1. DEVICES AND EQUIPMENT

a. When you are working in a shared or public space do not leave portable devices while you go off and do other things. Put it away and lock it in a drawer or take it with you.

b. Use strong passwords and store them securely away from your machines.   Do not share passwords with anyone else.

c. Do not let other people have access to the device you access our data from unless they are colleagues who are properly trained in data management using their own individual password and profile. Do not let your children play on your machine after working hours.

d. Encrypt all your devices and make sure you have a secure place to store any drives, USB sticks, CDs etc that store data.

e. Have a regular back-up routine for data you are holding, in a secure off-site location. Check that you can recover data properly from your back-ups.

f. Your screen must not be visible to other people when you are working.

g. You must have an automatic screen lock on that hides your work when you walk away from your desk.

h. You must have our specific permission before you download Confidential Information onto your own device and you may only use it or store it in locations we specify.

i. File sharing applications such as Dropbox, SharePoint, Google drive, will create local copies. We may specify you use them.

j. Use up-to-date anti-virus, anti-ransom and malware detection software on all your devices, update it regularly, scan all incoming and outgoing traffic from your devices, and run a full scan at least fortnightly.

k. Ensure that a software firewall is working on your devices.

l. Use a VPN when using your portable devices away from your home base. Other people can intercept your data on shared and public Wi-Fi.

m. If you are using your own home-based Wi-Fi make sure that is secured.

n. If you are going to dispose of a computer, device, or storage media that contains any Confidential Information, make sure you e-shred the data on it first (or pay a secure provider to do it for you).

2. TRAINING, AND SECURITY CHECKS

If your employees or associates will have access to any system containing our Confidential Information:

a. You must take proper care to recruit employees or associates or suppliers (with access to your systems and data) who are responsible, reliable and honest.

b. You must check that they are working to an appropriate level of security and knowledge around GDPR.

c. You must pass on our Data Processing Instructions and our Data Privacy Policy to any individual who is authorised to access information that comes from us.

d. Make sure they are properly contracted to handle information securely.

e. You must not give access to our systems (by password sharing or any other means) but request it from us.

f. Where you have permission to store data locally in your systems, you must not give access to anyone who is not authorised by us to view or use that data.

g. You must only give the lowest possible and most restricted level of access necessary for them to do the work as authorised. You must remove that access upon completion of the work or when they cease working with you and make sure they have no access after this point.

3. SOFTWARE AND DOCUMENT SHARING

a. When sharing log-ons and passwords we will share with you via a secure system such as last pass sharing; or create unique log ins for you that email themselves to the email address you are using; or we will email the log in or text or WhatsApp the password so the two are never sent in the same medium unencrypted.

b. If we ask you to set up new sites, apps and software for us you must create us as the master user/administrator and send us (securely as set out in 3a) the master log in. Where such systems are chargeable, we will need to log in and add our payment details. You may create yourself as a user with appropriate rights to do what we have asked you to do.

c. Where we require file sharing in platforms such as Dropbox, SharePoint, or Google Drive, we will set up a folder where you have rights to the documents we share. We must be the folder creator since that gives us the ability to remove your access once the work is complete.

d. We will give you by text a default password which will be used for all emailed attachments containing personal data. You must not send it back with the attachment or store it in your email folder. If you lose it we will text it.

e. Wherever possible we will set up multi factor authentication which means your logins may require authentication by text to your phone, or via an authenticator app such as Google or LastPass authenticator.

f. On completion of each Brief and at the end of your Engagement we will remove your access to files and platforms you no longer need. We may also vary your level of access if your assignment and need to access personal data changes.