Annie Knapman Yoga

IT Security Policy

May 2018

1. Introduction

This document sets out the measures to be taken by all employees of Annie Knapman Yoga (the "Company") and by the Company as a whole in order to protect the Company's computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate or accidental.

2. Key Principles

2.1 All IT Systems are to be protected against unauthorised access.

2.2 All IT Systems are to be used only in compliance with relevant Company Policies.

2.3 All data stored on IT Systems are to be managed securely in compliance with all relevant parts of the GDPR and all other laws governing data protection whether now or in the future in force.

2.4 All employees of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

2.5 All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

2.6 All IT Systems are to be installed, maintained, serviced, repaired and upgraded by Annie Knapman (the "IT Department") or by such third party/parties as the IT Department may from time to time authorise.

2.7 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity and confidentiality of that data) lies with the IT Department unless expressly stated otherwise.

2.8 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the IT Department.

2.9 All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the IT Department.

3. IT Department Responsibilities

3.1 The IT Manager, Annie Knapman shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;

b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, by way of periodic audits and risk assessments, with regular reports being made to the Company's internal

senior management on the condition of the Company's information security and compliance with this Policy;

c) ensuring organisational management and dedicated staff responsible for the development, implementation and maintenance of this Policy;

d) carrying out vulnerability assessments and patch management by using threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code; and

e) ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations and other relevant rules whether now or in the future in force including, but not limited to, the GDPR and the Computer Misuse Act 1990.

3.2 The IT Department shall be responsible for the following:

a) assisting all Users in understanding and complying with this Policy;

b) providing all Users with appropriate support and training in IT security matters and use of IT Systems;

c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities and any special security requirements;

d) receiving and handling all reports relating to IT security matters and taking appropriate action in response;

e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

f) assisting the IT Manager in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future;

g) ensuring that regular backups are taken of all data stored within the IT Systems at intervals no less than monthly and that such backups are stored at a suitable location off the Company premises; and

h) ensure compliance with all IT security standards set out in ISO 27001, to the extent such standards are not covered by the obligations set out in clause 3.2 a) – g).

4. Users' Responsibilities

4.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.

4.2 All Users must use the IT Systems only within the bounds of English law and must not use the IT Systems for any purpose or activity which is likely to contravene any English law whether now or in the future in force.

4.3 Users must immediately inform the IT Department of any and all security concerns relating to the IT Systems.

4.4 Users must immediately inform the IT Department of any other technical problems (including, but not limited to, hardware failures and software errors) which may

occur on the IT Systems.

4.5 Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

5.1 All software in use on the IT Systems (including, but not limited to, operating systems and individual software applications) will be kept up-to-date and any and all relevant software updates, patches, fixes and other intermediate releases will be applied at the sole discretion of the IT Department. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release and thus falls within the remit of new software procurement and outside the scope of this provision.

5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.

5.3 No Users may install any software of their own, whether that software is supplied on physical media (e.g. DVD-Rom) or whether it is downloaded, without the approval of the IT Manager. Any software belonging to Users must be approved by the IT Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

5.4 All software will be installed onto the IT Systems by the IT Department unless an individual User is given written permission to do so by the IT Manager. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

6.1 Most IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall and internet security software. All such anti-virus, firewall and internet security software will be kept up-to-date with the latest software updates and definitions.

6.2 All IT Systems protected by anti-virus software will be subject to a full system scan at least monthly.

6.3 All storage media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed by the User.

6.4 Users shall be permitted to transfer files using cloud storage systems. All files downloaded from any cloud storage system must be scanned for viruses during the download process.

6.5 Any files being sent to third parties outside the Company, whether by email, on physical media or by other means (e.g. FTP or shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. Where any virus is detected by a User this must be reported immediately to the IT

Department (this rule shall apply even where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided to limit disruption to the User.

6.6 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised individual access to such locations for any reason.

