

S

A

me>> (“the Company”) with
f data subject, e.g. website
ts”) in respect of their personal
the Act, “personal data” is
be identified from that data or
tion of, or is likely to come into
(context), and includes any
of the intentions of the data

M

by the Company, its employees, or the Company.

D

but also to the spirit of the law
handling of all personal data,
as with whom it deals.

P

er as a data controller under the
Section 19 of the Act.

P

1

It sets out eight principles with
personal data:

- L

at at least one of the following

- # E

consent to the processing;

the performance of a contract to
for the taking of steps at the
to entering into a contract;

liance with any legal obligation to
other than an obligation imposed

to protect the vital interests of the

E

- Page 2 of 10

S

A

M

P

L

E

2.1.13 The processing of personal data for the exercise of a function of the Crown

2.1.14 The processing of personal data by a person as a result of an agreement made by such an organisation, or any other person of sensitive personal data necessary for the purposes of preventing fraud;

2.1.15 The processing of personal data by a health professional who in the circumstances owes a duty of confidentiality to that person who is necessary for the purposes of preventing fraud;

2.1.16 The processing of personal data as to racial or ethnic origin for the purpose of monitoring the absence of equality of treatment between persons of different racial or ethnic origin to be promoted by the State, provided that appropriate safeguards for the rights and freedoms of data subjects are in place.

2.3 Must be obtained only for specified purposes and shall not be processed for any other purpose than those specified in any manner which is incompatible with those purposes;

2.4 Must be adequate, relevant and not excessive in relation to the purposes for which it is processed;

2.5 Must be accurate and, where necessary, up to date;

2.6 Must be kept for no longer than is necessary for the purposes for which it is processed;

2.7 Must be processed in accordance with the provisions of this Part, which, see Part 3 of this Policy;

2.8 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures;

2.9 Must not be transferred to a third country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

administration of justice, for the House of Parliament, for the exercise of a function of the Crown, a minister of the Crown, or a member of the House of Commons;

of sensitive personal data by a person as a result of an agreement made by such an organisation, or any other person of sensitive personal data necessary for the purposes of preventing fraud;

ical purposes and is undertaken by a health professional who in the circumstances owes a duty of confidentiality to that person who is necessary for the purposes of preventing fraud;

al data consisting of information as to racial or ethnic origin for the purpose of monitoring the absence of equality of treatment between persons of different racial or ethnic origin to be promoted by the State, provided that appropriate safeguards for the rights and freedoms of data subjects.]

oses and shall not be processed for any other purpose than those specified in any manner which is incompatible with those purposes;

respect to the purposes for which it is processed;

date;

t of the purpose(s) for which it is processed;

data subjects under the Act (for the purposes of this Part);

ful processing, accidental loss, destruction or damage through appropriate technical and organisational measures;

tside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

S

A

- # M

For personal data that is likely to be sensitive, data subjects should make any request for access in writing, stating their position and contact details>> The controller must either notifying the data subject or the data subject feels that any aspect of the

Automated means (where such a subject) and to be informed the data subject has the right to reconsider the decision;

sed by the Company's breach of

P

a living individual who can be identified by information which is in the possession or control of the data controller, and includes any information relating to the intentions of the data controller in relation to the individual.

ata relating to the racial or ethnic
us (or similar) beliefs; trade
their sexual life; the commission
edings for any offence
disposal of such proceedings or

ant to its dealings with a given
ed in accordance with the data
a may be collected, held and

- description of the reason that the

F

- [<<add more as require

Any and all personal data collected collected in order to ensure that the customers, and can work effectively manage its employees, contractors personal data in meeting certain ob

Personal data may be disclosed with this Policy. Personal data may be processed with the data protection principles and data be passed to any department or reasonably require access to that personal data was collected and is being processed.

- All personal data collected by any party is collected and

- # SAMPLE

es, certain information gathered
on will nonetheless be collected,

ed such disclosure complies with
ment to another in accordance
circumstances will personal
e Company that does not
t to the purpose(s) for which it

and on behalf of the Company by
lawfully;

the reasons for the collection of
se(s) for which the data will be

is necessary to fulfil the

tion and kept accurate and up to

ecessary in light of the purpose(s)

maintained and followed:

sed online by the Company, they
irements of the Privacy and
ng full details of cookie use and

the method of amending any data

by them online cannot be fully
ances (for example, because a file
ow to request that the Company
within the individual's right to do

S

- # A

or it is transmitted electronically or
 mod(s) including, where relevant,

European Economic Area (as
ation country offers adequate
nts of data subjects; and
th ease and without hindrance

M

contractors, or other parties
when working with personal

- P

networks only – transmission over
circumstances:

whether sent or received, and stored securely. The email associated therewith should also be

transmission the recipient should
should be waiting by the fax

copy form it should be passed
name(s) and/or type(s) of delivery

If an employee, agent, sub-
sidiary or the Company requires access to
the system, such access should be
granted based on the user's name, title
and/or position(s) and contact

electronic copies stored on
purely in a locked box, drawer,

F

S

without the authorisation of the Company and/or position(s) and contact details>>;

d/or position(s) and contact

- Personal data must be kept secure and should not be left unattended or on view to other parties at any time

mes and should not be left unattended, agents, sub-contractors or

- If personal data is being processed on a screen and the computer in question is to be left unattended for a period of time, the user must lock the computer and screen before leaving the desk

screen and the computer in question is to be left unattended for a period of time, the user must lock the

- Any unwanted copies of personal data (whether hardcopies or electronic duplicates) that are no longer needed should be securely destroyed. Hardcopies should be shredded and electronic copies should be securely deleted using a secure method(s)>>];

outs or electronic duplicates) that are no longer needed should be securely destroyed. Hardcopies should be shredded and electronic copies should be securely deleted using a secure method(s)>>];

- No personal data should be stored on any device (including, but not limited to, laptops, tablets, mobile phones, etc.) unless it has been approved by the Company or otherwise authorised by the Company. In the event of such approval, the device must be used strictly in accordance with the terms of the approval given, and for no other purpose

the device (including, but not limited to, laptops, tablets, mobile phones, etc.) unless it has been approved by the Company or otherwise authorised by the Company. In the event of such approval, the device must be used strictly in accordance with the terms of the approval given, and for no other purpose

- No personal data should be stored on any device (including, but not limited to, laptops, tablets, mobile phones, etc.) unless it has been approved by the Company or otherwise authorised by the Company. In the event of such approval, the device must be used strictly in accordance with the terms of the approval given, and for no other purpose

device personally belonging to an employee and personal data belonging to the Company must be stored on devices belonging to the Company where the device is used on behalf of the Company where the device is used with the letter and spirit of this Policy and of the Act (where applicable) and for no other purpose. It is the responsibility of the employee demonstrating to the Company that all necessary measures have been taken);

- All personal data stored on any device (including, but not limited to, laptops, tablets, mobile phones, etc.) must be backed up <<insert interval>> and stored securely. All backups should be encrypted and stored securely using passwords and encryption;

backed up <<insert interval>> and stored securely. All backups should be encrypted and stored securely using passwords and encryption;

- All electronic copies of personal data must be stored securely using passwords and encryption;

stored securely using passwords and encryption;

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that are easily guessed or otherwise predictable. All passwords should be a combination of uppercase and lowercase letters, numbers and special characters. Software used by the Company is

should be changed regularly and should not use words or phrases that are easily guessed or otherwise predictable. All passwords should be a combination of uppercase and lowercase letters, numbers and special characters. Software used by the Company is

- Under no circumstances should personal data be written down or shared with other parties working on behalf of the Company, irrespective of whether the data is written down or shared. If a password is forgotten, it must be reset using a secure method. IT staff do not have access to passwords;

be written down or shared with other parties working on behalf of the Company, irrespective of whether the data is written down or shared. If a password is forgotten, it must be reset using a secure method. IT staff do not have access to passwords;

- All personal data held by the Company should be regularly reviewed for accuracy and completeness. Where necessary, regular contact with data subjects, should be confirmed at least <<insert interval>>. If a

regularly reviewed for accuracy and completeness. Where necessary, regular contact with data subjects, should be confirmed at least <<insert interval>>. If a

A

M

P

L

E

inaccurate, it should be
any personal data is no
deleted and disposed of

- Where personal data held for marketing purposes, it shall be the responsibility of the relevant department to ensure that details>> to ensure that marketing preference details are up to date. The Preference Service, the Telephone Preference Service, and the Fax Preference Service should be checked at least <<insert interval>>.

7. Organisational Measures

The Company shall ensure that the measures taken with respect to the collection, holding and processing of

- The Company has appointed a Data Protection Officer as its Data Protection Officer, responsible for overseeing data protection compliance with this Policy and with the Data Protection Act. The Data Protection Officer shall be responsible for:
 - Overseeing the implementation of the Policy, in conjunction with the relevant departments, agents, contractors and other parties working on behalf of the Company;
 - Organising suitable training and awareness programmes within the Company;
 - Reviewing this Policy at least annually, or at intervals not less than <<insert interval>>;
 - <<insert further responsibilities>>.
- All employees, agents, contractors and other parties working on behalf of the Company are made fully aware of their individual responsibilities and the Company's responsibilities under this Policy, and shall be provided with a copy of the Policy.
- Only employees, agents, contractors and other parties working on behalf of the Company that need to process personal data in order to carry out their assigned duties can access personal data held by the Company;
- All employees, agents, contractors and other parties working on behalf of the Company handling personal data shall be regularly trained to do so;
- All employees, agents, contractors and other parties working on behalf of the Company handling personal data shall be regularly supervised;
- Methods of collecting, holding, processing and disposing of personal data shall be regularly evaluated and reviewed;
- The Performance of the Policy shall be regularly monitored by the Company, and by contractors, or other parties working on behalf of the Company.

and immediately where possible. If the Company, it should be securely stored and disposed of (s)>>];

ed for marketing purposes, it shall be the responsibility of the relevant department to ensure that details>> to ensure that marketing preference details are up to date. The Preference Service, the Telephone Preference Service, and the Fax Preference Service, should be checked at least

taken with respect to the

/or position and contact details>> as its Data Protection Officer, responsible for overseeing data protection compliance with this Policy and with the Data Protection Act. The Data Protection Officer shall be responsible for:

liance with this Policy, working in conjunction with the relevant departments, agents and/or department heads, contractors and other parties working on behalf of the Company;

on training and awareness

es not less than <<insert

.

ies working on behalf of the Company are made fully aware of their individual responsibilities and the Company's responsibilities under this Policy, and shall be

er parties working on behalf of the Company that need to process personal data in order to carry out their assigned duties can access personal data held by the

ies working on behalf of the Company handling personal data shall be regularly trained to do so;

ies working on behalf of the Company handling personal data shall be regularly supervised;

personal data shall be regularly

ontractors, or other parties working on behalf of the Company. Personal data shall be regularly

- evaluated and reviewed
- All employees, agents, and contractors of the Company handling personal data shall be bound by the principles of the Act and the Policy
- All agents, contractors, and subcontractors handling personal data on behalf of the Company shall be bound by the same conditions as those relevant employees and shall be held to the same conditions as those relevant employees
- Where any agent, contractor, or subcontractor handling personal data on behalf of the Company shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings

ies working on behalf of the Company shall do so in accordance with the principles of the Act and the Policy

on behalf of the Company shall be bound by the same conditions as those relevant employees and shall be held to the same conditions as those relevant employees

ing on behalf of the Company shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings

8. Access by Data Subjects

A data subject may make a subject access request to the Company about the information which the Company holds about them.

- SARs should be made in writing to the Company at <<insert contact details>>
- A SAR [may be made using the Company's Subject Access Request Form, but does not have to be, and may be made by any person acting on behalf of the data subject]
- SARs must make it clear that the request is for subject access, the request or whether it is for subject access. Proof of identity must be provided by the individual making the request or the person acting on their behalf in their capacity to act on behalf of the data subject
- The Company currently charges a fee of <<insert fee>> payable by <<insert method of payment>> for each SAR, up to the legal maximum)

at any time to find out more about the information which the Company holds about them.

<insert name and/or position>>,
the Company's Subject Access Request Form, but it must be clearly identifiable as a SAR.

subject themselves that is making the request or whether it is for subject access. In either case, proof of identity must be provided by the individual making the request or the person acting on their behalf in their capacity to act on behalf of the data subject

the legal maximum) for each SAR, up to the legal maximum) shall be required for access to a

Upon receipt of a SAR the Company shall respond within which to respond fully[, but shall not exceed <<insert business days>>]. The following information shall be provided to the data subject:

- Whether or not the Company holds the information requested
- A description of any personal data held
- Details of what that personal data is
- Details of how to access the personal data
- Details of any third-party to whom the personal data is passed to; and
- Details of any technical information held

period of 40 calendar days from the date of receipt of SARs within which to respond fully[, but shall not exceed <<insert business days>>]. The following information shall be provided to the data subject:

all data on the data subject;

data subject;

how to keep it up to date;

onal data is passed to; and

9. Notification to the Information Commissioner

As a data controller, the Company is required to notify the Information Commissioner's Office of the following information:

Office of the Information Commissioner's Office of the Information Commissioner's Office

Office that it is processing personal data, registered in the register of data controllers, registration number: <<insert reference number>>.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify could result in a fine.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Data Protection Officer shall be responsible for monitoring and updating the Information Commissioner's Office.

registered in the register of data controllers, registration number: <<insert reference number>>.

Information Commissioner's Office on an annual basis. Failure to notify could result in a fine.

Information Commissioner's Office within 28 days of taking place.

g and updating the Information Commissioner's Office.

10. Implementation of Policy

This Policy shall be deemed effective from the date of implementation and shall thus apply retroactive effect and shall thus apply to all data processing activities carried out on or after this date.

No part of this Policy shall have retroactive effect and shall thus apply to all data processing activities carried out on or after this date.

This Policy has been approved & authorised by the Data Protection Officer.

Name: <<insert full name>>

Position: <<insert position>>

Date: <<insert date>>

Due for Review by: <<insert date>>

Signature:

S
A
M
P
L
E