DATA PROTECTION

1. Introduction

CSG (Usher's) views the correct and lawful handling of personal data as key to professional dealings with third parties, and shall ensure that it handles personal data correctly and lawfully.

This document sets out the obligations of the company with regard to data protection and the rights of people with whom it works in respect of their personal data under the *Data Protection Act 1998.*

This Policy must be followed by CSG (Usher's') employees, contractors, consultants or other parties working on behalf of the company.

2. Data Protection Principles

This Policy aims to ensure compliance with the Act, which sets out eight principles with which any party handling personal data must comply. All personal data:

2.1 Must be processed fairly and lawfully (and not processed unless certain conditions are met)

2.2 Must be obtained only for specified and lawful purposes, and not processed in any manner which is incompatible with those purposes

2.3 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed

2.4 Must be accurate and, where appropriate, kept up-to-date

2.5 Must be kept for no longer than is necessary

2.6 Must be processed in accordance with the rights of data subjects under the Act

2.7 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage, through appropriate technical and organisational measures

2.8 Must 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

3. Rights of Data Subjects

Under the Act, data subjects have the following rights:

- The right to be informed that their personal data is being processed
- The right to access any of their personal data held by the Company within 40 days of making a request
- The right to prevent the processing of their personal data in limited circumstances
- The right to rectify, block, erase or destroy incorrect personal data

4. Personal Data

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data, and other information which is in the possession of, or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual, and any indication of the intentions of the data controller or any other person, in respect of the individual.

The Act also defines "sensitive personal data" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings, or the sentence of any court.

The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles and with the requirements of this Policy. The following data may be collected, held and processed by the Company from time-to- time:

- Personal Details
- Family, Lifestyle and Social Circumstances
- Education and Training Details
- Financial Details
- Racial or Ethnic Origin
- Religious or Other Beliefs of a Similar Nature
- Trade Union Membership
- Physical or Mental Health or Condition
- Goods or Services provided

5. Processing Personal Data

All personal data collected by the Company is meant to ensure that the Company can facilitate efficient transactions with third parties and efficiently manage its employees, contractors and consultants. Personal data shall also be used by the Company in meeting all relevant obligations imposed by law.

Personal data may be disclosed within the Company, but it may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to it. .

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully
- Data subjects are made aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected when it is necessary to fulfil the stated purpose(s)
- All personal data is accurate and updated as required
- No personal data is held for any longer than necessary
    - All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect it
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- All data subjects can exercise their rights set out above in Section 3 and, more fully, in the Act.

6. Data Protection Procedures

The Company shall ensure that all employees, contractors, consultants or other parties working on behalf of the Company comply with the following:

- All control measures to safeguard personal data identified within company procedures shall be followed
- The security of computer systems shall be taken into account before transmitting data electronically
- Consideration shall be given to the encryption or password protection of all emails containing personal data

- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email and all temporary files associated with it should also be deleted
- Personal data shall not be provided over the telephone without first confirming the identity of the caller and the reasonableness of their request for access to the information
- Where personal data is to be sent by facsimile, the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive it
- Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data should be stored securely using passwords and, where appropriate, data encryption
- Passwords used to protect personal data for a length of time should be changed regularly and should not use words or phrases which can be easily guessed

7. Organisational Measures

CSG Usher's shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- All employees, contractors, consultants or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company's responsibilities under the Act and shall be furnished with a copy of this Policy.
- All employees, contractors, consultants or other parties working on behalf of the Company handling personal data will be appropriately trained and supervised
- Methods of collecting, holding and processing personal data may be audited
- Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, consultant or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply may also constitute a criminal offence under the Act.
- Where any contractor, consultant or other party working on behalf of the Company handling personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings.

8. Access by Data Subjects

A data subject may make a subject access request (SAR) at any time to see the information which CSG (Usher's) Limited holds about them.

- SARs must be made in writing, accompanied by the correct fee
- The Company currently requires a fee of £10 (the statutory maximum) for all SARs

Upon receipt of a SAR, the Company shall have a maximum period of 40 days within which to respond. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject
- A description of any personal data held on the data subject
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to
- Details of any technical terminology or codes

9. Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. CSG (Usher's) is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

10. Implementation of Policy

This Policy shall be deemed effective as of 15th December 2011.

Rod Usher
Managing Director