Data Protection Policy.

1 Introduction

This Data Protection Policy (this "policy") sets out the obligations of the Cavendish Group ("Cavendish", "we", "us", "our") regarding data protection and the rights of individuals whose Personal Data we collect, use and process in the course of our business activities.

This policy applies to all Cavendish employees, workers, consultants, contractors and interns ("employees", "you", "your"). Your compliance with this policy is mandatory. Any breach of this policy or our other data protection policies and procedures may result in disciplinary action.

This policy has been prepared with due regard to the data protection laws applicable to Cavendish and our Personal Data Processing activities. These Data Protection Laws include the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018"), together referred to herein as the "Data Protection Law".

This policy should be read together with our: **Cavendish Data Protection by Design and by Default Policy**, **Cavendish Personal Data Retention Policy**, **Cavendish Information Security Policy**, **Cavendish Data Subject Rights Procedure**, **Cavendish Personal Data Breach Procedure** and **Cavendish DPIA Procedure and Assessment Template**.

2 Policy Statement

Cavendish place high importance on respecting the privacy and protecting the Personal Data of individuals with whom we work including our clients, end customers and employees. We are committed to the fair, lawful and transparent handling of Personal Data and to facilitating the rights of individuals. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

3 Scope

This policy applies to all Personal Data processed by Cavendish whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to Personal Data we process as a Controller and Personal Data we process as a Processor (on behalf of our clients).

The following Cavendish Group entities are registered as Controllers in the UK with the Information Commission:

- Cavendish Consulting Limited, registration number Z9262039
- BECG Limited, registration number Z7809249
- Cavendish Advocacy Limited, registration number ZA772436
- Cavendish Consulting Cymru Limited, registration number ZB856807
- Cavendish Insights Limited, registration number Z2513847
- Kaizo Limited, registration number ZB817194
- Liberty One Communications Limited, registration number ZA647930
- MCE NI Ltd, registration number ZC164349

4 Definitions

The following definitions apply across all data protection policies, procedures and supporting documents:

Term	Description
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes.
Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data.
Criminal information	Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.
"DPA 2018"	Data Protection Act 2018.
Data Protection Impact Assessment ("DPIA")	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change.
Data Protection Law	The UK GDPR, the DPA 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR").
Data Protection Officer ("DPO")	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law.
Data Subject	Any natural person (individual) whose Personal Data is being processed.
"EEA"	European Economic Area – the EU member states plus Norway, Iceland and Liechtenstein.
Information Commission ("IC")	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, DPA 2018 and PECR.

Legitimate Interest Assessment ("LIA")	Determines if individual's Personal Data is being used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Privacy and Electronic (EC Directive) Regulations 2003 ("PECR")	UK law that sits alongside the DPA 2018 and UK GDPR, providing specific privacy rights regarding electronic communications.
Personal Data	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	Any operation or set of operations that is performed on Personal Data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure.
Processor	A person, entity or organisation that processes Personal Data on behalf of a Controller.
"SCCs"	EU-approved Standard Contractual Clauses – a mechanism used to legitimise international transfers from the EU to third countries.
Sensitive Personal Data	Special Category Data and Personal Data relating to criminal convictions and offences.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, biometric data (where used to identify a data subject), data concerning health and data concerning a natural person's sex life or sexual orientation.
"UK"	The United Kingdom – England, Scotland, Wales and Northern Ireland.
"UK GDPR"	UK General Data Protection Regulation has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.
"UK IDTA"	UK International Data Transfer Agreement – a mechanism used to legitimise international transfers from the UK to third countries.

5 Responsibilities

Key data protection responsibilities within Cavendish are as follows:

- The Board of Directors are accountable for ensuring we meet our data protection obligations;
- The Data Protection Representative is responsible for implementing and enforcing this policy;
- Line Managers are responsible for ensuring that employees under their management are made aware of and adhere to this policy;
- Data Owners (employees working with Personal Data over which they have decision making authority) are required to ensure that data protection by design and by default (as more fully described below) is applied to new and existing business practices, processes, IT systems and technologies that involve the processing of Personal Data for which they are responsible;
- Project Managers are required to carry out a DPIA where the risks to Data Subjects associated with a data processing activity carried out by us as a Controller are high or where otherwise required by the **Cavendish DPIA policy**, and in such instances shall only process the Personal Data in question as permitted by the outcome of the DPIA.
- All employees are required to read, understand and adhere to this policy when processing Personal Data on our behalf.

