Microscope Service and Sales

Data Protection Policy

The General Data Protection Regulations (GDPR) comes into force on 25th May 2018. This document sets out the policy regarding data protection and the processing of personal data.

Who is responsible for the data protection policy?

John Groulef, Managing Director is responsible for Data Protection and the key contact if you have any questions regarding the data protection policy or anything related to the processing of personal data.

The procedure for processing data

- All personal data is received directly from individuals via phone, email or letter and not through third parties.
- Data is stored on a password protected database and is only used for the legitimate administration of the company and for the work being undertaken as requested by the customer.
- Personal data is not used for any other purpose such as marketing or sales or passed on to anyone outside the company.
- Personal data is retained only while it is required for the administration of the Company or to comply with legal or regulatory requirements.

The organisation's policy on processing sensitive personal data

The company does not store or process any sensitive personal data. All staff are trained to identify sensitive personal information which is defined by the GDPR as any data about an individual which consists of information relating to:

- the racial or ethnic origin of the data subject,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union (within the meaning of the **M1**Trade Union and Labour Relations (Consolidation) Act 1992),
- a physical or mental health or condition,
- a subject's sexual life,
- the commission or alleged commission of any offence, or
- any proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings or the sentence of any court in such proceedings.

Subject access requests

A subject access request is when an individual formally requests to see what information is held about them. Any received requests will be passed to the managing Director who will communicate to the individual what information is currently held by the company in line with their rights under the GDPR. Under the GDPR individuals have:

a) the right to see the information which we hold about you; we will provide this within 30 days, subject to you providing suitable evidence of your identity;
b) the right to have data corrected; please let us know of changes to your personal information, such as your address, so that we may update our records;
c) the right to object to us processing your information; if you object we will not be able to contact you about your ongoing work with us.

A register of subject access request is kept.

The process for reporting breaches in data protection

All staff members have an obligation to report data protection breaches or if they have concerns of such a breach. All concerns are to be raised immediately with the Managing Director.

Staff training

Staff will all undertake training in the GDPR to ensure they understand their responsibilities under the regulations relating to their role.

Privacy notice

A privacy notice is published on the company website detailing how the company collects and processes data, as well as how long it is kept for and who it will be shared with, this notice is also available by request.

What are the consequences of failing to comply with the data protection policy?

The company understands that there are severe consequences for failing to comply with data protection law and all staff understand that failing to comply with the policy may lead to disciplinary action by the company.

Signed: 

John Groulef
Manging Director 23rd April 2018