HIGHCLERE
INTERNATIONAL INVESTORS

Highclere International Investors LLP

DATA PROTECTION POLICY

August 2021

TABLE OF CONTENTS

1. INTRODUCTION

Highclere is required to comply with the UK's data protection legislative framework which comprises the 'UK General Data Protection Regulations' (which was adopted from the EU equivalent Regulation on 1 January 2021) and the Data Protection Act 2018 (the "DPA 2018") (the " UK **GDPR**"). Highclere's supervisory authority with respect to the UK GDPR is the Information Commissioners Office ("**ICO**"). In addition, the Financial Conduct Authority has indicated that Highclere should ensure compliance with UK GDPR as part of their obligations under the FCA Handbook.

This document constitutes Highclere's data protection policy (the "**Policy**"). It sets out the obligations of Highclere regarding data protection and the rights of data subjects in respect of their personal data under UK GDPR.

More specifically, the Policy sets out Highclere's obligations regarding the collection, processing, transfer, storage and disposal of personal data. The procedures set out in this Policy must be followed at all times by Highclere, and Highclere staff (as defined in the Highclere Personnel Handbook).

Highclere places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

2. PROCESSING PERSONAL DATA

2.1 INTRODUCTION

The UK GDPR defines "**personal data**" as "any information relating to an identified or identifiable natural person (a "**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Processing**" of personal data includes any operation or set of operations which is performed on personal data including 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.

Highclere collects and processes personal data directly from data subjects.

Under UK GDPR, a "**controller**" is any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

For the purpose of UK GDPR Highclere has determined that it is a controller.

Under UK GDPR, a "**processor**" is any natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller.

Highclere has determined that it is a processor with respect to certain personal data.

Due to the nature of its business Highclere processes only a limited amount of personal data. Therefore the Highclere has determined that it does not require a statutory Data Protection Officer given the limited amount of personal data that it processes. However, Highclere's Data Protection Manager / Compliance Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and with the UK GDPR.

2.2 THE DATA PROTECTION PRINCIPLES FOR PROCESSING

The UK GDPR sets out seven principles (the "**Principles**") with which any party handling personal data must comply. Highclere complies with these Principles at all times with respect to the personal data it collects and processes. The Principles are:

2.2.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2.2.2 PURPOSE LIMITATION

Personal data must be collected for a specified, explicit and legitimate purpose and should not be processed for any other purpose that is incompatible with that specified purpose.

2.2.3 DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed and for the purposes of which data subjects have been (or will be) informed.

2.2.4 ACCURACY

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay, including rectification at the request of a data subject.

2.2.5 STORAGE LIMITATION

Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the processing purpose(s).

2.2.6 INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.2.7 ACCOUNTABILITY

The controller is responsible for compliance with the Principles and should be able to demonstrate that processing activities are compliant with the Principles.

2.3 LAWFUL BASIS FOR PROCESSING

Highclere, as a controller, is required to have a lawful basis for each processing purpose unless it can rely on an exemption or derogation. There are six lawful bases:

2.3.1 CONSENT

The data subject has given valid consent to the processing of their personal data for one or more specific purposes. Consent should be "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent is given by forms of email correspondents or in the form of a legally binding contracts/agreements. This applies to staff and clients.

2.3.2 CONTRACTUAL NECESSITY

The processing is necessary for entering into or the performance of a contract to which the data subject is a party.

2.3.3 COMPLIANCE WITH LEGAL OBLIGATIONS

The processing is necessary for compliance with a legal obligation to which the data controller is subject.

2.3.4 VITAL INTERESTS

The processing is necessary to protect the vital interests of the data subject or of another natural person when the processing cannot be manifestly based on another lawful basis.

2.3.5 PUBLIC INTEREST

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

2.3.6 LEGITIMATE INTERESTS

The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data. Types of Personal Data Collected, Held and Processed

2.4 PERSONAL DATA

Highclere collects, holds and processes the following types of personal data:

Staff

Full name; current address; address history; next of kin details; passport copies; proof of address; bank details; NI numbers; work history; CRB check; work history verification screening report; company emails; records telephone calls incoming/outgoing from the office; pictures from staff events/offsite and professional photographs for client marketing purposes; personal email addresses; Investment preferences; CV's; education and training certificates.

Unitholders

We may hold personal data about Unitholders which is provided to us by you directly as a result of your investment in the Funds (by completing subscription forms, telephone calls and/or corresponding with us)

Or which is provided to us by third parties. This includes names, contact details, tax identification numbers, bank details, the names, contact details and signatures of authorised signatories, copies of IDs, contact details for individuals to receive correspondence and investor information. The actual data we hold will be dependent on the structure, regulatory and tax status of the particular commingled fund.

Prospects

Prospects are potential clients. We keep basic information - name, work correspondent address, work contact details and work email address, sometimes publically available work history. No passports or ID documents are kept unless laws and/or regulations dictate necessary.

Consultants

We keep basic information - name, work correspondent address, work contact details and work email address, sometimes publically available work history. No passports or ID documents are kept unless laws and/or regulations dictate necessary.

Suppliers

Business card information, work email addresses, work contact numbers. Highclere complies with the Principles at all times when handling and processing personal data.

How we collect data

We do not collect personal data about you through your use of our website and our website does not use cookies. Personal data may be collected about you from direct interactions with you, including by filling in forms and any email or other correspondence. This includes personal data you provide when you request information to be sent to you**.**

2.4.1 CRIMINAL OFFENCE DATA

For regulatory and / or employment purposes, Highclere may ask a third party processor to processes personal data relating to criminal convictions and offences from time to time. At all times the processing must be based on one of the lawful bases described in section 2.3 above. Furthermore, processing of criminal offence data requires specific legal authorisation by the law of the UK (this is set out in schedule 1 of the DPA 2018) and compliance with appropriate safeguards for the rights and freedoms of data subjects set out in the legislation.

Prior to processing criminal offence data, Highclere identifies the condition for lawful processing of the data and the relevant safeguards upon which it is relying, and this is documented.

Highclere does not maintain a comprehensive register of criminal convictions.

3. DATA SUBJECTS

3.1 TYPES OF DATA SUBJECT

Highclere has identified that is has the following types of data subject:

Staff, partners, clients, former clients, prospective clients and consultants.

The scope of the UK GDPR is not limited to the UK and extends to data subjects of Highclere wherever in the world they are located.

3.2 THE RIGHTS OF DATA SUBJECTS

The UK GDPR sets out the following rights applicable to data subjects:

3.2.1 THE RIGHT TO BE INFORMED

Where information is obtained directly from a data subject, Highclere shall provide the following information, free of charge, to the data subject at the same time in a transparent manner, which is concise, intelligible, easily accessible and in clear and plain language:

- Details of Highclere, including but not limited to, the identity of its Data Protection Manager.
- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
- If relevant, the legitimate interests upon which Highclere is justifying its collection and processing of the personal data;
- Details of third party recipients or categories of recipient of the data;
- Where the personal data is to be transferred to a third country or to an organisation that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see section 7 for further detail);
- Details of the retention period or the criteria to determine it;
- Details of the data subject's rights under the UK GDPR;
- Details of the data subject's right to withdraw their consent to Highclere's processing of their personal data at any time;
- Details of the data subject's right to complain to the ICO;
- Where applicable, details of any statutory or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Where applicable, details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Where information is obtained indirectly from a data subject, Highclere shall also provide the following information to the data subject within a reasonable period:

- The source of the personal data and whether the source is publicly accessible; and
- The categories of personal data.

3.2.2 THE RIGHT OF ACCESS

Data subjects may request access to the personal data that Highclere holds on them at any time to allow them to be aware of and verify the lawfulness of the processing of their personal data. This is commonly referred to as a Subject Access Request ("SAR").

In particular, data subjects have the right to receive:

- Confirmation of whether Highclere is processing their personal data;
- Information about the purposes of the processing;
- Information about the categories of personal data concerned;

- Information about the recipients with which the data has been or may be shared;
- Information about the envisaged period for which the data will be stored or the criteria used to determine that period;
- Information about the data subjects' rights of erasure, rectification, restriction of processing or to object to such processing;
- Information about the right to complain to the ICO;
- Information on the source of the data, if not received directly from the data subject;
- Information on the existence and logic of any automated processing that has a significant effect on the subject;
- If data is transferred outside of the UK, information on the relevant safeguards (see section 7 for further detail); and
- A copy of the personal data being processed.

Highclere shall normally respond to access requests within one month of receipt; however, this may be extended by up to two months if the request is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All requests received shall be handled by Highclere's Data Protection Manager / Compliance Officer.

Highclere does not charge a fee for the handling of normal access requests. However, Highclere reserves the right to either charge reasonable fees or to refuse to act in respect of requests that are manifestly unfounded or excessive, particularly where such requests are repetitive, and to charge reasonable fees for any further copies of the personal data that are requested.

3.2.3 THE RIGHT TO RECTIFICATION

Data subjects have the right to require Highclere to rectify any of their personal data that is inaccurate or incomplete.

Highclere shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Highclere of the issue.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

3.2.4 THE RIGHT TO ERASURE (AKA THE "RIGHT TO BE FORGOTTEN")

Data subjects have the right to request that Highclere erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for Highclere to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to Highclere holding and processing their personal data;
- The data subject objects to Highclere holding and processing their personal data and there are no overriding legitimate grounds for the processing;
- The personal data is processed for direct marketing purposes and the data subject objects to this processing;
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for Highclere to comply with UK law.

Unless Highclere has reasonable grounds to refuse to erase personal data, such as the exercise or defence of legal claims or compliance with a regulatory or other legal obligation all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

If the personal data has been made public in an online environment, for example on social networks, forums or websites, reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data.

3.2.5 THE RIGHT TO RESTRICT PROCESSING

If data subjects are not able to enforce the right to erasure, they may have a right to block the processing of personal data by Highclere.

Data subjects can require restrictions in a range of circumstances, including:

- Where the data's accuracy is contested by the data subject until Highclere can verify it;
- Where the processing is unlawful and the data subject requests restriction, rather than full erasure;
- Where Highclere no longer needs the data for its original purpose, but it is still needed by Highclere to establish, exercise or defend legal claims;
- Where the data subject has objected to processing based on legitimate grounds and Highclere, pending the verification of whether the legitimate grounds of Highclere override those of the data subject.

If a data subject requests a restriction, Highclere will only process data, with the exception of storage, with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person. Highclere will retain only the amount of personal data related to the data subject that is necessary to ensure that the personal data under restriction is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

3.2.6 THE RIGHT TO DATA PORTABILITY

Data subjects have the right to request and receive a copy of their personal data from Highclere in a machine readable format, and to transfer it from Highclere to another controller for their own purposes. It applies:

- To personal data an individual has provided to Highclere;
- Where the legal basis for processing of that data by Highclere is consent or the performance of a contract; and
- When processing is carried out by automated means.

All requests for copies of personal data that satisfy the above conditions shall be notified to the Data Protection Manager / Compliance Officer who shall ensure that such requests are complied with within one month of the data subject's request.

3.2.7 THE RIGHT TO OBJECT

Data subjects have the right to object to processing of their personal data by Highclere if the lawful basis relied upon is the legitimate interests of Highclere.

Where a data subject objects to Highclere processing their personal data based on its legitimate interests, Highclere shall cease such processing immediately, unless it can be demonstrated that Highclere's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to Highclere processing their personal data for direct marketing purposes, Highclere shall cease such processing immediately.

3.3 DATA SUBJECTS REQUESTS

Any requests received by an employee, contractor or agent of Highclere from a data subject shall be forwarded to the Data Protection Manager / Compliance Officer without delay.

4. OBLIGATIONS OF CONTROLLERS AND PROCESSORS

4.1 OBLIGATIONS OF CONTROLLERS

Highclere has identified that it is a controller. The most relevant obligations for Highclere as a controller under the UK GDPR are:

4.1.1 COMPLIANCE WITH THE PRINCIPLES

Highclere is required to comply, and to be able to demonstrate such compliance, with the Principles in both the planning and implementation phases of processing activities associated with a particular product or service.

4.1.2 TECHNICAL AND ORGANISATIONAL MEASURES

Highclere must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the UK GDPR.

4.1.3 TRANSPARENCY

Highclere must communicate in a transparent manner to data subjects certain information regarding the processing of their personal data, and their rights in respect of such processing.

4.1.4 RECORDKEEPING

Highclere is required to maintain records of relevant processing activities.

4.1.5 NOTIFICATION OF DATA BREACHES

Highclere is required to notify the ICO and, in certain circumstances, data subjects of data breaches. See section 12 for further details.

4.1.6 JOINT CONTROLLERS

N/A to Highclere

4.1.7 APPOINTMENT OF PROCESSORS

N/A to Highclere

4.1.8 COOPERATION

Highclere must cooperate with the ICO on request in the performance of its tasks.

4.2 OBLIGATIONS OF PROCESSORS

Highclere has identified that in certain circumstances it is a processor. The most relevant obligations for Highclere as a processor under the UK GDPR are:

4.2.1 APPOINTMENT AND CONTROLLERS' INSTRUCTIONS

Highclere can only be appointed as a processor if it guarantees compliance with the UK GDPR in the provision of its processor services and by way of a written binding agreement. It can only process data on instructions from a controller. See section 5 for further details.

4.2.2 NATIONAL LEGISLATION

The UK GDPR requires processors to consider the implications of any national enabling legislation that may apply to them, in addition to the obligations pursuant to the regulation. Processors should

immediately inform the controller should there be a conflict between the requirements of the UK GDPR or any other applicable national data protection laws.

4.2.3 RECORDKEEPING

Highclere, as a processor, is required to retain records of its processing activities performed on behalf of a controller.

4.2.4 COOPERATION

Highclere, as a processor, is required to cooperate on request with the ICO in the performance of its tasks.

4.2.5 DATA SECURITY

The UK GDPR directly imposes data security requirements on processors. Such requirements include the encryption of personal data, ongoing reviews of security measures, back up facilities and regular security testing. See section 9 for further details.

4.2.6 REPORTING BREACHES

Highclere, as a processor, should report any data breach to the relevant controller without undue delay after becoming aware of it.

4.2.7 CROSS-BORDER INTERNATIONAL DATA TRANSFERS

Highclere, as a processor, is subject to compliance with the international data transfer rules. See section 7 for further details.

5. APPOINTMENT OF THIRD PARTY PROCESSORS

Highclere sometimes utilises the services of third party service providers who act as processors with respect to personal data collected by Highclere.

Highclere ensures that any third party providers have a current policy that discloses all of their procedures with regards to UK GDPR.

Highclere monitors its third party processors on an on-going basis to ensure compliance with the UK GDPR.

6. JOINT CONTROLLERS

N/A to Highclere.

7. CROSS BORDER TRANSFERS

Highclere may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK, so called third countries.

Our US office has access to client data and documents and staff data which is used for our marketing presentations.

8. NEW ACTIVITIES – DATA PROTECTION ASSESSMENT

Highclere shall carry out a data protection assessment every time there is a new project with a new process, business activity or product, which could constitute a new processing purpose under the UK GDPR.

9. PERSONAL DATA SECURITY

9.1 TRANSFERRING PERSONAL DATA AND COMMUNICATIONS

Highclere has put in place measures to ensure the security of the personal data it collects and stores about you, see 9.2. It will use its reasonable endeavours to protect your personal data from unauthorised disclosure and/or access, including through the use of network and database security measures, but it cannot guarantee the security of any data it collects and stores. We have put in place

procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9.2 INFORMATION CYBER SECURITY POLICY

Further details of Highclere's general data security procedures can be found in its Cyber Security Summary.

10. ORGANISATIONAL MEASURES

Highclere shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- Only staff, agents, sub-contractors, or other parties working on behalf of Highclere that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Highclere;
- All staff, agents, contractors, or other parties working on behalf of Highclere handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- All personal data held by Highclere shall be reviewed periodically to ensure compliance with retention periods;
- All staff, agents, contractors, or other parties working on behalf of Highclere handling personal data will be bound to do so in accordance with the principles of the UK GDPR.;

  All agents, contractors, or other parties working on behalf of Highclere handling personal data must ensure that all of their staff who are involved in the processing of personal data are held to the same conditions as those relevant staff of Highclere arising out of this Policy and the UK GDPR.

11. MONITORING

11.1 INTRODUCTION

Highclere has an obligation to monitor the effectiveness of its data protection arrangements and this Policy and to demonstrate compliance with this Policy. This obligation has been incorporated into Highclere's general compliance monitoring process.

11.2 RESPONSIBILITY FOR PERSONAL DATA MONITORING

Monitoring is performed by Highclere's Data Protection Manager / Compliance Officer with on-going review and oversight from Highclere's compliance function.

In the event that Highclere's monitoring procedures identify any deficiencies in Highclere's Policy, the issue identified shall be promptly escalated to the governing body with sufficient detail and any proposed corrective action to be taken, including any proposed changes to this Policy.

12. DATA BREACHES – NOTIFICATION AND SANCTIONS

All personal data breaches must be reported immediately to Highclere's Data Protection Manager / Compliance Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Manager /Compliance Officer must ensure that the ICO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. It may also be necessary to inform the FCA and any other regulators of the Firm as applicable.
.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Manager / Compliance Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;

- The categories and approximate number of personal data records concerned;
- The name and contact details of Highclere's data protection officer (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Highclere to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

13. POLICY REVIEW

Highclere's Data Protection Manager /Compliance Officer is responsible for the maintenance and annual review of this Policy and Highclere's data protection procedures and records.

The review takes into account a number of factors including:

- any deficiencies with this Policy and/or Highclere's data protection procedures identified during Highclere's monitoring processes;
- new purposes for processing personal data;
- changes to the types of personal data collected and processed;
- changes to the types of data subject;
- changes to the methods of processing personal data; and
- changes in relevant legislation.