7.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment and network infrastructure) and any other areas where personal data may be stored (eg. data centre or server room facilities) shall be designed to (i) protect information and physical assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of the relevant facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the IT Manager. Under normal circumstances whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Manager.

7.4 All non-mobile devices (including, but not limited to, desktop computers, workstations and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

7.5 All mobile devices (including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight.

7.6 The IT Department shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled and the corresponding data shall be kept on the asset register.

8. Access Security

8.1 All IT Systems (and in particular mobile devices including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) shall be protected with a secure password or such other form of secure log-in system as the IT Department may deem appropriate. Such alternative forms of secure log-in may include fingerprint identification and facial recognition.

8.2 Logical access controls designed to manage electronic access to data and IT System functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all Users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

8.3 All passwords must, where the software, computer or device allows:

8.3.1 be at least 8 characters long;

8.3.2 contain a combination of upper and lower case letter and numbers;

8.3.3 be changed at least every 180 days;

8.3.4 be different from the previous password;

8.3.5 not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.);

8.3.6 be created by individual Users; and

8.3.7 newly issued passwords must be changed after first use

8.4 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone including the IT Manager and the IT Staff. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password they should change their password immediately and report the suspected breach of security to the IT Department.

8.5 If a User forgets their password, this should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.

8.6 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 30 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

8.7 The IT Department shall conduct regular system audits or event logging and related monitoring procedures to proactively record User access and activity on the IT Systems for routine review.

8.8 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the IT Manager.

8.9 Users may connect their own devices (including, but not limited to, mobile telephones, tablets and laptops) to the Company network subject to the approval of the IT Department. Any and all instructions and requirements provided by the IT Department governing the use of Users' own devices when connected to the Company network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the IT Systems. The IT Department shall reserve the right to request the immediate disconnection of any such devices without notice.

9. Data Protection

9.1 All personal data (as defined in the General Data Protection Regulation ("GDPR")) collected, held and processed by the Company will be collected, held and processed strictly in accordance with the GDPR and the Company's Data Protection Policy.

9.2 The IT Department shall ensure there are data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data that is:

a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or

b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

9.3 All emails containing personal data must be encrypted.

9.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

9.5 Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

9.6 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

9.7 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

9.8 The IT Department shall ensure operational procedures and controls to provide to provide for the secure disposal of any part of the IT Systems or any media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Company's possession.

9.9 Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be

securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

9.10 The IT Department shall ensure that it has in place appropriate technical and, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

9.11 All personal data stored electronically should be backed up monthly with backups stored electronically on-site. All backups should be encrypted.

9.12 All electronic copies of personal data should be stored securely using passwords and data encryption.

9.13 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Annie Knapman (info@annieknapmanyoga.co.uk) to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

9.14 Only Users that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

9.15 All Users handling personal data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy.

10. Internet and Email Use

10.1 All Users shall be subject to, and must comply with, the provisions of the Company's Communications, Email and Internet Policy when using the IT Systems.

10.2 Where provisions in this Policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by the Communications, Email and Internet Policy, Users must take such steps as required.

11. Reporting IT Security Breaches

11.1 All concerns, questions, suspected breaches or known breaches shall be referred immediately to the IT Manager.

11.2 Upon receiving a question or notification of a breach, the IT Department shall, within 24hrs assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the IT Department deems necessary to respond to the issue.

11.3 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the IT Department. Users may only attempt to

resolve IT security breaches under the instruction of, and with the express permission of, the IT Department.

11.4 All IT security breaches, whether remedied by the IT Department or by a User under the IT Department's direction, shall be fully documented.

12. Business Continuity

The Company shall have in place adequate business resiliency/continuity and disaster recovery procedures designed to maintain any information and the supply of any service and/or recovery from foreseeable emergency situations or disasters.

13. Implementation of Policy

This Policy shall be deemed effective as of 17/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Annie Knapman
Position:	Business Owner
Date:	17/05/2018
Due for Review by:	17/05/2019
Signature: