Data Protection Policy

1. Overview

a) The Company needs to gather and use information or 'data' about individuals as part of its business. The Company intends to comply with its legal obligations under the Data Protection Act 1998 (the '1998 Act') in respect of the processing of 'personal data' and 'sensitive personal data'. These rules apply whether data is stored electronically, on paper or on other materials.

b) This policy explains how the Company will hold and process this information. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of the Company.

c) This policy applies to all employees, volunteers, consultants, suppliers and anyone else working for or on behalf of the Company. It applies to all data that the Company holds relating to identifiable individuals.

d) If you are an employee, this policy does not form part of your contract of employment and it can be amended at any time.

2. Data Protection Principles

a) Personal data must be processed in accordance with eight 'Data Protection Principles.' It must:

- be processed fairly and lawfully;
- be obtained and processed only for one or more legal purposes which are set out in the 1998 Act. These purposes include getting the consent of the data subject, the processing being necessary for performance of the contract with the data subject, compliance with a legal obligation or for a legitimate interest;
- be adequate, relevant and not excessive;
- be accurate and kept up to date;
- not be kept for longer than is necessary;
- processed in accordance with the rights of the data subject;
- be protected in appropriate ways; and
- not be transferred to a country or territory outside the European Economic Area, unless that country or territory also ensures an adequate level of protection.

3. How we define personal data

b) 'Personal data' means data which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person.

4. How we define sensitive personal data

a) 'Sensitive personal data' is a type of personal data consisting of information as to:

- The racial or ethnic origin of the person;
- His or her political opinions;

- His or her religious or other beliefs;
- Whether he or she is a member of a trade union;
- His or her physical or mental health or condition;
- His or her sexual life;
- The commission or alleged commission by him or her of any offence;
- Any criminal proceedings for any such offence or allegation, the disposal of the proceedings or any court sentence.

5. How we define processing

a) 'Processing' means obtaining, recording or holding the information or data or carrying out any operation(s) on that information or data, including:

- Organisation, adaptation or alteration of it;
- Retrieval, consultation or use of it;
- Disclosure of it by transmission, dissemination or otherwise making available; or
- Alignment, combination, blocking, erasure or destruction of it.

6. How will we process personal data?

a) The Company will process personal data (including sensitive personal data) in accordance with our obligations under the 1998 Act and the Data Protection Principles in paragraph 2.
b) We will **notify** a data subject about the purpose for which we intend to process the personal data, who we might share it with and how the data subject can object.

7. How should you process personal data for the Company?

a) Everyone who works for, or on behalf of the Company, has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy. The Company's Data Protection Officer is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data.
b) You should only access data covered by this policy if you need it for the work you do for, or on behalf of the Company and are authorised to do so.
c) You should not share personal data informally.
d) You should keep personal data secure and not share it with unauthorised people.
e) You should regularly review and update personal data which you have to deal with for work.
f) You should not make unnecessary copies of personal data and should keep and dispose of those copies securely.
g) You should use strong passwords.
h) You should lock your computer screens when not at your desk.
i) Personal data should be encrypted before being transferred electronically to authorised external contacts.
j) Do not save personal data to your own personal computers or other devices.
k) Personal data should never be transferred outside the European Economic Area without the consent of the data subject or the authorisation of the Data Protection Officer.

l) You should lock drawers and filing cabinets. Don't leave paper with personal data lying about.
m) You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.
n) Personal data should be shredded and disposed of securely when you have finished with it.
o) You should seek the express consent of the data subject before using or disclosing sensitive personal data if you are authorised to do so, or if not, highlight to your line manager if you think additional consent is required.
p) You should ask for help from your manager or our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection we can improve upon.

8. How must sensitive personal data be processed?

a) There are additional conditions on processing of sensitive personal data which must be met under the 1998 Act. This includes the express consent of the data subject. You should refer to the Data Protection Officer for advice.

9. Subject access requests

b) Data subjects can make a 'subject access request' to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.