

S

1. **Introduction**

This Policy sets out the registered in <<insert company registration number>>, with the Company”) regarding data protection Legislation (defined below)

This Policy also provides guidance of data subject access requests. The procedures and principles must be followed at all times by the Company, its employees, and other parties working on behalf of the Company.

Company name>>, a company registered under number <<insert company registration number>>, with its office is at <<insert address>> (“the Company”) regarding data protection Legislation (defined below)

2. **Definitions**

“data controller”

person or organisation which, alone or with others, determines the purposes of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data used in the business;

“data processor”

person or organisation which processes personal data on behalf of a data controller;

“Data Protection Legislation”

all applicable data protection and privacy legislation, including, but not limited to, the Data Protection Act 2018, and any applicable national laws, regulations, and secondary legislation in England and Wales governing the processing of personal data, the privacy of electronic communications, as amended, replaced, or otherwise from time to time;

“data subject”

any living, identified, or identifiable individual about whom the Company holds personal data;

“personal data”

any information relating to a data subject which can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;

A

M

P

L

E

“processing”

“special category person

### 3. Data Protection Officer &

3.1 The Company’s Data Protection Officer (<<insert name of data protection officer>>), <<insert name of Data Protection Officer>>, is responsible for administering and implementing applicable related procedures, and/or handling requests are handled for ensuring that all on behalf of the Company in accordance with the Data Protection Legislation and their

3.2 The Company collects <<insert type(s) of data subject>>. The Company is a ‘data controller’ under the Data Protection Legislation.

3.3 Data subjects have the right under the Data Protection Legislation (Article 15 of the UK GDPR) to request the Company collect, hold, process and to obtain a copy of their personal information. The right is designed to help data subjects to understand how and why their personal data is processed lawfully.

3.4 This Policy is an information handling data subject access policy, privacy policy, privacy notice, and is not designed to be made available to third parties (not limited to, data subjects). This Policy should, where applicable, be read in conjunction with the Company’s Data Protection Policy and other applicable policies<>].

3.5 Any questions relating to the collection, processing, or holding of personal data should be referred to the Data Protection Officer.

3.6 Parts 1 to 4 and Part 5 apply to staff and Part 6 apply to staff author

S

A

M

P

L

E

operation or set of operations on personal data or sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, communication by transmission, dissemination or otherwise making available, alignment or restriction, erasure or destruction and

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life, sexual orientation, genetic data.

<<insert name of data protection officer>>. The Data Protection Officer is responsible for developing and implementing any policies (referred to in this Policy), ensuring that all data subject access requests are handled in accordance with the Data Protection Legislation; and ensuring that all contractors, or other parties working on behalf of the Company, have a clear understanding of the Data Protection Legislation and that it applies to their job role(s).

The Company processes personal data about <<insert type(s) of data subject>>, such as business contacts etc.>>. The purposes of the Data Protection Legislation are to

ensure that individuals have their personal data under the Data Protection Legislation. Specifically with the right of access, data subjects have the right to find out whether the Company holds personal data about them, the right to request a copy of that data and certain other supplementary information designed to help data subjects to understand how and why their personal data is processed and to check that we are doing so lawfully.

This Policy is designed to provide guidance on how the Company handles personal data. It is not a data protection policy, privacy policy, privacy notice, and is not designed to be made available to third parties (not limited to, data subjects). This Policy should, where applicable, be read in conjunction with the Company’s Data Protection Policy and other applicable policies<>].

Any questions relating to the Company’s collection, processing, or holding of personal data should be referred to the Data Protection Officer.

Parts 1 to 4 and Part 5 apply to all staff and Parts 5 to 13 apply to staff author

S

4. **How to Recognise a Data Subject Access Request**

4.1 The Data Protection Act 1998 requires that a data subject access request must be made orally or in writing. A request can be made in any form of communication. A request must use the words 'subject access request', 'data protection request' or 'data subject access request'. The request must be made to the Company of the UK GDPR (or the Data Protection Act 1998) and could receive a SAR if the request has been received.

st  
set out a particular format which a SAR ("SAR") must follow. A SAR may be made to the Company, and by any means of communication. The request must use the words 'subject access request', 'data protection request' or 'data subject access request'. The request must be made to the Company of the UK GDPR (or the Data Protection Act 1998) and could receive a SAR if the request has been received.

