1. The legislation covering this activity is the Data Protection Act 1998 'the Act'. This provides for certain exemptions, namely:

> *"Organisations that process personal data only for:*
> - *staff administration (including payroll);*
> - *advertising, marketing and public relations (in connection with their own business activity); and*
> - *accounts and records"*

Staff in Stanmore Group outsourcing division have some limited access to personal data. Accordingly, from dated 24 Oct 2014 Stanmore is registered with the Information Commissioner's Office under the Act.

2. The Company follows best practice recommendations of the Information Commissioner's Office, including:

2.1 For computer security:

- Ensuring that firewalls and virus-checking software is installed on all computers and servers connected to the internet.
- Making sure that operating systems is set up to receive automatic updates.
- Protecting computers by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allowing staff access to the information they need to do their job and having a policy not to share passwords.
- Encrypting any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Taking regular back-ups of the information on the computer systems and keeping them in a separate place so that information is not lost in the event of a computer failure.
- Securely removing all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Installing anti-spyware software. Spyware is the generic name given to programs that are designed to secretly monitor activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect computers from spyware threats, and it is often free to use and update.

2.2 For other security:

- Shredding all your confidential paper waste.
- Checking the physical security of your premises.
- Training staff:
    - so they know what is expected of them;
    - to be wary of people who may try to trick them into giving out personal details so that they can be prosecuted if they deliberately give out personal details without permission;
    - to use strong passwords - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters, like the asterisk or currency symbols;
    - not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
    - not to believe emails that appear to come from a bank asking for account, credit card details or password details (a bank would never ask for this information in this way);
    - not to open spam – not even to unsubscribe or ask for no more mailings – but to delete the email
    - to get spam filters on the email system or to use an email provider that offers this service.

Signed: _____ dated 18.5.18

Managing Director