<<

1. **Introduction**

This document sets out th n by all employees of <<insert Company name>> (the "C ompany as a whole in order to protect the Company's c vices, infrastructure, computing environment and any and ment (collectively, "IT Systems") from damage and threats wh deliberate, or accidental.

2. **Key Principles**

2.1 All IT Systems are to authorised access.

2.2 All IT Systems are pliance with relevant Company Policies.

2.3 All employees of the all third parties authorised to use the IT Systems inclu contractors and sub-contractors (collectively, "Users" are familiar with this Policy and must adhere to and c

2.4 All line managers mu under their control and direction must adhere to and at all times as required under paragraph 2.3.

2.5 All data stored on IT aged securely in compliance with all relevant parts n Legislation. "Data Protection Legislation" means a ction and privacy laws including, but not limited to, th n of the General Data Protection Regulation ((EU) 20 "), as it forms part of the law of England and Wales, Ireland by virtue of section 3 of the European Union he Data Protection Act 2018, the Privacy and Electron ulations 2003 as amended, and any successor legisla

2.6 All data stored on IT sified appropriately (including, but not limited to, pers ersonal data, and confidential information) **[**with re sifcation system/procedure etc. if appropriate>>**]**. All st be handled appropriately in accordance with its c

2.7 All data stored on IT lable only to those Users with a legitimate need for a

2.8 All data stored on IT cted against unauthorised access and/or processing.

2.9 All data stored on protected against loss and/or corruption.

2.10 All IT Systems are tained, serviced, repaired, and upgraded by <<inser partment>> (the "IT Department") or by such third pa partment may from time to time authorise.

2.11 The responsibility fo ty of all IT Systems and the data stored thereon (inc to, the security, integrity, and confidentiality of that partment unless expressly stated otherwise.

2.12 All breaches of sec T Systems or any data stored thereon shall be uently investigated by the IT Department. **[**Any b known or suspected to involve personal data shall b Protection Officer, <<insert name and contact details>>

2.13 All Users must repor ncerns relating to the IT Systems or to the data stored the IT Department. **[**If any such concerns relate in a , such concerns must **[**also**] OR [**instead**]** be reported fficer.**]**

3. **IT Department Responsibi**

3.1 The IT Manager, <<i details>>, shall be responsible for the following:

a) ensuring that sessed and deemed suitable for compliance w ty requirements;

b) ensuring that thin the Company are effectively implemented working in consultation with the Company's s nd Data Protection Officer, as appropriate,**]** come of such reviews to the Company's se

c) ensuring that are of the requirements of this Policy and o regulations, and other relevant rules whether orce including, but not limited to, the Data Prot e Computer Misuse Act 1990.

3.2 The IT Staff shall be ving:

a) assisting all U nd complying with this Policy;

b) providing all upport and training in IT security matters and u

c) ensuring that vels of access to IT Systems that are appropria ng into account their job role, responsibilitie ty requirements;

d) receiving and ating to IT security matters and taking approp **[**including, in the event that any reports relate ng the Data Protection Officer**]**;

e) taking proacti e, to establish and implement IT security proce areness;

f) assisting the oring all IT security within the Company and tion to implement this Policy and any changes future; and

g) ensuring that en of all data stored within the IT Systems at i <insert interval>> and that such backups are s ion **[**onsite**] AND/OR [**offsite**]**. All backups shou <insert type(s) of encryption>>**]**.

4. **Users' Responsibilities**

4.1 All Users must comp s of this Policy at all times when using the IT Systems

4.2 All Users must use t n the bounds of UK law and must not use the IT Syste tivity which is likely to contravene any UK law whether rce.

4.3 Users must immedia ment **[**(and, where such concerns relate to personal da Officer)**]** of any and all security concerns relating to t

4.4 Users must immedi partment of any other technical problems (including, vare failures and software errors) which may occur on

4.5 Any and all delibera s of this Policy by Users will be handled as appropria disciplinary procedures.

5. **Software Security Measur**

5.1 All software in use d ding, but not limited to, operating systems, individual s firmware) will be kept up-to-date and any and all tes, patches, fixes, and other intermediate release the sole discretion of the IT Department. This pr d to upgrading software to new 'major releases' (e.g ion 2.0), only to updates within a particular major relea 0 to version 1.0.1 etc.). Unless a software update is e it will be classed as a major release, falling within are procurement and outside the scope of this provisio

5.2 Where any security software that flaw will be either fixed immediately or ndrawn from the IT Systems until such time as the sec ely remedied. **[**If the security flaw affects, is likely to af ffect any personal data, the Data Protection Officer sh ely.**]**

5.3 No Users may insta own, whether that software is supplied on physical ownloaded, without the approval of the IT Manager. A Users must be approved by the IT Manager and may that installation poses no security risk to the IT System ion would not breach any licence agreements to which bject.

5.4 All software will be i ems by the IT Department unless an individual User is on to do so by the IT Manager. Such written permis which software may be installed and onto which comp y be installed.

6. **Anti-Virus Security Measu**

6.1 Most IT Systems (in d servers) will be protected with suitable anti-virus, f le internet security software. All such software will b the latest software updates and definitions.

6.2 All IT Systems prote re will be subject to a full system scan at least <<inser

6.3 All physical media (s or disks of any kind) used by Users for transferrin canned before any files may be transferred. Such v performed **[**automatically upon connection / insertio he User**]** **OR [**by the IT Staff / Manager**]**.

6.4 Users shall be permi g cloud storage systems only with the approval of the I vnloaded from any cloud storage system must be scar e download process.**]**

6.5 Any files being sent the Company, whether by email, on physical media, shared cloud storage) must be scanned for viruses part of the sending process, as appropriate. **[**All ema ed automatically upon sending.**]**

6.6 Where any virus is must be reported immediately to the IT Department (en where the anti-virus software automatically fixes t partment shall promptly take any and all necessary ac em. In limited circumstances this may involve the te e affected computer or device. Wherever possible a mputer or device will be provided **[**immediately**]** **OR [**w >>**]** to limit disruption to the User.

6.7 **[**If any virus or othe ely to affect, or is suspected to affect any personal c bove, the issue must be reported immediately to the D

6.8 Where any User deli malicious software or virus to the IT Systems this will nce under the Computer Misuse Act 1990 and will be under the Company's disciplinary procedures.

7. Hardware Security Measu

7.1 Wherever practical, cated in rooms which may be securely locked whe priate cases, at all times whether in use or not (with au anted access by means of a key, smart card, door cod ess to such locations is restricted, Users must not allo ccess to such locations for any reason.

7.2 All IT Systems not in y Users (including, but not limited to, servers, networ network infrastructure) shall be located, wherever po ecured, climate-controlled rooms and/or in locked c accessed only by designated members of the IT D

7.3 No Users shall have ns not intended for normal use by Users (including s d above) without the express permission of the I mal circumstances, whenever a problem with such I y a User, that problem must be reported to the IT De umstances should a User attempt to rectify any such xpress permission (and, in most cases, instruction an T Manager.

7.4 All non-mobile devi limited to, desktop computers,

workstations, and [illegible]ver possible and practical, be physically secured i[illegible] locking mechanism. Where the design of the hardw[illegible]ases shall be locked to prevent tampering with or the[illegible]s.

7.5 All mobile devices [illegible]mited to, laptops, tablets, and smartphones) provi[illegible] should always be transported securely and handle[illegible]nces where such mobile devices are to be left unatten[illegible]d inside a lockable case or other suitable container. U[illegible]easonable efforts to avoid such mobile devices from[illegible]at any location **[**other than their private homes or Co[illegible]such mobile device is to be left in a vehicle it must be[illegible]nd, where possible, in a locked compartment.

7.6 The IT Department s[illegible]e asset register of all IT Systems. All IT Systems shall [illegible]responding data shall be kept on the asset register.

8. Access Security

8.1 Access privileges for[illegible]determined on the basis of Users' levels of authority wi[illegible]e requirements of their job roles. Users shall not be g[illegible]Systems or electronic data which are not reasonably re[illegible]of their job roles.

8.2 All IT Systems (and [illegible]ices including, but not limited to, laptops, tablets, and [illegible]rotected with a secure password or passcode, or such [illegible]g-in system as the IT Department may deem appropri[illegible]ll forms of biometric log-in are considered secure. C[illegible]roved by the IT Department may be used.

8.3 All passwords must, [illegible]puter, or device allows:

a) be at least <<[illegible]ers long;

b) contain a com[illegible] lower case letters / numbers / spaces / symb[illegible]

c) be changed a[illegible]erval>> days;

d) be different fr[illegible]d;

e) not be obviou[illegible] birthdays or other memorable dates, memor[illegible]places etc.); and

f) be created by[illegible]

8.4 Passwords should b[illegible] User. Under no circumstances should a User share[illegible]nyone, including the IT Manager and the IT Staff. No[illegible]ely asked for their password by anyone at any time [illegible]should be refused. If a User has reason to believe th[illegible]s obtained their password, they should change their [illegible]and report the suspected breach of security to the IT D[illegible]personal data could be accessed by an unauthorised i[illegible]ction Officer**]]**.

8.5 If a User forgets thei[illegible]e reported to the IT Department. The IT Department w[illegible]eps to restore the User's access to the IT Systems w[illegible]ssuing of a temporary password

which may be fully o ember of the IT Staff responsible for resolving the is must be set up by the User immediately upon the the IT Systems.

8.6 Users should not wri s possible to remember them. If a User cannot remem ld be stored securely (e.g. in a locked drawer or in a ase) and under no circumstances should passwords be s to see (e.g. by attaching a note to a computer displa

8.7 All IT Systems with devices (e.g. mouse, keyboard, touchscreen etc.) s ere possible, with a password protected screensav fter <<insert time period>> of inactivity. This time ed by Users and Users may not disable the screens screensaver will not interrupt or disrupt any other on the computer (e.g. data processing).

8.8 All mobile devices mited to, laptops, tablets, and smartphones) provid l be set to lock, sleep, or similar, after <<insert time p uiring a password, passcode, or other form of log-in t ar. Users may not alter this time period.

8.9 Users may not use allow outside parties to access the IT Systems with nt of the IT Manager. Any such software must be rea User for the performance of their job role and must b eared by the IT Manager **[**and, where such access r cessible by the outside party, the Data Protection Offic

8.10 **[**Users may connect uding, but not limited to, laptops, tablets, and smartp rt specific network name(s), if appropriate>>**]** Com ct to the approval of the IT Department. Any ar equirements provided by the IT Department governin devices when connected to the Company network r times. Users' use of their own devices shall be sub y, all relevant Company Policies (including, but not lin e those devices are connected to the Company netw art of the IT Systems. The IT Department shall res t the immediate disconnection of any such devices wit

9. Data Storage Security

9.1 All data, and in pa hould be stored securely using passwords and **[**<<in >>**]** data encryption.

9.2 All data stored elec edia, and in particular personal data, should be store x, drawer, cabinet, or similar.

9.3 No personal data sh mobile device (including, but not limited to, laptops, ta , whether such device belongs to the Company or oth nal written approval of the Data Protection Officer ar approval, strictly in accordance with all instructions a at the time the approval is given, and for no longer tha y**]**.

9.4 No data, and in p should be transferred to any

computer or device p User unless the User in question is a contractor or su behalf of the Company and that User has agreed to ompany's Data Protection Policy and the Data Protect

10. **Data Protection**

10.1 All personal data (a Protection Legislation) collected, held, and processed e collected, held, and processed strictly in accordance e Data Protection Legislation, the provisions of the D tion and the Company's Data Protection Policy.

10.2 All Users handling da the Company shall be subject to, and must comply wit Company's Data Protection Policy at all times. In particu pply:

a) All emails co ust be encrypted **[**using <<insert type(s) of enc

b) All emails co ust be marked "confidential";

c) Personal da d over secure networks only; transmission rks is not permitted under any circumstance

d) Personal data over a wireless network if there is a wired alte y practicable;

e) Personal dat y of an email, whether sent or received, sho rom the body of that email, and stored secure ld be deleted. All temporary files associated th eleted **[**using <<insert method of deletion>>**]**;

f) All personal d physically, including that on removable el ransferred in a suitable container marked "confi

g) Where any co ta is being viewed on a computer screen and t is to be left unattended for any period of tim he computer and screen before leaving it.

10.3 Any questions relat should be referred to **[**the Data Protection Officer,**]** < t details>>.

11. **Internet and Email Use**

11.1 All Users shall be s mply with, the provisions of the Company's Commu ernet Policy when using the IT Systems.

11.2 Where provisions in additional steps to be taken to ensure IT security t or email over and above the requirements impos ons, Email and Internet Policy, Users must take suc

12. **Reporting IT Security Brea**

12.1 Subject to paragrap estions, suspected breaches, or known breaches sha ely to **[**<<insert specific name>>**]** **OR [**the IT Departme **OR [**a member of the IT Staff**]**.

12.2 **[**All concerns, questi , or known breaches that involve personal data shall b o the Data Protection Officer who shall handle the ma the Company's Data Protection Policy.**]**

12.3 Upon receiving a qu breach, the IT Department shall, within <<insert perio including, but not limited to, the level of risk associat ake any and all such steps as the IT Department deem o the issue.

12.4 Under no circumsta tempt to resolve an IT security breach on their own the IT Department **[**(or the Data Protection Officer, a may only attempt to resolve IT security breaches un d with the express permission of, the IT Department.

12.5 All IT security breach y the IT Department or by a User under the IT Departm fully documented.

13. **Policy Review**

The Company shall review t <<insert interval>> and otherwise as required in order to en -to-date and fit for purpose. All questions, concerns, and ng to this Policy should be communicated to the IT Ma nd contact details>> **[**and/or the Data Protection Officer, <<in etails>>**]**.

14. **Implementation of Policy**

This Policy shall be deeme rt date>>. No part of this Policy shall have retroactive effect y to matters occurring on or after this date.

This Policy has been approv

Name: <<insert f

Position: <<insert p

Date: <<insert d

Due for Review by: <<insert d

Signature: