

<< >>

1. Introduction

This document sets out the policy to be followed by all employees of <<insert Company name>> (the “Company”) in order to protect the Company’s data, information, services, infrastructure, computing environment and any and all IT Systems from damage and threats whether 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 in compliance with relevant Company Policies.
- 2.3 All employees of the Company who use the IT Systems including contractors and sub-contractors (collectively, “Users”) must adhere to and comply with this Policy and any other relevant policies.
- 2.4 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 2.3.
- 2.5 All data stored on IT Systems must be stored securely in compliance with all relevant parts of the Data Protection Legislation. “Data Protection Legislation” means all data protection and privacy laws including, but not limited to, the Data Protection Regulation ((EU) 2016/679) in England and Wales, the Data Protection Act 2018 in the European Union, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.
- 2.6 All data stored on IT Systems must be classified appropriately (including, but not limited to, personal data, and confidential information) [with reference to the classification system/procedure etc. if appropriate>>]. All data must be handled appropriately in accordance with its classification.
- 2.7 All data stored on IT Systems must be accessible only to those Users with a legitimate need for access.
- 2.8 All data stored on IT Systems must be protected against unauthorised access.
- 2.9 All data stored on IT Systems must be protected against loss and/or corruption.
- 2.10 All IT Systems are to be maintained, serviced, repaired, and upgraded by <<insert Company name>> (the “IT Department”) or by such third party as the IT Department may from time to time authorise.

S

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

2.12 All breaches of security of IT Systems or any data stored thereon shall be promptly investigated by the IT Department. [Any breach known or suspected to involve personal data shall be reported to the Data Protection Officer, <<insert name and contact details>>]

2.13 All Users must report any concerns relating to the IT Systems or the data stored thereon to the IT Department. [If any such concerns relate in any way to personal data, such concerns must [also] **OR** [instead] be reported to the Data Protection Officer.]

3. IT Department Responsibilities

3.1 The IT Manager, <<insert name and contact details>>, shall be responsible for the following:

- a) ensuring that the IT Department is assessed and deemed suitable for compliance with the relevant security requirements;
- b) ensuring that the IT Department within the Company are effectively implemented and working in consultation with the relevant Data Protection Officer, as appropriate,] and that the outcome of such reviews to the Company's security requirements;
- c) ensuring that the IT Department are aware of the requirements of this Policy and of the relevant regulations, and other relevant rules whether or not in force including, but not limited to, the Computer Misuse Act 1990.

3.2 The IT Staff shall be responsible for the following:

- a) assisting all Users and complying with this Policy;
- b) providing all Users with support and training in IT security matters and understanding;
- c) ensuring that the levels of access to IT Systems that are appropriate to their job role, taking into account their job role, responsibilities and security requirements;
- d) receiving and responding to reports relating to IT security matters and taking appropriate action [including, in the event that any reports are received by the Data Protection Officer];
- e) taking proactive measures to establish and implement IT security procedures and awareness;
- f) assisting the IT Manager in bringing all IT security within the Company and ensuring that the Company is able to implement this Policy and any changes to it in the future; and
- g) ensuring that the security of all data stored within the IT Systems at intervals of <<insert interval>> and that such backups are stored securely [onsite] **AND/OR** [offsite]. All backups should be encrypted using <<insert type(s) of encryption>>].

A

M

P

L

E

S

4. Users' Responsibilities

- 4.1 All Users must comply with the provisions of this Policy at all times when using the IT Systems.
- 4.2 All Users must use the IT Systems within the bounds of UK law and must not use the IT Systems for any activity which is likely to contravene any UK law whether or not it is a criminal offence.
- 4.3 Users must immediately report any concerns [(and, where such concerns relate to personal data, the Data Protection Officer)] of any and all security concerns relating to the IT Systems to the IT Department.
- 4.4 Users must immediately report any problems (including, but not limited to, hardware failures and software errors) to the IT Department.
- 4.5 Any and all deliberate breaches of this Policy by Users will be handled as appropriate under disciplinary procedures.

A

5. Software Security Measures

- 5.1 All software in use on IT Systems, including, but not limited to, operating systems, individual software applications and any and all intermediate releases, will be kept up-to-date with the latest patches, fixes, and other updates at the sole discretion of the IT Department. This includes 'major releases' (e.g. Windows 2.0), only to updates within a major release (e.g. from version 1.0.1 to version 2.0). Unless a security flaw is identified, it will be classed as a major release and outside the scope of this provision.
- 5.2 Where any security flaw is identified in software that will be either fixed immediately or withdrawn from the IT Systems until the flaw is remedied. [If the security flaw affects any personal data, the Data Protection Officer should be notified immediately.]
- 5.3 No Users may install software on IT Systems supplied on physical media without the approval of the IT Manager. All software must be approved by the IT Manager and may not be installed if it poses a security risk to the IT Systems or would not breach any licence agreements to which the IT Systems are subject.
- 5.4 All software will be installed on 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 specify which software may be installed and onto which computer it may be installed.

M

P

L

6. Anti-Virus Security Measures

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

E

S

6.2 All IT Systems protected by anti-virus software will be subject to a full system scan at least <<insert>> times per week.

6.3 All physical media (floppy disks or disks of any kind) used by Users for transferring files to or from the Company's network shall be scanned before any files may be transferred. Such scanning shall be performed [automatically upon connection / insertion by the User] **OR** [by the IT Staff / Manager].

6.4 Users shall be permitted to use cloud storage systems only with the approval of the IT Department. Files downloaded from any cloud storage system must be scanned before the download process.]

6.5 Any files being sent to or from the Company, whether by email, instant messaging, or shared cloud storage) must be scanned for viruses as part of the sending process, as appropriate. [All email attachments shall be scanned automatically upon sending.]

6.6 Where any virus is detected on a User's computer, the User must be reported immediately to the IT Department (or the IT Manager where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any necessary action to remove the virus from the system. In limited circumstances this action may involve the temporary removal of the affected computer or device. Wherever possible a replacement computer or device will be provided to the User [or the User's home computer >>] to limit disruption to the User. [If any virus or other malware is detected on a User's computer, the User must be reported immediately to the IT Department (or the IT Manager where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any necessary action to remove the virus from the system. In limited circumstances this action may involve the temporary removal of the affected computer or device. Wherever possible a replacement computer or device will be provided to the User [or the User's home computer >>] to limit disruption to the User.

6.7 [If any virus or other malware is detected on a User's computer, the User must be reported immediately to the IT Department (or the IT Manager where the anti-virus software automatically fixes the problem). The IT Department shall promptly take any necessary action to remove the virus from the system. In limited circumstances this action may involve the temporary removal of the affected computer or device. Wherever possible a replacement computer or device will be provided to the User [or the User's home computer >>] to limit disruption to the User.

6.8 Where any User delivers a file containing malicious software or virus to the Company's network under the Computer Misuse Act 1990 and will be subject to disciplinary procedures under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1 Wherever practical, all IT Systems shall be securely locked when not in use or not (with appropriate access by means of a key, smart card, door code, etc.) and access to such locations is restricted, Users must not allow 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, network infrastructure) shall be located in secure, climate-controlled rooms and/or in locked cabinets and accessed only by designated members of the IT Department.

7.3 No Users shall have access to IT Systems not intended for normal use by Users (including, but not limited to, servers, network infrastructure) without the express permission of the IT Department. In exceptional circumstances, whenever a problem with such IT Systems is reported by a User, that problem must be reported to the IT Department and the IT Manager should a User attempt to rectify any such problem without express permission (and, in most cases, instruction and approval of the IT Manager).

7.4 All non-mobile devices shall be limited to, desktop computers,

A

M

P

L

E

S

workstations, and
physically secured i
design of the hardw
tampering with or the

ver possible and practical, be
locking mechanism. Where the
ases shall be locked to prevent
s.

7.5 All mobile devices (including smartphones) provided to Users should always be transported securely and handled in a manner that ensures they are not left unattended. If mobile devices are to be left unattended, they should be stored in a suitable container. Users must make reasonable efforts to avoid such situations at any location [other than their private homes or Companies]. If a mobile device is to be left in a vehicle it must be stored in a locked compartment.

mitted to, laptops, tablets, and
should always be transported
ances where such mobile devices
ed inside a lockable case or other
reasonable efforts to avoid such
at any location [other than their
such mobile device is to be left in
nd, where possible, in a locked

7.6 The IT Department shall maintain an asset register of all IT Systems. All IT Systems shall be recorded in the asset register.

asset register of all IT Systems.
responding data shall be kept on

8. Access Security

8.1 Access privileges for IT Systems shall be determined on the basis of Users' levels of authority within the Company. Users shall not be granted access to IT Systems or electronic data which are not reasonably required for the performance of their job roles.

determined on the basis of Users'
requirements of their job roles.
Systems or electronic data which
of their job roles.

8.2 All IT Systems (and associated devices including, but not limited to, laptops, tablets, and mobile phones) shall be protected with a secure password or passcode, or such other security measure as the IT Department may deem appropriate. All forms of biometric log-in are considered secure. Only those log-in methods approved by the IT Department may be used.

ices including, but not limited to,
protected with a secure password
g-in system as the IT Department
all forms of biometric log-in are
roved by the IT Department may

8.3 All passwords must, when used to log-in to a computer, or device allows:
a) be at least << characters long;
b) contain a combination of upper case letters / numbers / lower case letters / numbers / spaces / symbols;
c) be changed at an interval >> days;
d) be different from previous passwords;
e) not be obvious (e.g. birthdays or other memorable dates, memorable places etc.); and
f) be created by the User. Under no circumstances should a User share their password with anyone, including the IT Manager and the IT Staff. No User should be asked for their password by anyone at any time. If a User has obtained their password, they should be refused. If a User has reason to believe that their password has been obtained, they should change their password and report the suspected breach of security to the IT Department. If a User's personal data could be accessed by an unauthorised individual, the IT Manager shall be notified [by the Information Officer].

puter, or device allows:
ers long;
lower case letters / numbers /
erval>> days;
d;
birthdays or other memorable
laces etc.); and

8.4 Passwords should be changed regularly. Under no circumstances should a User share their password with anyone, including the IT Manager and the IT Staff. No User should be asked for their password by anyone at any time. If a User has reason to believe that their password has been obtained, they should change their password and report the suspected breach of security to the IT Department. If a User's personal data could be accessed by an unauthorised individual, the IT Manager shall be notified [by the Information Officer].

