DATA PROTECTION POLICY

MARCH 2023

CAPITAL GEARING TRUST P.L.C

CONTENTS

1. INTRODUCTION

1.1. Capital Gearing Trust P.L.C. (the "**Company**", "**we**", "**our**", "**us**") obtains, keeps and uses personal data about data subjects (including shareholders, investors, potential shareholders or investors, business contacts, website users and directors or prospective directors) for a number of specific lawful purposes, as set out in the Company's privacy notice, which is available on our website at www.capitalgearingtrust.com.

1.2. This policy covers all personal data collected, processed and stored by or on behalf of the Company in the course of its activities, regardless of the media on which that data is stored.

1.3. The Company's advisers may process personal data on behalf of the Company. The Company's current advisers include:

1.3.1. CG Asset Management Limited (as investment manager);

1.3.2. The Northern Trust Company (as depositary, custodian and/or banker);

1.3.3. Juniper Partners Limited (as secretary and administrator); and

1.3.4. Computershare Investor Services PLC (as registrar).

The Company may also appoint other advisers and/or service providers from time to time who may process personal data on behalf of the Company.

1.4. Where this data protection policy refers to the processing of personal data by the Company, such reference shall include the processing of personal data on behalf of the Company by its service providers (including as detailed above) who are instructed to process such personal data in accordance with this policy.

1.5. This policy applies to the Company's board of directors (the "**Board**"), as well as the Company's advisers and any other service providers appointed by or on behalf of the Company from time to time to whom this policy is intimated and their respective employees, in each case who process and/or have access to personal data which is processed by or on behalf of the Company. In this policy, "**you**" refers to any of those persons who access and/or process personal data by or on behalf of the Company.

1.6. This policy sets out the Company's policies and procedures for complying with the data protection laws. Compliance with this policy is mandatory.

1.7. The correct and lawful treatment of personal data will maintain stakeholder confidence in the Company. Protecting the confidentiality and integrity of personal data is a critical responsibility that should be taken seriously at all times. The Company is exposed to potentially significant sanctions (including fines) for failure to comply with the provisions of the data protection laws (as defined below).

1.8. While the Board has delegated responsibility for the implementation of this policy to its service providers who conduct (amongst other things) the day-to-day administrative functions of the Company, the Board will oversee the Company's compliance with the data protection laws.

2. DEFINITIONS

In this policy, the following definitions apply:

"**criminal records information**"	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
"**data breach**"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
"**data protection laws**"	means all laws applicable from time to time relating to the processing of personal data and/or privacy in the UK, including to the extent applicable (a) the UK Data Protection Act 2018; (b) the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") as it forms part of the laws of the UK by virtue of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (the "**UK GDPR**"); (c) the GDPR; and (d) the Privacy and Electronic Communications Regulations 2003;
"**data subject**"	means the identified or identifiable individual to whom the personal data relates;
"**personal data**"	means information relating to an individual who can be identified (directly or indirectly) from that information;
"**processing**"	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**pseudonymised**"	means the process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that

	the personal data cannot be attributed to an identifiable individual; and
"**special category personal data**"	means personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3. DATA PROTECTION PRINCIPLES

3.1. Most obligations under the data protection laws fall on the "controller". It is the controller who determines the purposes and means of the processing of personal data and it is the controller who must also comply with various fundamental principles (explained in more detail below).

3.2. In the course of its daily activities, the Company (through its advisers and service providers) acquires, processes and stores personal data. To that extent, the Company is the controller of the personal data processed by or on behalf of the Company and accordingly has obligations under data protection laws.

3.3. The Company will comply with the following data protection principles when processing personal data:

3.3.1. we will process personal data lawfully, fairly and in a transparent manner;

3.3.2. we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

3.3.3. we will only process the personal data that is adequate, relevant and necessary for the relevant purposes for which it is processed;

3.3.4. we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay (having regard to the purposes for which such data is processed);

3.3.5. we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

3.3.6. we will process personal data in a manner that ensures that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage (including by using appropriate technical and organisational measures to protect personal data).

4. BASIS FOR PROCESSING PERSONAL DATA

4.1. In relation to any processing activity we will:

4.1.1. review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing. Guidance on the lawful bases for processing personal data is available on the ICO website (here). The lawful bases for processing personal data include:

(a) that the data subject has given clear consent to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject (such as the FCA Listing Rules and Disclosure Guidance and Transparency Rules);

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person (i.e. to protect that person's life);

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official functions, and the task or function has a clear basis in law; or

(f) that the processing is necessary for the purposes of the legitimate interests of the Company or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject - see paragraph 4.3 below.

4.1.2. satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose, including by anonymising personal data);

4.1.3. document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

4.1.4. include information about both the purposes of the processing and the lawful basis for it in our privacy notice;

4.1.5. where special category personal data is processed, also identify a lawful special condition for processing that information (see paragraph 5.2.2 below), and document it; and

4.1.6. where criminal records information is processed, also identify a lawful condition for processing that information, and document it.

4.2. Consent to processing personal data requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to process personal data for a different and incompatible purpose which was not disclosed to the data subject when the data subject first consented.

4.3. When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing it is best practice to:

4.3.1. conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision; and

4.3.2. keep the LIA under review, and repeat it if circumstances change.

4.4. Further information on conducting a LIA is available on the ICO website (here).

4.5. The Company must include information about the legitimate interests we rely upon to process personal data in our privacy notice(s).

5. SPECIAL CATEGORY PERSONAL DATA

5.1. Special category personal data is sometimes referred to as 'sensitive personal data'.

5.2. The Company may from time to time need to process special category personal data. We will only process special category personal data if:

5.2.1. we have a lawful basis for doing so as set out in paragraph 4.1.1 above, e.g. to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

5.2.2. one of the special conditions for processing special category personal data applies. Guidance on the lawful bases for processing special category personal data is available on the ICO website (here). The lawful bases for processing special category personal data include::

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) the processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest, such as for equality of opportunity or treatment or racial and ethnic diversity at senior levels of organisations.

5.2.3. Particular care must be exercised in protecting special category personal data from loss and unauthorised access, use or disclosure. Any potential processing of special

category personal data should be referred to the Board before the processing takes place.

5.2.4. The Company's privacy notice which is available on our website at www.capitalgearingtrust.com sets out the types of special category personal data that the Company processes, what it is used for and the lawful basis for the processing. In general, the Company only expects to process special category data as part of its onboarding/appointment process of a director (including by undertaking background checks) or to comply with the requirements of the FCA Listing Rules and Disclosure Guidance and Transparency Rules.

5.3. The Company may (depending on the lawful basis on which it relies to process special category personal data) be required to implement an appropriate policy document (APD) to process special category personal data. A template APD is available on the ICO website, together with guidance on completing an APD. The Company has in place an APD for the purposes of complying with the FCA Listing Rules and Disclosure Guidance and Transparency Rules, in which case the Company expects to rely on the substantial public interest for processing personal data as referred to in paragraph 5.2.2 (above).

6. CRIMINAL RECORDS INFORMATION

6.1. Criminal records information will be processed in accordance with the Company's privacy notice which is available on our website www.capitalgearingtrust.com. The Company must meet one of the conditions set out in Schedule 1 of the Data Protection Act 2018 to process criminal records information. These conditions are summarised at a high level on the ICO website (here).

6.2. The Company may (depending on the lawful basis on which it relies to process criminal records information) be required to implement an APD to process criminal records information. A template APD is available on the ICO website, together with guidance on completing an APD.

7. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

7.1. Where processing is likely to result in a high risk to an individual's rights and freedoms, the Company is required by data protection laws to, before commencing the processing, carry out a DPIA to assess:

7.1.1. whether the processing is necessary and proportionate in relation to its purpose;

7.1.2. the risks to individuals; and

7.1.3. what measures can be put in place to address those risks and protect personal data.

7.2. Further information on conducting a DPIA is available on the ICO website (here).

8. PRIVACY NOTICE

8.1. The UK GDPR requires data controllers to provide detailed, specific information to data subjects when they process the personal data of those data subjects. Where the we collect

personal data from data subjects, directly or indirectly, then we must provide data subjects with a privacy notice. In order to ensure transparency, we maintain a privacy notice which we make available to all data subjects on our website at www.capitalgearingtrust.com.

8.2. The Company recognises the need to regularly audit the personal data we hold and to check that it is being processed in accordance with the privacy notice set out on our website at www.capitalgearingtrust.com and the terms of this policy.

8.3. We will take appropriate measures to provide information in our privacy notice in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

8.4. Further information on the requirements for informing data subjects of the processing of their personal data is available on the ICO website (here).

9. INDIVIDUAL RIGHTS

9.1. Under the data protection laws, data subjects have a number of rights in respect of their personal data. We are committed to ensuring that those rights are recognised and that we fulfil our obligations in this regard. The key rights for data subjects are as follows:

9.1.1. the right to obtain, on request, a copy of all personal data held about them by the Company;

9.1.2. the right to prevent the processing of their personal data for direct marketing purposes;

9.1.3. the right to have inaccurate data rectified or erased without undue delay;

9.1.4. the right to object to certain processing of their information;

9.1.5. the right to be "forgotten" (in other words, to request that the Company erases personal data about them);

9.1.6. the right to restrict the processing of their personal data in certain circumstances;

9.1.7. the right to obtain and reuse their personal data (for example, if they wish to move, copy or transfer their information to another organisation); and

9.1.8. the right to withdraw consent to processing.

9.2. In most cases, CG Asset Management will be the first point of contact with a data subject in the event of a request from that data subject. Any request made from a data subject in relation to personal data controlled by the Company must be promptly reported to the Board and no response should be made without the Board's approval. At the Board's request, persons subject to this policy will assist the Board in complying with data subject rights and requests in accordance with the time frames set out in the data protection laws.

9.3. If you wish to exercise any of the rights in paragraph 9.1, please contact CG Asset Management.

10. INFORMATION SECURITY

10.1. The Company will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

10.1.1. making sure that, where possible, personal data is pseudonymised or encrypted;

10.1.2. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

10.1.3. ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

10.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

11. STORAGE AND RETENTION OF PERSONAL DATA

11.1. Personal data (and special category personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.

11.2. Personal data (and special category personal data) that is no longer required will be deleted and/or put beyond use and any hard copies will be destroyed securely.

12. DATA BREACHES

12.1. A data breach may take many different forms, for example:

12.1.1. loss or theft of data or equipment on which personal data is stored;

12.1.2. unauthorised access to or use of personal data by a third party;

12.1.3. loss of data resulting from an equipment or systems (including hardware and software) failure;

12.1.4. human error, such as accidental deletion, disclosure or alteration of data;

12.1.5. unforeseen circumstances, such as a fire or flood;

12.1.6. deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

12.1.7. ‘blagging’ offences, where information is obtained by deceiving the organisation which holds it.

12.2. The Company will:

12.2.1. make the required report of a data breach to the ICO without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

12.2.2. notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

12.3. Accordingly, if you become aware of or suspect a data breach has occurred, you must immediately report the matter to the Board and CG Asset Management. The Company will then decide how to deal with the matter reported. It is important to note that a data breach may be as simple as sending an email or contact details to the wrong person. If you are in any doubt please contact CG Asset Management.

12.4. You should not take any action whatsoever in respect of an actual or suspected data breach except to report it to the Board and CG Asset Management.

13. THIRD PARTY PROCESSORS

13.1. Where the Company allows a third party (such as one of its advisers) to process personal data on behalf of it (a "**processor**"), the Company needs to ensure that a formal, written contract is put in place with the relevant processor which complies with the data protection laws. This contract should impose obligations on the processor as required by Article 28 of the UK GDPR including confirmation that the processor will only process personal data in accordance with the Company's instructions.

13.2. If you wish to appoint a third party to provide services which involves the third party processing any of the Company's personal data, you should first contact CG Asset Management, who will ensure that all necessary steps are taken to comply with the above requirements.

13.3. The Company should only use a processor that provides sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets the requirements of data protection laws. This means that the Company is responsible for assessing that its processors are competent to process the personal data in line with the requirements of data protection laws. This assessment should take into account the nature of the processing and the risks to the data subjects.

14. INTERNATIONAL TRANSFERS

14.1. Under the data protection laws, the Company may not transfer any personal data to a country outside the UK or EEA without complying with various conditions. It should be noted that such transfers can sometimes take place in a way that is not particularly obvious (for example, if a processor in the UK is storing data outside the UK).

14.2. The Company may only transfer personal data outside the UK or EEA if an appropriate safeguard is in place, including for example that:

14.2.1. the country or territory that we send the data to is approved by the Secretary of State or European Commission (as applicable) as offering equivalent protections to those afforded by data protection law in the UK and EEA (as applicable); or

14.2.2. we have put in place specific standard contracts approved by the Secretary of State or European Commission (as applicable) which give personal data the same protection it has in the UK and EEA (as applicable).

14.3. If you become aware that any personal data is or may be transferred outside the UK, you should immediately raise this with the Board and CG Asset Management who will assist in ensuring that all necessary steps are taken to comply with the data protection laws. You shall not authorise or make a transfer of personal data outside the UK until the Board confirms that steps to ensure compliance with the data protection laws have been put in place.

15. ELECTRONIC MARKETING

15.1. Prior consent is required for electronic direct marketing (for example, by email) to data subjects but there is a limited exception available which allows us to send marketing texts or emails where:

15.1.1. the data subject is an existing or past investor;

15.1.2. the communication relates to an offer of similar services to the services already provided to the data subject by the Company;

15.1.3. the data subject is given the chance to opt-out of such communications when their data is collected; and

15.1.4. the data subject continues to be given an option to opt-out of such communications in each communication.

15.2. The right to object to electronic direct marketing must be explicitly offered to a data subject in an intelligible manner so that it is clearly distinguishable from other information (including via an unsubscribe option in each communication sent). A record must be kept of all data subjects who opt-out of or object to receiving electronic marketing communications.

15.3. Where consent is relied upon to send marketing communications, that consent must be specific and informed. Please refer to paragraph 4.2 (above) for further details.

16. TRAINING

Persons who process personal data on behalf of the Company should undergo adequate training on data protection to enable them to understand and comply with the data protection laws.

17. RECORD KEEPING

The Company shall maintain records showing the steps it has taken to seek to ensure compliance with data protection laws, including records of compliance audits and its processing activities.

18. DATA PROTECTION BY DESIGN

We recognise that when pursuing our business activities, where these activities involve the processing of personal data, we are required to bear in mind our obligations under the data protection laws and, balancing costs and the likely risk of damage to data subjects, consider measures which might be applied to that processing which might better safeguard that data and protect the rights of the data subjects. Such measures might include pseudonymisation, data minimisation and/or reducing the personal data collected, the extent of processing, the period of storage, and the accessibility. You are required to consider whether processing activities could be adjusted to achieve these goals and any ideas which they may have should be brought to the attention of the Board and CG Asset Management.

19. CONSEQUENCES OF FAILING TO COMPLY

19.1. The Company takes compliance with this policy very seriously. Failure to comply with the policy:

19.1.1. puts at risk the individuals whose personal data is being processed; and

19.1.2. carries the risk of significant civil and criminal sanctions for the Company (and potentially those who process personal data on its behalf); and

19.1.3. may, in some circumstances, amount to a criminal offence.

19.2. Because of the importance of this policy, failure to comply with any requirement of it may lead to the Company taking action against you (for example to terminate our contractual relationship with you or to initiate legal proceedings against you).

19.3. If you have any questions or concerns about anything in this policy, do not hesitate to contact CG Asset Management.