4.2 [The Company provides a Subject Access Request Form, available from the Company website, to data subjects to make a SAR and to make it easier for data subjects to recognise the request; however, data subjects are under no obligation to use the form and care must be taken at all times to identify SARs.

s Request Form, available from the Company website, to data subjects to make a SAR and to make it easier for data subjects to recognise the request; however, data subjects are under no obligation to use the form and care must be taken at all times to identify SARs.

4.3 SARs may instead be made to the Company via social media. The Company will treat such information you have provided in the same way as a message sent specifically to a 'subject access request' under the UK GDPR.

terminology, using terms such as 'subject access request'. For example, a message sent to the Company via social media should please provide details of all the information you have provided in the SAR and must be treated in the same way as a message sent specifically to a 'subject access request' under the UK GDPR.

4.4 Individuals may make a SAR via a third party.

half. It is also possible to make an SAR via a third party.

a) This may be done on behalf of a data subject by a third party. This may be one private individual or a company. It is permissible for a third party to make a request on behalf of the data subject concerned.

request on behalf of a client, or it may be made on behalf of another. This may be one private individual or a company. It is permissible for a third party to make a request on behalf of the data subject concerned.

b) In certain limited circumstances, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of a data subject who lacks mental capacity.

may not have the mental capacity to make a SAR. In these cases, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of that individual.

c) Adults, such as parents, may make SARs on behalf of children. The child's consent is not required. However, when dealing with a child it is important to consider whether that child is capable of understanding their rights. If so, a response should be provided to the child. It may, however, be permissible for a third party to exercise the child's right on their behalf with their authorisation, or if it is evident that doing so is in the child's best interests.

s, may make SARs on behalf of children. The child's consent is not required. However, when dealing with a child it is important to consider whether that child is capable of understanding their rights. If so, a response should be provided to the child. It may, however, be permissible for a third party to exercise the child's right on their behalf with their authorisation, or if it is evident that doing so is in the child's best interests.

4.5 When a SAR is identified, you are in anyway to ensure that the request is forwarded to the relevant department(s) details>>[, or to <<insert contact details>>] as set out below in Part 5.

ication or request is received and you are in anyway to ensure that the request is forwarded to the relevant department(s) details>>[, or to <<insert contact details>>] as set out below in Part 5.

5. **What to do When a Subject Access Request is Received**

**What to do When a Subject Access Request is Received**

5.1 The Company has a process in place to ensure that it is important to act on a SAR as soon as possible.

h which to respond to a SAR, so it is important to act on a SAR as soon as possible.

A

M

P

L

E

S

5.2 Unless you are authorised to do so, it must be forwarded to the Data Protection Officer [or <<insert job title(s) and/or department(s)>>] immediately, as set out in the policy with respect to any such information.

5.3 SARs may come in a variety of forms. Determine how to forward the SAR to the appropriate member of staff.

a) For SARs received via email or social media], the message [or a link, if appropriate] should be forwarded immediately to the Company's Data Protection Officer [or <<insert job title(s) and/or department(s)>>], or to <<insert job title(s) and/or department(s)>>.

b) For SARs received on any other hardcopy form, the SAR should first be scanned and then forwarded immediately to the Company's Data Protection Officer [or <<insert job title(s) and/or department(s)>>], or to <<insert job title(s) and/or department(s)>>. The original sent to the same recipient using a secure means possible (e.g. in person, by courier or by Royal Mail Special Delivery).

c) For SARs received by the data subject should be notified of the data subject's right to be informed of the Company's Data Protection Officer [or <<insert job title(s) and/or department(s)>>] for full details of their SAR. The information provided by the data subject should be forwarded to the Data Protection Officer [or <<insert job title(s) and/or department(s)>>] as soon as possible of the time and date on which the SAR was made.

5.4 The Company's Data Protection Officer [or <<insert job title(s) and/or department(s)>>] should send a confirming receipt of the SAR, within <<insert period, e.g. 5 working days>> of you sending it. If you do not receive a response within this time limit, you must contact them again to confirm receipt.

