<<
D

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 data (electronic a , held, and processed by the Company, and to protect th systems, devices, infrastructure, computing environment, an vant equipment (collectively, "IT Systems") from damage nternal, external, deliberate, or accidental.

For the purposes of this Poli e following type(s) of data:

a) <<insert list o

b) <<add further

This Policy shall be subj in accordance with, the Data Protection Legislation. "Da on" means all legislation and regulations in force from ti e use of personal data and the privacy of electronic commu ot limited to, the retained EU law version of the General Data EU) 2016/679) (the "UK GDPR"), as it forms part of the law c cotland, and Northern Ireland by virtue of section 3 of the Eu al) Act 2018, the Data Protection Act 2018, the Privacy and E s Regulations 2003 as amended, and any successor legislatio

For the purposes of this Po all carry the meaning defined in Article 4 of the UK GDPR g to an identified or identifiable natural person (a "data sub tural person is one who can be identified, directly or indirec rence to an identifier such as a name, an identification num nline identifier, or to one or more factors specific to the physi ic, mental, economic, cultural, or social identity of that natural

2. Key Principles

2.1 All IT Systems and d gainst unauthorised access.

2.2 All IT Systems and nly in compliance with relevant Company Policies.

2.3 All personal data mu pliance with the Data Protection Legislation and the C n Policy.

2.4 All employees of the all third parties authorised to use the IT Systems and nd processed by the Company including, but not li nd sub-contractors (collectively, "Users"), must ensur ith this Policy and must adhere to and comply with it at

2.5 All line managers mu under their control and direction

must adhere to and y at all times as required under paragraph 2.4.

2.6 All data must be mar ance with all relevant parts of the Data Protection Legi cable laws whether now or in the future in force.

2.7 All data must be clas uding, but not limited to, personal data, "special categ described in Article 9 of the UK GDPR), and confide eference to <<insert classifcation system/procedure et ata so classified must be handled appropriately in acco tion.

2.8 All data, whether s r in hardcopy format, shall be available only to thos need for access.

2.9 All data, whether s r in hardcopy format, shall be protected against un processing.

2.10 All data, whether s r in hardcopy format, shall be protected against los

2.11 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.

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

2.13 The responsibility fo y of data that is not stored on the IT Systems lies with ficer, <<insert name and contact details>>**] AND/OR** individuals and/or department(s) responsible>>.**]**

2.14 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>>

2.15 All breaches of secu t is not stored on the IT Systems shall be reported a igated by **[**the Data Protection Officer, <<insert nam **AND/OR [**<<insert details of the individuals and/or de >>.**] [**Any breach which is either known or suspected a shall be reported to the Data Protection Officer, << details>>.**]**

2.16 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.**]**

2.17 All Users must repor ncerns relating to data that is not stored on the IT Syst Data Protection Officer, <<insert name and contact insert details of the individuals and/or department(s) such concerns relate in any way to personal data, su **OR [**instead**]** be reported to the Data Protection Offic

3. **Department Responsibiliti**

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

a) ensuring that sessed and deemed suitable for compliance w ity 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 of the IT-related requirements of this Policy an n, regulations, and other relevant rules whether orce including, but not limited to, the Data Prot e Computer Misuse Act 1990.

3.2 **[**The Data Protectior and contact details>>**] AND/OR [**<<insert details of t partment(s) responsible>>**]** shall be responsible for th

a) ensuring that systems and methods are assessed and mpliance with the Company's security requi

b) ensuring that within the Company are effectively im reviewed, working in consultation with the Com nt **[**and Data Protection Officer, as appropriat ome of such reviews to the Company's se

c) ensuring that of the non-IT-related requirements elated legislation, regulations, and other rele or in the future in force including, but not limited Legislation.

3.3 The IT Staff shall be ving:

a) assisting all U nd complying with the IT-related aspects of thi

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>>**]**.

3.4 **[**The Data Protection… …nd contact details>>**] AND/OR [**<<insert details of th… …artment(s) responsible>>**]** shall be responsible for th…

a) assisting all U… …nd complying with the non-IT-related aspec…

b) providing all U… …pport and training in data security matte…

c) ensuring that … …els of access to data that are appropriate fo… …account their job role, responsibilitie… …ity requirements;

d) receiving and… …ning non-IT-related data security matters and t… …in response **[**including, in the event that any… …al data, informing the Data Protection Of…

e) taking proacti… …e, to establish and implement security proce… …vareness; and

f) assisting **[**<<i… …e managers" or "department heads">>**] AN**… …on Officer**]** in monitoring data security within… …g all necessary action to implement thi… …s made to this Policy in the future.

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… …only within the bounds of UK law and must not use th… … any purpose or activity which is likely to contravene a… …or in the future in force.

4.3 Users must immedia… …ment and/or **[**the Data Protection Officer, <<insert nam… …**] AND/OR [**<<insert details of the individuals and/or de… …>>.**] AND/OR [**(and, where such concerns relate to p… …Protection Officer)**]** of any and all security concerns rel… …r data.

