Data Protection Policy

The Organisation needs to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the General Data Protection Act 2018.

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly.

Most businesses hold personal data on their clients, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level.

These include:

1.Human Rights Act 1998
2.Freedom of Information Act 2000
3.Privacy and Electronic Communications Regulations 2003
4.Regulation of Investigatory Powers Act 2000
5.Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
6.General Data Protection Act 2016
7.Computer Misuse Act 1990.

The Organisation will, through appropriate management, strict application of criteria and controls:

1.Observe fully the conditions regarding the fair collection and use of information
2.Meet its legal obligations to specify the purposes for which information is used
3.Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
4.Ensure the quality of information used
5.Apply strict checks to determine the length of time information is held

DATA PROTECTION POLICY
(continued)

6. Ensure that the rights of people about whom information is held, can be fully exercised under the act (these include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
7. Take appropriate technical and organisational security measures to safeguard personal information
8. Provide individuals that request it, within a maximum of 30 days from request, with access to personal information held about them for no charge.
9. Correct or erase any information on an individual that is inaccurate or misleading
10. Not use information for a purpose which is incompatible with the original purpose for which permission was given by the data subject
11. Obtain clear, express permission for handling and using 'sensitive' personal data such as race, ethnicity, political opinions, religious beliefs, trade union membership, state of health both physical and mental, sexual life, criminal convictions and sentences and allegations of criminal behaviour
12. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
13. Set out clear procedures for responding to requests for information
14. Allocate such resources as may be required to ensure the effective operation of the policy.

In addition, the Organisation ensures that:

1.There is an data protection officer (DPO) in place with specific responsibility for Data Protection within the Organisation
2.Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
3.Everyone managing and handling personal information is appropriately trained to do so
4.Everyone managing and handling personal information is appropriately supervised
5.Anybody wanting to make enquiries about handling personal information knows what to do
6.Queries about handling personal information are promptly and courteously dealt with
7.Methods of handling personal information are clearly described
8.A regular review and audit are made of the way personal information is held, managed and used
9.Methods of handling personal information are regularly assessed and evaluated
10.Performance with handling personal information is regularly assessed and evaluated
11.A breach of the rules and procedures identified in this Policy may lead to disciplinary action being taken against the members of staff concerned.

DATA PROTECTION POLICY
(continued)

The General Data Protection Act 2018

The General Data Protection Act 2018 replaces and extends the 1998 Act and places a legal obligation on persons who record and process personal information relating to living individuals. Although this area of the law appears to be complicated, the Act simply requires that adequate controls exist to protect individuals from the consequences of poor quality information and/or the misuse of information held about them. Under the new act organisations in breach of GDPR can be fined up to 4% of annual global turnover or £20 Million (Whichever is greater) this is the maximum fine that can be imposed for the most serious infringement.

Whilst the 1998 Act dealt with automatically processed information including information processed on computer, the GDPR Act places additional obligations on that processing information contained in 'structured manual files'. It also applies to the lawfulness and integrity of the CCTV systems operated by the Organisation.

The term 'processing' includes any function that can be performed using information and includes the actual disclosure of information. The Organisation has introduced this Data Protection Policy for the information and guidance of all employees.

The General Data Protection Act Principles

The Act applies to every organisation that handles (processes) personal information such as names (data) on living individuals (subjects). The Act has eight data protection principles, which are intended to guide the interpretation and implementation of the Act. These principles are:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purpose(s), and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, whenever necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall 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.

DATA PROTECTION POLICY
(continued)

Guiding Principles

Fair Obtaining and Processing

The Organisation will ensure that as far as practicable, all individuals whose details are processed by the Organisation are aware of the way in which that information will be obtained, held, used and disclosed. Whenever possible, individuals will be informed of the potential recipients of the information. Processing of personal information by the Organisation will be fair and lawful and, in addition, it is the Organisation's Policy that individuals will not be misled regarding the purposes to which the Organisation will process the information.

Notification

The Organisation will not use or process personal information in any way that contravenes its notified purposes, or in any way that would constitute a breach of the Data Protection Act. When appropriate, the Organisation will notify the Information Commissioner of any amendments to the existing Organisation's notified purposes or of new purposes to be added to the Notification Register entry.

Information Quality and Integrity

The Organisation will endeavour to process personal information, which is accurate, current and is of good quality. Information that is obtained by the Organisation will be adequate and not excessive for the purpose for which it is processed. In addition, information will be kept by the Organisation for no longer than is necessary for the purpose or purposes for which it was obtained.

Subject Access

The Organisation will respond positively to subject access requests, replying as quickly as possible, and in any event within the 30-day time limit. Whilst individuals have a general right of access to any of their own personal information which is held, the Organisation will be mindful of those circumstances where an exemption may apply.

The Organisation will only disclose personal data to those recipients listed in the Notification Register, or whenever it is otherwise permitted by law to do so. The Organisation will always endeavour to seek the permission of the data subject, where it is required by law to do so. The company will only collect the minimal amount required.

Technical and Organisational Security

The Organisation has in place appropriate security measures as required by the General Data Protection Act. Information systems are installed with adequate security controls and company employees who use these systems will be properly authorised to use them for company business.

DATA PROTECTION POLICY
(continued)

Computer Misuse
The Computer Misuse Act 1990 makes it an offence to gain unauthorised access to a computer, even if no damage is done and no files are deleted or changed. Anyone who accesses a computer without authorisation, say by guessing a password, faces a maximum six-month prison sentence, or a maximum fine of £2,000, or both.

If an individual gains unauthorised access with the intent to commit a further offence, for example access your bank account online to transfer money, they face five years' imprisonment and/or a fine.

This Act also makes it an offence to purposefully change files on a computer with intent and without authorisation. This could include deleting files or even changing computer settings. Anyone who does so, even if there is no intent to defraud or do damage, faces a maximum prison sentence of five years and/or an unlimited fine.

Controlling Access
The Organisation has tightened physical access to data by restricting access to employees needing to access specific data in order to carry out their jobs. The Organisation takes steps to prevent accidental loss or theft of personal data by using server backup processes and increased security at our offices.

Safeguarding Data
Our business relies on computers to store data, so it was necessary to introduce the following electronic safeguards:

1.We have up-to-date antivirus software to protect against viruses damaging our data and computers
2.We protect our computer network from hackers with a firewall
3.We have introduced housekeeping measures by regular backups and disabling people's accounts as they leave the business
4.We have introduced a clear strategy for managing all our computer security tools.

E-mail and Internet Privacy
The inappropriate use of e-mail and the Internet by employees, e.g. using the Internet for non-work purposes, can have significant consequences for our Organisation. This can be in terms of:

1.Embarrassment/damage to the Organisation's reputation
2.Loss of productivity
3.Increased risk of liability and legal action, e.g. For sexist or racist e-mails
4.Increased virus risk.

DATA PROTECTION POLICY
(continued)

To avoid inappropriate usage, we have introduced security electronic safeguards. A firewall checks, guarantees and manages e-mail attachments. The Organisation has installed filtering software that searches e-mails for specific words or phrases, normally obscene or discriminatory, and monitors which websites our employees are accessing as well as filtering which types of websites our employees can access.

Acceptable use of E-mail and the Internet
Please see the E-mail and Internet Acceptable Usage Policy.

In addition, the Organisation's employees will be kept fully informed about overall information security procedures and the importance of their role within these procedures. Similarly, manual filing systems are held in secure locations and only authorised employees can access them.

Responsibilities & Review
The Managing Director and data protection officer has overall responsibility for the administration and implementation of the Organisation's General Data Protection Policy.

Each Department Manager will assume authority for the compliance of the employees within their department.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Act 2018.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

1.Weakness in the Policy is highlighted
2.Weaknesses in hardware and software controls are identified
3.In case of new threat(s) or changed risks
4.Changes in legislative requirements
5.Changes in Government, company or other directives and requirements.