6. **Responding to a Subject's Request for Information: Identifying Data Subjects and Clarifying Requests**

6.1 Before responding to a request for information, steps must be taken to verify the identity of the individual making the request, and, particularly if the Company is processing a large amount of information about them, to clarify their request (i.e. to specify the information requested and the period to which their SAR relates). Information requests must be reasonable and proportionate. Individuals must be asked to provide any more information than is reasonably necessary to identify the individual. A request for clarification be used to narrow the scope of the request.

6.2 If additional information is required to confirm an individual's identity, the individual must be asked to provide it as soon as possible. If additional information is required, the time limit for a SAR does not begin until that information is received.

6.3 If additional information is required to identify the individual by the SAR, the individual must be asked to provide it as soon as possible. If additional information is required, the time limit for a SAR does not begin until that information is received. The time limit is measured from the date that a response is received.

A

M

P

L

E

S

on the same day, possible extensions

use is unchanged. (Note also the d in Part 8, below).

6.4 If a SAR is made by individual acting on sufficient evidence t

f a data subject (see Part 4.4), the subject must be required to provide to act on the data subject's behalf.

6.5 Examples of inform identity include (not unless it is necessa

requested to confirm an individual's documents should not be requested

- a) A copy of the
- b) A copy of the
- c) [ <insert ad

ce;

6.6 If, having requested still not possible to Company may refus

to verify an individual's identity, it is the individual does not comply), the as set out below in Part 11.

6.7 If, having requested not comply (e.g. do the Company must reasonable searches generally be possib required by the Data

to clarify a SAR, the individual does es to provide further information), comply with the SAR by making relating to the request. It will also all the supplementary information see below in Part 9).

6.8 The Company does to respond to a pote

for the sole purpose of being able

7. Responding to a Subject

Fee Fees

7.1 Under normal circ charging of a fee fo for SARs.

Protection Legislation prohibits the company does not normally charge

7.2 In limited cases, it is the administrative of unfounded', 'excess data following the S to comply with a SA

a 'reasonable fee' in order to cover a SAR if that SAR is 'manifestly ct requests further copies of their may also be permissible to refuse b).

7.3 The following factor

when calculating a reasonable fee:

- a) Administrative
  - a) Asses
  - b) Loca
  - c) Provi
  - d) Send
- b) Specific cost
  - a) Photo
  - b) Equip
  - c) Staff

Company is processing the data

cting that information;

ation; and

onse to the data subject.

de:

ge, and any other costs incurred to the data subject;

A

M

P

L

E

S

8. Responding to a Subject Request: Time Limits

- 8.1 Under normal circumstances, you must respond to a SAR 'without undue delay' and, as a general rule, all SARs must be responded to within one month of receipt. The date of receipt of the SAR is the due date for response.
- 8.2 Under the Data Protection Act 1998, the one-month period referred to in Part 8.1 begins on the first business day – that the request is received and ends on the first business day in the following month (or, if the following month does not have a corresponding day (e.g. January 31<sup>st</sup> to February), the first day of that month). [Consequently, the time limit set by Part 8.1 for responding to SARs is 28 calendar days.] If the last day of the one-month period falls on a weekend or bank holiday, the time limit is extended to the first business day following that day.
- 8.3 If additional information is requested from the individual making the SAR to confirm an individual's identity under Part 6.2, the time limit under Part 8.1 is paused until the information is received.
- 8.4 If additional information is requested from the individual making the SAR to clarify the SAR, as long as the information is relevant to the request, the time limit under Part 8.1 is paused until the information is received on the same day, in which case the time limit resumes on the day following receipt.
- 8.5 If the SAR is complex or if the subject makes a number of SARs, it is permissible to extend the time limit up to two months. If such an extension is necessary, the subject must be informed, in writing, of the reasons for the extension and the new one-month time limit.

A

M

9. Responding to a Subject Request: Information to be Provided

- 9.1 Data subjects must be provided with the following information in response to a SAR:
  - a) the purpose for which the Company collects, holds, and processes their personal data;
  - b) the categories of personal data held;
  - c) the recipient or categories of recipient to whom the Company discloses the personal data;
  - d) details of how long the personal data is retained or, if there is no fixed retention period, details of how long it will be retained;
  - e) details of the rights of the individual to request the Company to rectify or erase their personal data or to object to our processing of it;
  - f) details of the right of the individual to make a complaint to the ICO;
  - g) if any of the personal data was not obtained from the data subject, details of the source of the data;
  - h) if the Company has used automated decision-making (including profiling), details of the logic involved and the significance and envisaged consequences of such processing for the individual (also see Part 9.2); and

P

L

E

S

- i) if the Company transfers personal data to a third country or international organization, the safeguards in place to protect that data.