You should speak with Data Protection Representative to ask a question, or raise a concern, relating to this policy or data protection in general.

6 Data Protection Principles

The following data protection principles shall govern the collection, use, retention, transfer, disclosure and destruction of Personal Data by Cavendish:

Principle 1 - Fair, Lawful and Transparent

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

Principle 2 - Purpose Limitation

Personal Data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Principle 3 - Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4 - Accuracy

Personal Data must be accurate and kept up to date.

Principle 5 - Storage Limitation

Personal Data which permits identification of Data Subjects (i.e. data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.

Principle 6 - Security

Personal Data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Principle 7 - Accountability

As Controller, we are responsible for demonstrating compliance with the data protection principals listed above.

7 Data Protection by Design and by Default

Cavendish shall ensure that the risks to rights and freedoms of Data Subjects associated with processing are key considerations when:

- Designing, implementing and during the life of business practices and processes that involve the processing of personal data ("processing activities"); and
- Developing, designing, selecting, procuring, and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing, and otherwise processing personal data ("processing systems").

This risk led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall consider both the likelihood and the severity of the potential harm to the rights and freedoms of Data Subjects.

Where the risk to the rights and freedoms of Data Subjects is likely to be high, or where otherwise required by law or the relevant supervisory authority, a DPIA shall be performed in accordance with our **Cavendish DPIA procedure**.

Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g. policy, awareness, governance, and assurance) as well as technical measures (e.g. pseudonymisation). The objectives of such safeguards and measures shall include:

- Data minimisation.
- Limiting the extent of the processing, storage, and access to what is strictly necessary.
- Ensuring transparency for data subjects regarding the processing activities; and
- Ensuring the security of the personal data.

8 Data Processing Obligations

Cavendish as a Processor

Where we are a Processor, we may only process Personal Data in accordance with the Controller's documented instructions as set out in a data processing agreement. We may only transfer Personal Data out of the UK and the EEA and appoint sub-Processors as permitted by the data processing agreement.

Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Access to the Personal Data must be limited only to employees who are subject to an obligation of confidentiality and who need access to carry out their assigned duties.

We must assist the Controller to meet their compliance obligations under applicable laws including for the purposes of:

- Ensuring the security of processing, including by implementing appropriate technical and organisational measures;
- Supporting the facilitation of subject rights of Data Subjects whose Personal Data we hold;
- Enabling the Controller to notify the relevant supervisory authority following a Personal Data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of affected Data Subjects;
- Enabling the Controller to notify affected Data Subjects following a Personal Data breach which is likely to result in a high risk to the rights and freedoms of affected Data Subjects; and
- Supporting data protection impact assessments carried out by the Controller as appropriate.

Upon termination of the data processing agreement, we must delete or return Personal Data as set out at Section 14 of this policy.

We must also support the Controller to demonstrate Accountability and compliance with applicable laws by providing them with all information necessary to demonstrate compliance by Cavendish and allow for and participate in audits by the Controller or their representative.

Cavendish as a Controller

Where we are the Controller, Data Subjects must be provided with information notifying them of the purposes for which we will process their Personal Data (a "privacy notice"). When Personal Data is obtained directly, the privacy notice shall be provided to the Data Subject at the time of collection. When Personal Data is obtained indirectly, the privacy notice shall be provided to the Data Subject as soon as possible (and not more than one calendar month) after it is obtained from a third party. The privacy notice must explain what processing will occur and must also include the information set out at Schedule 1.

Our use of the Personal Data must match the description given in the privacy notice and be limited to what is necessary for the specific purposes stated. Where our lawful basis for processing is based on our legitimate interests, we may only process the Personal Data if our legitimate interests are not

outweighed by the interests, rights and freedoms of the Data Subjects in question. A legitimate interests assessment should be performed to confirm this.

We must not collect or process any more Personal Data than is strictly necessary for the purposes of the processing ("data minimisation"), as set out in our privacy notice, and must ensure that data minimisation continues to be applied throughout the lifetime of the processing activities.

Personal Data must be kept accurate and up to date. The accuracy of Personal Data must be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps are to be taken without delay to amend or erase that data, as appropriate. Personal Data must not be kept for any longer than is necessary for the purpose for which that data was originally collected and processed. When the data is no longer required, all reasonable steps must be taken to securely erase or dispose of it without delay, as set out at Section 14 of this policy.

Personal Data must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9 Third Party Supplier Onboarding

When engaging a new supplier that will process Personal Data on our behalf, we will:

- Complete a DPIA screening questionnaire and full DPIA if required, in accordance with our **Cavendish DPIA Procedure**;
- Complete our **supplier data protection due diligence questionnaires**;
- Ensure there is a written agreement in place between Cavendish and the relevant supplier that contains appropriate data protection provisions; and
- Resolve any risks or issues identified when completing the points contained in this section before any processing takes place.

10 Accountability

Only those employees that need access to, and use of, Personal Data to carry out their assigned duties correctly will be permitted access to Personal Data we hold. All employees handling Personal Data on our behalf must be:

- Made fully aware of both their individual and our responsibilities under this policy and applicable law, and be provided with a copy of this policy;
- Appropriately trained to do so and suitably supervised, with training to be provided upon starting with Cavendish and refresher training to be provided annually; and
- Bound to handle the Personal Data in accordance with this policy and the law by contract.

The methods of collecting, holding and processing Personal Data by employees, or other parties working on our behalf, are to be regularly evaluated and reviewed by the Data Protection Representative.

All consultants, agencies and other parties working on our behalf and handling Personal Data must ensure that all of their employees who are involved in the processing of Personal Data are held to the same obligations as applicable to Cavendish employees arising out of this policy.

When using a Processor (or, where permitted, a sub-Processor), a binding contract must be implemented between Cavendish and the Processor, setting out: the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the controller. Processor contracts must also include the terms set out at Schedule 2.

We will keep written internal records of processing activities ("RoPA") in respect of all Personal Data collection, holding, and processing. We will maintain both a Controller and Processor RoPA within the same spreadsheet.

Processor RoPA

Where we are a Processor, the RoPA will incorporate the following information:

- The name and contact details of the Processor and of each Controller on behalf of which we are acting as Processor and of our Data Protection Representative (if applicable);
- The categories of processing carried out on behalf of each Controller;
- Details of any transfers of Personal Data to countries outside the UK or European Economic Area ("EEA") including all mechanisms and security safeguards; and
- Descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

Controller RoPA

Where we are the Controller, the RoPA will incorporate the following information:

- The name and contact details of us as the Controller, our Data Protection Representative and any Joint Controllers (if applicable);
- The purposes for which we process Personal Data;
- Details of the categories of Personal Data collected, held and processed by us; and the categories of Data Subject to which that Personal Data relates;
- Details (and categories) of any third parties that will receive Personal Data from us;
- Details of any transfers of Personal Data to countries outside the UK or European Economic Area ("EEA") including all mechanisms and security safeguards;
- The envisaged retention periods for the different categories of Personal Data; and
- Descriptions of the technical and organisational measures we have implemented to ensure the security of Personal Data.

11 Risk Management

We will monitor the risks to Data Subjects associated with all existing and planned Personal Data processing activities and implement appropriate technical and organisational measures to safeguard Data Subjects and ensure the data protection principles set out in this policy are met. This risk led approach to data protection will be applied across all our business activities to ensure data protection by design and by default, as set out in our **Cavendish Data Protection by Design and by Default Policy**.

Where the risks to the rights and freedoms of Data Subjects associated with any existing or planned Personal Data processing to be carried out by Cavendish are potentially high or where otherwise required by applicable law or a supervisory authority in a country or territory in which we operate, we will carry out a Data Protection Impact Assessment ("DPIA"). All DPIAs are to be undertaken as set out in our **Cavendish DPIA Policy and Procedure**. A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of next review.

Where a Controller carries out a DPIA in relation to a processing activity in which we are a Processor, we will provide all information and assistance to the Controller as is reasonably required for the purpose of the DPIA.

