and/or received over SNA's IT resources (including: computer hardware, software, telephones, fax machines, voicemail, e-mail, building and facility access and CCTV systems) and/or record your use of SNA's IT resources in order to:**

- detect and/or prevent crime;
- establish the existence of business related facts. (e.g., in your absence to establish whether or not you have responded to a client's e-mail);
- ascertain whether you and/or SNA are complying with SNA's rules and policies (including, but not limited to, this Policy) and also with legal and/or regulatory obligations to which you and/or SNA are subject;
- ascertain whether communications are relevant to SNA's activities (e.g. checking incoming messages in your absence to ensure that SNA's standards of service do not suffer);
- ascertain and/or demonstrate whether you are attaining standards which are achieved or ought to be achieved by you (e.g. compliance with service obligations);
- carry out maintenance of IT resources and to monitor for viruses and/or any other programme which has contaminating and/or destructive properties;
- investigate or detect unauthorised use of the IT resources; and
- protect the vital interests of you as an individual including without limitation concerns regarding your whereabouts and/or safety.

SNA will, in conducting such monitoring activities, use all reasonable endeavours to comply with the UK Information Commissioner's best practice guidelines and to respect your privacy and that of third parties using the IT Resources.

**Please note that where SNA identifies the commission or alleged commission of a specific criminal activity and determines that there is a need to obtain evidence of this activity by monitoring, which would be prejudiced by informing employees about any such monitoring, SNA will conduct covert monitoring by means and for a period of time which**

**SNA considers necessary to obtain evidence of the criminal activity. Any such activity may be conducted with the knowledge of and/or in conjunction with law enforcement authorities.**

q. **CCTV** - please note that SNA may use CCTV monitoring on its premises to:

- protect your personal safety and the safety of the public when they are on SNA's premises;
- investigate, detect and/or prevent crime and to apprehend/prosecute offenders; and/or
- ascertain whether employees are complying with behavioural requirements and standards specified in their employment contracts, SNA rules and policies and statutory or regulatory obligations to which employees and/or SNA are subject.

Any such CCTV monitoring will be carried out in accordance with the DPA. To do this, SNA will rely on the CCTV Code of Practice issued by the Information Commissioner. If you would like to see a copy of the CCTV Code, please contact the Head of Human Resources or the Head of Legal Services.

SNA may sometimes disclose CCTV footage to third parties such as law enforcement authorities, solicitors and the Courts for the purposes listed above at 2.1(p). SNA may also disclose CCTV footage to the media if it believes that this will assist in the apprehension of criminals.

Other parties who may come into contact with the CCTV footage which SNA records, include individuals or organisations operating the CCTV system on SNA's behalf and organisations providing SNA with footage editing services.

**2.2** Your personal data will, on occasion, be made available to third parties who perform services for SNA (e.g. solicitors, auditors, banks, agents etc) or to inward investors or other potential business partners. These individuals may be situated outside of the United Kingdom. Any such disclosures will be subject to written contracts, confidentiality requirements and security arrangements where necessary in order to protect your personal data.

**2.3** SNA operates an Intranet to which SNA employees, and potentially contractors and temporary staff may be given access for the purpose of facilitating communication between such individuals and promoting SNA's business. SNA also operates a number of Extranets to which SNA may grant access to third parties for facilitating communication between SNA and such third parties and promoting SNA's business. You should be aware that certain of your personal data (e.g. names and office details) may be included on the Intranet and Extranets.

**2.4** SNA operates Internet websites to provide information about the activities of SNA. This may include the disclosure of certain of your personal data. The information placed on these websites may be downloaded and transferred anywhere in the world. Information placed on the Internet may be accessed by various individuals within and outside SNA. We therefore require you to be aware that if you consent to your personal data (e.g. names and office contact details) being placed on the SNA Internet websites, you are in fact consenting to this data being transferred outside of the United Kingdom and being viewed by third parties.

**2.5** In accordance with the DPA, you may request access to your personal data, which is being processed by SNA and/or request SNA not to process certain of your personal data and/or to amend or update any personal data relating to you, which is inaccurate. This will also include CCTV footage on which you appear and from which you can be identified. Any such request must be made in writing to the Head of Human Resources or the Head of Legal Services, a copy of which will be retained on your personnel file. Where you have exercised any of the above-mentioned rights, SNA will comply with your request, subject to any lawful requirements and/or exemptions granted to SNA under the DPA.

If you would like more information about your right to request access to your personal data (including CCTV footage), held by Safety Net Associates Limited who may charge you a fee (subject to the statutory maximum) for supplying you with your personal data

If you have any comments, concerns or complaints about SNA's use of your personal data, CCTV and/or SNA's compliance with the Information Commissioner's codes of practice, please contact the CEO.

## PART II

# EMPLOYEES' OBLIGATIONS WHEN PROCESSING PERSONAL DATA

**When processing any personal data for and on behalf of SNA, we require you to comply with the following obligations:**

### **1. Process personal data fairly and lawfully**

This means that we require you:

**1.1** not to **mislead or deceive** data subjects as to the **identity** of who will be holding their personal data and for what **purposes** such data will be processed by SNA.

**1.2** to be aware that personal data cannot be processed by SNA unless, either:

**1.2.1** the data subject has given his/her **consent**; or

**1.2.2** the processing is necessary for the **performance of a contract** or for the **entering into of a contract** with the data subject; or

**1.2.3** the processing is necessary for **compliance with any legal obligation** to which SNA is subject (other than an obligation imposed by a contract); or

**1.2.4** the processing is necessary to protect the **vital interest** of the data subject; or

**1.2.5** the processing is necessary for the **administration of justice**; or

**1.2.6** the processing is necessary for the purposes of **legitimate interests** pursued by SNA, except where the processing is unwarranted by reason of prejudice to the rights or legitimate interests of the data subject.

**1.3** to comply with all **procedures, which** SNA put in place in order to process personal data fairly and lawfully;

**1.4** to exercise a high degree of **care and security** when required to process any personal data and in particular **sensitive personal data**;

**1.5** be aware that at least **one of the conditions** set out below must be met when processing sensitive personal data:

- a. the data subject must have given his/her **explicit consent**; or
- b. the processing must be necessary to enable SNA to exercise its legal rights or obligations in connection with **employment**; or
- c. the processing must be necessary to protect the **vital interest** of the data subject (e.g. in life and death situations); or
- d. the processing must be carried out for the purpose of monitoring **equal opportunities** in respect of race or ethnic origin; or
- e. the information contained in the **personal data has been made public** as a result of steps deliberately taken by the data subject; or
- f. the processing must be necessary for the purposes of establishing, exercising or defending the **legal rights** of SNA; or
- g. the processing must be necessary for the **administration of justice**; or
- h. the processing must be necessary for **medical purposes** and is undertaken by a health professional (or equivalent).

**2. Personal data must only be obtained and processed for one or more specified and lawful purposes**

**2.1** This means that you should only be processing data during the course of your employment with SNA for purposes which are either **obvious** to the data subject; or have been **made apparent** to the data subject and are reflected in **SNA's Data Protection registration or notification**.

**2.2 SNA's Data Protection registration or notification is available from SNA's Data Protection Officer** . If you become aware of any additional purposes (other than those set out in the registration or notification), for which personal data is being processed by SNA, you should report the additional purposes to **SNA's Data Protection Officer** .

**3. Personal data must be processed in accordance with certain data quality requirements**

**3.1** Personal data must be **adequate, relevant and not excessive** in relation to the purpose or purposes for which such data is processed.

**3.2** Personal data must be **accurate** and where necessary, **up to date**.

**3.3** Personal data processed for any purpose or purposes must **not be kept for longer than is necessary** for that purpose or those purposes.

**3.4** In relation to points 3.1, 3.2 and 3.3 above, SNA require you to:-

- a. comply with the SNA Document Retention Policy;
- b. **update** information which appears to you to have become inaccurate and/or out of date; and
- c. only collect, disclose and/or further process personal data, which is **necessary** for a particular business related purpose.

#### **4. Personal data must be processed in accordance with the rights of data subjects under the DPA**

**4.1** You should be aware that data subjects have rights under the DPA with respect to the processing of their personal data by SNA, including where this consists of CCTV footage. In order to assist SNA to comply with data subjects' rights, you are required to inform the Head of Human Resources/ SNA's Data Protection Officer when:

- a. any request is made by a data subject for **access** to or for a copy of information about themselves, which is being processed by SNA. Any such request must not be complied with, without consent from the Head of Human Resources or SNA's Data Protection Officer or the Legal Department.
- b. any request is made by a data subject to **refrain** from starting to process or from any further processing of the data subject's personal data;
- c. a data subject requests further information about the logic involved in a decision which has been taken by SNA by automated means (without any human input) about the data subject (e.g. by a computer).

#### **5. Security arrangements**

**5.1** You must comply with all **appropriate technical** and **organisational security** measures taken by SNA against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data processed by SNA including the SNA Information Security and associated policies.

**5.2** In particular, you must comply with all other organisational **policies** issued to you by SNA including, but not limited to the SNA Information Security and associated policies and any other security access and disclosure procedures notified to you.

## **6. Disclosure of personal data**

### **6.1 YOU MUST NOT DISCLOSE ANY PERSONAL DATA PROCESSED BY SNA UNLESS SUCH DISCLOSURE:**

- a. is with the consent of SNA (such consent to be provided by SNA's Data Protection Officer or the Head of Human Resources) or in circumstances where SNA would agree to the disclosure; **and**
- b. is to an organisation and/or individual whose identity you have ascertained and are certain is entitled to obtain such information; **and**
- c. is necessary for the business purposes of SNA; **and**
- d. is, where necessary, protected by sufficient security safeguards and/or confidentiality obligations

**6.2** The consent of SNA can be assumed, where the disclosure is required:

- a. the prevention or detection of **crime**; or
- b. the **apprehension** or **prosecution** of offenders or
- c. the assessment or collection of any **tax** or **duty** or compliance with any obligation of a similar nature; or
- d. the purpose of **discharging statutory functions** on SNA; or
- e. under any **enactment**, or by any **rule of law** or by the **order of a Court**; or
- f. the purpose of, or in connection with, any **legal proceedings** (including prospective legal proceedings); or
- g. the purpose of establishing, exercising or defending **legal rights** .

## **7. Transfer of personal data outside of the European Economic Area (EEA) <sup>1</sup>**

**7.1** You should be aware that there are **restrictions** on SNA's ability to transfer personal data to a territory outside of the EEA, unless:-

- a. such territory is regarded by the European Commission as providing an **adequate level of protection** for such personal data (currently only Switzerland, Hungary, Canada and Argentina); or
- b. **consent** has been obtained from the data subject in question; or
- c. **agreements** are in place to offer adequate protection to the data; or

- d. the transfer is in order to **give effect to a contract** for or with the data subject; or
- e. the recipient company/organisation, if based in the USA, is certified as a member of the "**safe harbour**" program in the USA.

**7.2** If you are unsure about whether you are entitled to transfer personal data in an automated or manual fashion out of the EEA on behalf of SNA, consult the Head of Human Resources or the Head of Legal Services.

## **8. Liability**

**8.1** SNA will regard a failure by you to comply with the contents of this policy as a **disciplinary offence**.

**8.2** You need to be aware that in your capacity as an employee of SNA it is a **criminal offence** under Section 55 of the DPA if you knowingly or recklessly obtain or disclose personal data (or the information contained in such data), or procure the disclosure to another person of that information, without the consent of SNA.

## **9. Confidentiality**

**9.1** You should be aware that the obligations placed on you as a result of the DPA and this compliance policy are in addition to the **duty of confidentiality** which you owe to SNA in respect of all information (including personal data) processed by you about SNA, its clients, employees, suppliers and any other data subjects.

**9.2** You must keep all personal data which you process on behalf of SNA completely secret and confidential and must not disclose any such information unless **authorised** to do so by:

**9.2.1** in the case of personal data relating to SNA employees, the CEO;

**9.2.2** in the case of personal data relating to persons other than SNA employees an Executive Management Board Member or your Head of Function;

**9.2.3** in the case of any personal data this policy document and other security documents referred to in this policy and/or contained in your Conditions of Service.

## **10. Termination**

You should be aware that all information (including personal data) processed by you, during your employment with SNA (whether in a manual or automated fashion), is and will remain **the property of SNA**. On termination of your employment with SNA, you must promptly **return** the original and any copies (whether in manual or automated form) of any information including personal data) obtained by you during your employment to SNA.

## **11. Updates to this Policy**

This Policy will change from time to time to keep abreast of legislation in this area. You are therefore required to refer to this Policy on a regular basis. You will be informed of any changes to the policy.