9.2 In cases where a data subject requests a SAR in relation to automated decision-making, the following shall apply:

- a) Where a SAR is received in relation to an automated decision underlying an automated decision that has been made in relation to important matters relating to the data subject, the data subject shall be provided with an explanation of the logic involved in the decision-making, including the following conditions:

- the decision-making process must be solely automated (i.e. there is no human involvement in the process); and
- the information shall be presented in such a way as to protect the Company's trade secrets and confidential information.

- b) The data subject shall be provided with information related to the automated decision-making process and shall be able to seek to exercise the right to human intervention. The data subject shall be able to appoint a person to review the automated decision on their own point of view about the decision, and the data subject making a SAR seeks to exercise the right to human intervention, the Company's department(s) responsible for SARs shall be named in accordance with the Data Protection Policy and applicable company policy / policies>>].

9.3 The information set out in 9.2 must be provided:

- a) in a concise, clear and plain language and easily accessible form, using plain language;
- b) in writing; [and if the data subject requests otherwise];
- c) if the data subject requests otherwise, used electronically (e.g. via email) [and] OR [.]
- d) [where possible, a secure system used to provide data subjects with access to the information, providing secure access for data subject.]

9.4 It is important to note that the Company is only entitled to access personal data that the Company processes in the process of responding to a SAR. The definition of "personal data" (see Part 1), the Data Protection Policy does not entitle the data subject to access it. In certain circumstances, it may be necessary to separate personal data from non-personal data in order to respond to a SAR.

## 10. Responding to a Subject's Request for Access to Personal Data: Locating Information

10.1 The Company holds personal data in the following location[s] and/or system[s]. It is important to identify the location[s] of personal data to which a SAR relates in order to respond to the SAR. The location[s] shall include the following place:

- a) <<insert list of location[s] and/or system[s] types of elements, including, for example, departments, systems etc. Also include data types, where relevant>>.

A

M

P

L

E

S

b) <<add further  
10.2 The Data Protection  
efforts' to find and  
access is not limited

the Company to make 'reasonable  
response to a SAR. The right of  
is easy to find.

11. **Refusing to Respond to a**

est

11.1 In certain cases, it  
SAR:

Company to refuse to comply with a

a) if it is not p  
requesting a

individual making the SAR after  
er Part 6.2; or

b) if the request  
into account  
request is re  
the context  
and the indiv  
to request a

d' or 'manifestly excessive', taking  
ing (but not limited to) whether the  
ature of the information requested,  
relationship between the Company  
t. In such cases, it is also possible  
e it, as set out in Part 7.2.

11.2 If either of the above  
the SAR must be  
individual making the  
The individual must  
of the possibility of s

Company's refusal to comply with  
ination must be provided to the  
lar month after receiving the SAR.  
r right to complain to the ICO and  
7.

11.3 Certain exemptions  
Protection Legislatio

s are also included in the Data  
2 for more information.

12. **Exemptions to the Right**

12.1 The Data Protection  
to SARs and there  
Those most likely to  
the personal data in

number of exemptions which apply  
y refusing to comply with a SAR.  
e Company are situations in which

a) subject to le

or

b) purely perso

hold activity; or

c) a reference  
employment

) in confidence for purposes of  
r

d) is processe  
purposes in  
extent that c  
business or

casting or management planning  
or other activity (but only to the  
would prejudice the conduct of the

e) consists of n  
employer an  
SAR would p

n respect to negotiations between  
the extent that complying with the  
ns); or

f) contains per

third party; or

g) is of a type l  
the apprehen  
or]

vention or detection of a crime, or  
offenders if it is disclosed[.] OR [;

h) [<<insert ad

ons>>.]

A

M

P

L

E





shall have retroactive effect  
this date.

ly to matters occurring on or after

This Policy has been approved and

**Name:** <<insert

**Position:** <<insert

**Date:** <<insert

**Due for Review by:** <<insert

**Signature:**

S

A

M

P

L

E