12 Data Subjects Rights

Data subjects have the following rights regarding Personal Data processing and the data that is collected and held about them:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object;
- The right to register a complaint with the Controller; and
- Rights with respect to automated decision-making and profiling.

Requests by Data Subjects to exercise their rights must be facilitated as set out in our **Cavendish Data Subject Rights Procedure**.

Where we are the Controller, we are responsible for facilitating Data Subject rights. Where we are a Processor, we must assist the Controller to facilitate Data Subject rights as appropriate.

13 Protection of Personal Data

All employees must comply with the following when working with Personal Data:

- Personal Data must be handled with care at all times and must not be shared with any colleague, who does not have access to it, or with any third party without authorisation;
- Physical records must not be left unattended or on view to unauthorised employees, agents, contractors or other parties at any time and must not be removed from the business premises without authorisation;
- If Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- All physical copies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked filing cabinet, drawer, box or similar;
- All electronic copies of Personal Data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised;
- Personal Data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication or equivalent service (such as a personal cloud service);
- Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the Data Protection Law and all other applicable law (which may include demonstrating that all suitable technical and organisational measures have been taken and entering into a Processor contract with us);
- All Personal Data stored electronically shall be backed up regularly and securely; and
- Under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

In addition to the obligations set out above, all employees involved in processing Personal Data are required to read and adhere to our **Cavendish Information Security Policy**.

14 Data Retention and Destruction

Cavendish as a Processor

Where we are a Processor, we may only retain Personal Data for the duration of the data processing agreement. Upon termination of the data processing agreement, we must, at the choice of the Controller, delete or return all the Personal Data to the Controller and delete all existing copies unless otherwise required to store a copy by UK or EU member state law.

Cavendish as a Controller

Where we are the Controller, we may only retain Personal Data for as long as is reasonably required and in any event, only for as long as set out in our **Cavendish Personal Data Retention Policy**. Written authorisation from the Data Protection Representative is required to retain Personal Data for longer than as set out in the **Cavendish Personal Data Retention Policy**.

Once Personal Data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used.

15 Internal Data Transfers

We will only transfer ('transfer' includes making available remotely) Personal Data from countries in the UK to countries outside of the UK where:

- The transfer is to a country (or an international organisation) that the UK government / European Commission has determined ensures an adequate level of protection ("Adequacy");
- A UK IDTA or EU-approved SCCs with supplementary measures have been put in place between the entity in the UK or EEA and the entity located outside the UK or EEA;
- Binding corporate rules have been implemented, where applicable; or
- Where the transfer is otherwise permitted by the law.

Where we are a Processor, transfers of Personal Data outside the UK or EEA shall only be made with the Controller's agreement.

Where a transfer is not based on Adequacy, we will undertake a **Transfer Impact Assessment** ("TIA") to ensure that Data Subjects (whose Personal Data is transferred) continue to have a level of protection essentially equivalent to that under the UK GDPR. If the TIA outcome is that the appropriate safeguard does not provide the required level of protection, we will implement supplementary measures e.g., encryption.

16 Data Breach Notifications

All Personal Data breaches must be reported immediately to the Data Protection Representative and must be added to the register of Personal Data breaches.

Cavendish as a Processor

Where we are a Processor, and 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 Controller must be notified immediately with further information about the breach provided as soon as information becomes available.

Cavendish as a Controller

Where we are the Controller, if a Personal Data breach occurs which 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 relevant supervisory authority must be notified of the breach without delay, and in any event, within 72 hours after having become aware of it, if this is feasible. If the notification is not made within 72 hours, it should be made as soon as possible, together with reasons for the delay.

In the event that a Personal Data breach is likely to result in a high risk (that is, a higher risk than that described immediately above) to the rights and freedoms of Data Subjects, all affected Data Subjects are to be informed of the breach directly and without undue delay.

Irrespective of whether we are a Processor or a Controller, all data breach notifications must be handled strictly in accordance with our **Cavendish Personal Data Breach Procedure** and be added to our Breach Register.

17 Policy Review

The Company shall review this Policy not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. The Company will communicate any changes to employees and associated parties. The Company reserves the right to amend and update this Policy as required.

This policy will be reviewed annually by the Data Protection Representative and DPO and following any significant Personal Data breach.

This Policy has been approved and authorised by:
Name: Oli Folkerd
Position: Head of IT
Date: May 2026
Due For Review By: May 2027

Schedule 1 – Privacy Notices

Privacy notices for Data Subjects shall include:

- The identity and contact details of the Controller including, but not limited to, the identity of our Data Protection Officer;
- The purpose(s) for which the Personal Data is being collected and will be processed and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which we are justifying the collection and processing of the Personal Data;
- Where the Personal Data is not obtained directly from the Data Subject, the source used to obtain the Personal Data;
- The categories of Personal Data collected and processed;
- Where the Personal Data is to be transferred to one or more third parties, details of those parties;
- Where the Personal Data is to be transferred to a third party located outside the UK or EEA, details of that transfer, including but not limited to the safeguards in place;
- Details of the length of time the Personal Data will be held, or where there is no predetermined period, details of how that length of time will be determined;
- Details of the Data Subject's rights;
- Where applicable, details of the Data Subject's right to withdraw their consent to the processing of their Personal Data at any time;
- Details of the Data Subject's right to complain to a supervisory authority;
- Where applicable, details of any legal 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
- Details of any automated decision-making that will take place using the Personal Data, including but not limited to profiling, providing information on how decisions will be made, the significance of those decisions and any consequences.

Schedule 2 – Processor Contract

Contracts with Processors who will process Personal Data must set out the subject matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Data Subject; and the obligations and rights of the Controller. They must also include terms requiring the Processor to:

- Only act on the written instructions of the Controller;
- Ensure that people processing the data are subject to a duty of confidence;
- Take appropriate measures to ensure the security of processing;
- Only engage sub-Processors with the prior consent of the Controller and under a written contract;
- Assist the Controller in providing subject access and allowing Data Subjects to exercise their rights under the UK GDPR;
- Assist the Controller in meeting its UK GDPR obligations (or obligations under other applicable laws) in relation to the security of processing, the notification of Personal Data breaches and data protection impact assessments;
- Delete or return all Personal Data to the Controller as requested at the end of the contract; and
- Submit to audits and inspections, provide the Controller with whatever information we need to ensure that we are both meeting our data protection obligations, and tell us immediately if it is asked to do something infringing the Data Protection Law (or other applicable legislation).

Schedule 3 – Personal Data Processed

The following personal data are collected, held and processed by Cavendish (for details of data retention, please refer to our **Cavendish Data Retention Policy)**:

Data Ref.	Type of Data	Purpose of Data
Name	Name	To enable us to identify a data subject who: • Is participating in a public consultation process. • Is taking part in market research activities. Is participating in a marketing or PR campaign.
Address	Postal address	To enable us to contact data subjects to discuss: • The project on which a public consultation is being held. • Market research activities. • Various products and services promoted by us on behalf of our clients.
Telephone	Mobile and landline numbers	To enable us to contact data subjects to discuss: • The project on which a public consultation is being held. • Market research activities. • Various products and services promoted by us on behalf of our clients.
E-mail	Email address	To enable us to contact data subjects to discuss: • The project on which a public consultation is being held. • Market research activities. • Various products and services promoted by us on behalf of our clients.

Gender	Gender	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. • To enable us to correctly target the promotion of various products and services on behalf of our clients.
Sexual orientation	Sexual Orientation	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. • To enable us to correctly target the promotion of various products and services on behalf of our clients.
Date of birth	Date of Birth	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. • To enable us to correctly target the promotion of various products and services on behalf of our clients. • To ensure that we are not collecting data from anyone under the age of 13.
Age Group	Age Group	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. • To enable us to correctly target the promotion of various products and services on behalf of our clients. • To ensure that we are not collecting data from anyone under the age of 13.

Ethnicity	Ethnicity	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. • To enable us to correctly target the promotion of various products and services on behalf of our clients.
Employment	Employment details	• To enable us to ensure that public consultation programmes and activities have taken into account the demographic makeup of a particular geography (or group of service-users). • To ensure that market research activity is targeted at the correct audiences. To enable us to correctly target the promotion of various products and services on behalf of our clients.