4.4 Users must immedi… …partment of any other technical problems (including, … …ware 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 o… …ding, but not limited to, operating systems, individual s… …d 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 sha 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 in 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, fi 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 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 scan 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 cess 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 s 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 ver possible and practical, be physically secured i locking mechanism. Where the design of the hardw ases shall be locked to prevent tampering with or the s.

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

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

8. Organisational Security

8.1 All Users handling da rsonal data) personal data will be appropriately trained

8.2 All Users handling d rsonal data) will be appropriately

supervised.

8.3 All Users handling da sonal data) shall be required and encouraged to exerc discretion when discussing work-related matters that r ner in the workplace or otherwise.

8.4 Methods of collecti essing data (and in particular, personal data) shall d reviewed.

8.5 All personal **[**and no the Company shall be reviewed periodically, as set o Retention Policy.

8.6 The performance of personal data shall be regularly evaluated and review

8.7 All Users handling pe d to do so in accordance with the principles of the Da n and the applicable Company Policies by contract.

8.8 No data, personal shared informally and if a User requires access to a erwise, that they do not already have access to, su ormally requested from <<insert name(s) and/or posit s>>.

8.9 No data, personal or sferred to any unauthorised User without the authorisa s) and/or position(s) and contact details>>.

8.10 All data must be h l times and should not be left unattended or on vie or other parties at any time.

9. Access Security

9.1 Access privileges for shall be determined on the basis of Users' levels of au any and the requirements of their job roles. Users shal to any IT Systems or data which are not reasonably re f their job roles.

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

9.3 All passwords must, puter, or device allows:

a) be at least << ers long;

b) contain a com lower case letters / numbers / spaces / sym

c) be changed a erval>> days;

d) be different fr d;

e) not be obviou birthdays or other memorable dates, memor laces etc.); and

f) be created by

9.4 Passwords should b User. Under no circumstances should a User share nyone, including the IT Manager

and the IT Staff. N ely asked for their password by anyone at any time should be refused. If a User has reason to believe th s obtained their password, they should change their and report the suspected breach of security to the IT D personal data could be accessed by an unauthorised i ction Officer**]]**.

9.5 If a User forgets thei e reported to the IT Department. The IT Department w eps to restore the User's access to the IT Systems w 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.

9.6 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

9.7 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).

9.8 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 ar. Users may not alter this time period.

9.9 Users may not use allow outside parties to access the IT Systems with t 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

9.10 **[**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

10. Data Storage Security

10.1 All data stored in el rticular personal data, should be stored securely usin ert type(s) of encryption>>**]** data encryption.

10.2 All data stored in h tronically on removable physical media, and in particu d be stored securely in a locked box, drawer, cabinet,

10.3 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 **]**.

10.4 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

11. Data Protection

11.1 All personal data c essed by the Company will be collected, held, and rdance with the principles of the Data Protection Leg f the Data Protection Legislation and the Company's D

11.2 All Users handling d 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 nd/or other data covered by this Policy must b ert type(s) of encryption>>**]**;

b) All emails co nd/or other data covered by this Policy must b

c) Personal dat overed by this Policy may be transmitted o ly; transmission over unsecured networks is n rcumstances;

d) Personal dat ered by this Policy may not be transmitted o there is a wired alternative that is reasonably pr

e) Personal data ed by this Policy contained in the body of an e ceived, should be copied directly from the bod tored securely. The email itself should be de associated therewith should also be deleted **[**u deletion>>**]**;

f) All personal covered by this Policy to be transferred p on removable electronic media, shall be trans iner marked "confidential".

g) Where any p r data covered by this Policy is being viewed nd the computer in question is to be left unatte f time, the User must lock the computer and

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

12. **Deletion and Disposal of Data**

12.1 When any data, and a, is to be erased or otherwise disposed of for any r opies have been made and are no longer needed), it d and/or disposed of using <<insert method(s)>>.

12.2 For further informatio sposal of personal data, please refer to the Company .

13. **Internet and Email Use**

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

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

14. **Reporting Security Breach**

14.1 Subject to paragrap estions, suspected breaches, or known breaches that s shall be referred immediately to **[**<<insert specific na rtment**] OR [**the IT Manager**] OR [**a member of the IT

14.2 Subject to paragrap estions, suspected breaches, or known breaches tha covered by this Policy shall be referred immediately me>>**] OR [**The Data Protection Officer**] AND/OR [**< ndividuals and/or department(s) responsible>>**]**.

14.3 All concerns, questio , or known breaches that involve personal data shall ly to the **[**The Data Protection Officer**] OR [**<<ins ividual(s) and/or department(s) responsible>>**]** who s accordance with the Company's Data Protection Polic

14.4 Upon receiving a c of a breach, the individual or department respons ert period>>, assess the issue including, but not lim associated therewith, and shall take any and all such ry to respond to the issue.

14.5 Under no circumstan pt to resolve a security breach on their own without firs individual or department **[**(or the Data Protection Offi ers may only attempt to resolve security breaches un d with the express permission of, the <<insert details o department(s) responsible>>, as appropriate.

14.6 All security breaches hall be fully documented.

15. **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 <<i dividual(s) and/or department(s) responsible>>, as appropria rotection Officer, <<insert name and contact details>>**]**.

16. **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: