General Data Protection Regulation Policy Document

December 2017 – Reviewed May 2018

This policy document is the basis of our commitment to the General Data Protection Regulation.

It is itemised in the following steps:

1 Network Security

Anti-virus software (Bit Defender, installed network wide), automatically updated, monitored by ourselves and monitored and maintained by ECS Computers of King's Lynn, who advise on changes and updates.

We have a UTM (Unified Threat Management device) providing a firewall and other services providing a high level of security between the server and outside world. The UTM is maintained by ECS. All wireless connections are protected and isolated.

Regular reports from ECS Computers confirm that these systems are maintained and effective.

Password changes are made approximately monthly.

Personal devices are not allowed to be used without permission from management.

2 User Education and Awareness

All staff having computer access are informed of our policy regarding computer use. This is continuously reviewed, and staff are updated on any known threats.

This includes

Not opening any suspicious email content.

Not accessing dubious or unauthorised websites.

Not downloading potentially unsafe content.

Not using the computer system for personal use without express permission from management.

Use of removable media devices is not allowed without management authorisation. This includes (but not limited to) memory sticks, disks, removable drives.

3 Malware Prevention

Largely covered by our anti-virus software and UTM as noted in point 1 above.

Supported by user awareness as noted in point 2 above.

4 Removable Media Controls

Unless we can reasonably assess the content, staff are not permitted to access drop-boxes. If any personal data is sent via email, it is password protected

Only authorised removable devices (e.g. memory sticks, USB disk drives) are to be used to help prevent malware and virus transfer into our system.

5 System Configuration

ECS Computers manage server and workstation updates.

A reporting system is to be gradually introduced by ECS Computers providing evidence that workstation and server updating is complete and up to date.

Existing Windows XP workstations (still in use for compatibility reasons) are denied internet access to minimise their inherent security weaknesses.

Visitors using laptops or similar devices for demonstration purposes etc are not allowed to connect to our network and must run their devices on a stand-alone basis (applies to any devices including mobile 'phones and tablets).

6 Managing User Privileges

Due to the company structure, all personnel using computer workstations have access to all our data. It is not deemed practical to restrict users to only the data appropriate to their role.

Emails on remote devices, such as phones, tablets etc are allowed by agreement from management

Only a limited number of personnel have administration rights to the server.

All personnel and payroll information are handled by the companies' accountant Hayhow & Company.

7 Incident Management

Our risk assessment for the computer system has led to several safeguards being put in place. These include:

Main server backup with on-site and off-site (NAS box and cloud) copies of our server / data backup files, managed by ECS Computers. These backups allow our system to be restored to existing or replacement hardware in a minimal amount of time.

Additional extra backups are also carried out, including manual copies of the Users, Advantage and Pegasus Capital Gold data.

Images of workstations are made regularly to potentially allow workstations to be restored if they are rendered inoperable (e.g. by ransomware attack).

A more detailed outline of backup operations is available. Logs are also kept detailing backups.

Data breaches and incidents such as ransomware attacks must be reported to the relevant authorities.

8 Monitoring

As mentioned throughout the above points, aspects of the IT system will be monitored and reported to or logged to provide evidence that security is being maintained and help identify unusual behaviour possibly indicating attacks or other problems.

The backup system is tested regularly (by running test restores of certain data).

9 Home and Mobile Working

Appropriate personnel will agree on who is permitted to log on to, or otherwise access our system remotely.

Laptops and similar devices must have password protection. Passwords must not be saved locally in case of theft. Similarly, any encryption keys for devices must not be kept with the device but retained separately and securely.