User. Under no circumstances
nyone, including the IT Manager
ely asked for their password by
should be refused. If a User has
s obtained their password, they
and report the suspected breach
personal data could be accessed
ction Officer]].

8.5 If a User forgets their password, they should report this to the IT Department. The IT Department will then take the necessary steps to restore the User's access to the IT Systems and issue a temporary password.

be reported to the IT Department.
steps to restore the User's access
ssuing of a temporary password

A

M

P

L

E

E

member of the IT Staff responsible must be set up by the User the IT Systems.

- is possible to remember them. If a
ould be stored securely (e.g. in a
ase) and under no circumstances
s to see (e.g. by attaching a note

- devices (e.g. mouse, keyboard, etc.) are possible, with a password prompt after <<insert time period>> of inactivity. Users and Users may not be able to use screensaver will not interrupt or prevent any work on the computer (e.g. data

- limited to, laptops, tablets, and
may be set to lock, sleep, or similar,
requiring a password, passcode, or
similar. Users may not alter this time

- allow outside parties to access
nt of the IT Manager. Any such
User for the performance of their
eared by the IT Manager [and,
cessible by the outside party, the

- including, but not limited to, laptops, specific network name(s), if subject to the approval of the IT requirements provided by the IT devices when connected to the times. Users' use of their own, all relevant Company Policies those devices are connected to part of the IT Systems. The IT of the immediate disconnection of

L

- should be stored securely using data encryption.

- media, and in particular personal
box, drawer, cabinet, or similar.

- mobile device (including, but not
whether such device belongs to
nal written approval of the Data
approval, strictly in accordance
at the time the approval is given,
1).

- should be transferred to any

computer or device p
is a contractor or su
User has agreed to
and the Data Protect

User unless the User in question
behalf of the Company and that
company's Data Protection Policy

10. Data Protection

10.1 All personal data (a
held, and processed
strictly in accordance
provisions of the D
Protection Policy.

Protection Legislation) collected,
e collected, held, and processed
e Data Protection Legislation, the
tion and the Company's Data

10.2 All Users handling d
and must comply with
at all times. In particu

the Company shall be subject to,
Company's Data Protection Policy
apply:

a) All emails cor
type(s) of enc

must be encrypted [using <<insert

b) All emails cor

must be marked "confidential";

c) Personal da
transmission
circumstance

d over secure networks only;
rks is not permitted under any

d) Personal da
is a wired alte

over a wireless network if there
y practicable;

e) Personal da
received, sho
stored secure
associated th
deletion>>];

y of an email, whether sent or
from the body of that email, and
ld be deleted. All temporary files
eleted [using <<insert method of

f) All personal
removable ele
marked "conf

d physically, including that on
transferred in a suitable container

g) Where any co
screen and th
period of tim
leaving it.

ta is being viewed on a computer
is to be left unattended for any
he computer and screen before

10.3 Any questions relat
Protection Officer,] <

should be referred to [the Data
t details>>].

11. Internet and Email Use

11.1 All Users shall be s
Company's Commu
Systems.

mply with, the provisions of the
Internet Policy when using the IT

11.2 Where provisions in
ensure IT security
requirements impos
Users must take suc

additional steps to be taken to
t or email over and above the
ons, Email and Internet Policy,

12. Reporting IT Security Breaches

- 12.1 Subject to paragraph 12.2, any questions, suspected breaches, or known breaches shall be reported immediately to [<<insert specific name>>] OR [the IT Department] OR [a member of the IT Staff].
- 12.2 [All concerns, questions, or known breaches that involve personal data shall be reported to the Data Protection Officer who shall handle the matter in accordance with the Company's Data Protection Policy.]
- 12.3 Upon receiving a question or suspected breach, the IT Department shall, within <<insert period>>, investigate the breach, including, but not limited to, the level of risk associated with the breach and take any and all such steps as the IT Department deems appropriate to resolve the issue.
- 12.4 Under no circumstances shall the IT Department attempt to resolve an IT security breach on their own. Only the Data Protection Officer, and the Data Protection Officer may only attempt to resolve IT security breaches under the express permission of, the IT Department.
- 12.5 All IT security breaches shall be reported by the IT Department or by a User under the IT Department's supervision and fully documented.

13. Policy Review

The Company shall review this Policy <<insert interval>> and otherwise as required in order to ensure it is up-to-date and fit for purpose. All questions, concerns, and suggestions relating to this Policy should be communicated to the IT Manager and contact details>> [and/or the Data Protection Officer, <<insert details>>].

14. Implementation of Policy

This Policy shall be deemed to have been in effect from the start date>>. No part of this Policy shall have retroactive effect prior to matters occurring on or after this date.

This Policy has been approved by:

Name: <<insert full name>>

Position: <<insert position>>

Date: <<insert date>>

Due for Review by: <<insert date>>

Signature: