



Data Protection Policy

Data Protection Policy

The General Data Protection Regulation (GDPR) and the current Data Protection Act regulates our use of your personal data. As an employer, it is our responsibility to ensure that the personal data we process in relation to you is done so in accordance with the required principles. Any data held shall be processed fairly and lawfully and in accordance with the rights of data subjects.

You have several rights in relation to your data. More information about these rights is available in our "Policy on your rights in relation to your data". We commit to ensuring that your rights are upheld in accordance with the law and have appropriate mechanisms for dealing with such.

We may ask for your consent for processing certain types of personal data. In these circumstances, you will be fully informed as to the personal data we wish to process and the reason for the processing. You may choose to provide or withhold your consent. Once consent is provided, you are able to withdraw consent at any time.

You are required to comply with all Company policies and procedures in relation to processing data. Failure to do so may result in disciplinary action up to and including dismissal.

Company Property and Copyright

All written material, whether held on paper, electronically or magnetically which was made or acquired by you during the course of your employment with us, is our property and, where appropriate, our copyright. At the time of termination of your employment with us, or at any other time upon demand, you shall return to us any such material in your possession.

Statements To the Media

Any statements to reporters from newspapers, radio, television, etc. in relation to our business will be given only by the Director.

Virus Protection Procedures

In order to prevent the introduction of virus contamination into the software system, the following must be observed:

- a) unauthorised software including public domain software, USBs, external hard drives, CDs or internet downloads must not be used; and
- b) all software must be virus checked using standard testing procedures before being used.

Use Of Computer Equipment

In order to control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

- a) the introduction of new software must first of all be checked and authorised by the Director before general use will be permitted;
- b) only authorised staff should have access to the Company's computer equipment;
- c) only authorised software may be used on any of the Company's computer equipment;
- d) only software that is used for business applications may be used;
- e) no software may be brought onto or taken from the Company's premises without prior authorisation;
- f) unauthorised access to the computer facility will result in disciplinary action; and



Data Protection Policy

- g) unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.