

# **The 100 Children Report 2022**

## **Technical Report**

November 2022

Prepared for the Advertising Standards Authority (ASA)



*This technical report gives an overview on the background, planning and execution of the 100 Children Report, conducted by Kantar on behalf of the Advertising Standards Authority (ASA) in 2022.*

*It includes a synopsis of the various considerations taken to ensure data protection. The rights of all participants were at the centre of the methodological design and approach taken.*

## Contents

<b>1. Introduction</b>	<b>5</b>
1.1 Background	5
1.2 Objectives	5
<b>2. Methodology</b>	<b>5</b>
2.1 Step 1: Feasibility check using Kantar’s Online Kids’ Omnibus	6
2.2 Step 2: Recruitment Survey	6
2.2.1 Sample requirements	7
2.2.2 Recruitment through Kantar Panels	7
2.2.3 Sample design	7
2.2.4 Questionnaire coverage	7
2.2.5 Getting to the truth	8
2.2.6 Fieldwork considerations	8
2.2.7 Fieldwork stages	9
2.2.8 Fieldwork timings	9
2.2.9 Incentives	10
2.2.10 Fieldwork metrics	10
2.2.11 Quality checks	10
2.2.12 Defining the monitoring period for Ad Metric analysis	11
2.3 Step 3: Capturing Ad Exposure	11
2.3.1 Approach to collecting Digital Behaviour	11
2.3.2 Coverage across operating systems	12
2.3.3 How Android data collection works	13
2.3.4 What RealityMine Meter technology collects	15
2.3.5 What was possible to capture across the four social media platforms	16
<b>3. Processing the data</b>	<b>17</b>
<b>4. Achieved sample</b>	<b>17</b>
<b>5. Usage data</b>	<b>18</b>
<b>6. Optional follow-up survey</b>	<b>19</b>
<b>7. Data protection</b>	<b>20</b>
<b>8. Appendix</b>	<b>21</b>

**Appendix A: Example email invitation to download and install app** 21

**Appendix B: Example reminder email to download and install app** 21

**Appendix C: App installation guide shared with email invitations** 22

**Appendix D: Survey screenshots to show how to find your registered age on social media platforms** 25

## Table contents

Table 1: Kids’ Omnibus - demographic profile achieved..... 6

Table 2: Fieldwork timings ..... 9

Table 3: Fieldwork metrics .....10

Table 4: Number of days the app was active across the 104 successful completes.....10

Table 5: Number of days app was active, for our final 97 participants .....11

Table 6: Coverage across operating systems .....12

Table 7: Possible Android coverage .....13

Table 8: How Accessibility and On-Device VPN data collection works .....13

Table 9: How Ad Broker and Image capture methods work .....14

Table 10: Top-level view of what RealityMine Meter collects .....15

Table 11: Demographic breakdown of the 97 children.....18

Table 12: Demographic breakdown of optional follow-up survey .....19

## 1. Introduction

### 1.1 Background

The Advertising Standards Authority (ASA) is the UK's independent regulator of advertising across all media. It sets and enforces rules to prevent advertisements from misleading, harming or seriously offending their audience. Appropriately limiting children's and young people's exposure to age-restricted ads such as alcohol, gambling and foods that are high in fat, salt or sugar (HFSS) is a critical part of its work.

Kantar was commissioned by the ASA to conduct research to identify the types of ads being seen by children online, including within logged-in social media account environments, to help develop its regulation in this area.

In this technical report, Kantar details the approach taken to investigate advertising content exposure amongst 11–17-year-olds<sup>1</sup> on social media platforms.

### 1.2 Objectives

The ASA identified two core objectives for this study:

1. Identify the types of online ads being served to 11–17-year-olds in logged-in social media environments and across other online environments, with a particular focus on age-restricted ads.
2. Determine the relative exposure of 11-17-year-olds to age-restricted ads, and to draw out where ad exposure may occur, in part or otherwise, as a result of the child being falsely registered as, or incorrectly inferred to be, 18 or over.

## 2. Methodology

The project consisted of three core elements:

- A UK-wide online survey with a nationally representative sample of 1,000 11-17-year-olds
- A monitoring study, capturing ads served to a panel of 100 11-17-year-olds
- An optional follow-up survey with the panellists

---

<sup>1</sup> Collectively referred to as 'children' throughout the report.

## 2.1 Step 1: Feasibility check using Kantar’s Online Kids’ Omnibus

Before recruitment of the 100 children began, we conducted a survey through Kantar’s Online Kids’ Omnibus, amongst those aged 11-17. The survey provided useful contextual data on social media account ownership, the setting up of accounts and enabled us to check the feasibility of identifying children who give a false age when creating social media accounts.

The Kids’ Omnibus had UK coverage and we surveyed a sample of 1,000 11-17-year-olds. Interviewing was conducted by online self-completion from 20 January and 25 January 2022.

The demographic profile achieved is detailed in the table below.

**Table 1: Kids’ Omnibus - demographic profile achieved.**

Demographics		Unweighted fallout	Weighted Profile*
Gender	Male	51%	50%
	Female	48%	49%
Age bands	11-12	30%	30%
	13-15	43%	42%
	16-17	27%	28%
Region	North East	5%	4%
	North West	12%	11%
	Yorkshire / Humberside	10%	8%
	East Midlands	9%	7%
	West Midlands	10%	9%
	East of England	4%	9%
	London	10%	14%
	South East	17%	14%
	South West	10%	8%
	Scotland	5%	8%
	Wales	6%	4%
	Northern Ireland	2%	3%

\*Regional weighting was applied.

## 2.2 Step 2: Recruitment Survey

To identify eligible children to take part in the monitoring phase, we conducted a 10-minute recruitment survey. Below we detail the different considerations for this stage.

## 2.2.1 Sample requirements

The sample specification for the recruitment survey was 100 children in the UK aged 11-17 who:

- Have their own personal Android device [See section 2.3.2 'Coverage across operating systems' for details on why we focused on Android devices only]
- Use social media at least once a week
- Have at least one of the following social media accounts:



Facebook



Instagram



Twitter



YouTube

## 2.2.2 Recruitment through Kantar Panels

Using a combination of Kantar's UK consumer survey panel and Kantar's Public Voice panel, Kantar looked to recruit 100 11-17-year-olds to download and install the Kantar Scope app containing RealityMine meter technology for a period of 7 days.

Children were recruited through their parents who were members of Kantar's and its partners' panels.

## 2.2.3 Sample design

Given the target audience of the overall 100 sample, it was not possible to apply specific quotas. Nonetheless, a least-fill approach<sup>2</sup> was adapted to ensure we achieved a good distribution of participants across the age groups, and fallout of gender and geographical location was closely monitored during fieldwork.

## 2.2.4 Questionnaire coverage

Key considerations for the recruitment questionnaire were:

- To capture the informed consent of parents and children aged 13+ to ensure the project adhered to the MRS code of conduct.
- To be completely transparent about the aims of the research, what we would be doing with the data and that the ASA was the project sponsor to help recruit participants.

---

<sup>2</sup> When more than one child within a household qualified to take part in the study, we selected the child whose age was in an age-band with fewer completes than others, to ensure we had a well distributed sample.

Note: Following GDPR guidelines, 11- and 12-year-olds cannot give valid consent for processing their personal data, so parental consent was sought.

## 2.2.5 Getting to the truth

An essential part of the recruitment survey was establishing the age children have registered on their social media accounts.

To elicit honest responses from children, who may not wish to admit they created accounts with false dates of birth, we framed the questions in the survey to encourage open and honest responses.

Extract from Recruitment Survey Questionnaire:

*“For our results to give us a true picture of the ads that children see online, we are asking you to be honest with us about the age you are registered as on each social media platform you use.*

*We know that platforms often have age restrictions in place, but lots of people give false ages to create an account. You won’t get into any trouble if you’ve said you’re older than you are (and remember all the data shared with the ASA will be anonymous), but it might just help us to understand why children are seeing the ads they’re seeing.”*

Rather than relying on recall, we shared both written and visual instructions to show respondents how to access details of their registered age on each platform. See Appendix D for screenshots from the survey.

## 2.2.6 Fieldwork considerations

- Asking respondents to have the app installed for a 7-day period to capture both weekday and weekend usage<sup>3</sup>
- To capture typical device usage/behaviour, conduct fieldwork during school time – avoiding both February half term and Easter where device usage could be heightened
- Soft launch survey to:
  - Ensure all routing was set up as required

---

<sup>3</sup> To ensure 7 days ad exposure was captured, we extended the monitoring period to 10-days in case participants had any difficulty in successfully installing the app.



- Ensure respondents were able to answer questions and were not dropping out at specific points along the survey

## 2.2.7 Fieldwork stages

The below illustrates the various stages for respondents taking part in this project:

- Complete the recruitment survey
- Receive an email invitation to download and install the app. The email included a detailed instruction guide (see Appendix C)
- Have the app installed for at least 7 days
- Receive an email informing the participant that they have completed the monitoring stage and should remove the app from their device. This email also invited the participant to an optional follow-up survey.

Reminder invitations were shared to those who completed the recruitment survey but had not proceeded to download and install the app. Reminder invites were shared to encourage participation and to remind respondents of the incentive should they complete the task.

See Appendix A and B for example invitation and reminder emails.

## 2.2.8 Fieldwork timings

The below table shows project fieldwork dates:

**Table 2: Fieldwork timings**

Project stage	Date
Stage One: Kid's Omnibus	20/01/2022 – 25/01/2022
Recruitment survey soft launch	09/03/2022
Fieldwork ended	19/04/2022

Whilst it was our intention to avoid school holidays, lower than expected conversion between successfully completing the recruitment survey and installing the app meant that we had to extend the fieldwork period beyond the planned 4-week phase and into the Easter holidays.

School holidays differ across the country, and in 2022 some schools broke for Easter on 4 April and others on 9 April. The below indicates the number of successful completes (participants who had the app installed for 7+ days) we had achieved ahead of both dates:

- 4 April 2022: 78 successful completes
- 9 April 2022: 93 successful completes

To reduce the fieldwork delay and the amount of monitoring taking place over the Easter break, we removed the contingency of monitoring 10 days of device usage and instead asked participants to download and install the app for the required 7-day period.

## 2.2.9 Incentives

As standard practice, to encourage participation, respondents were incentivised if they completed the recruitment survey and installed the app for at least 7 days.

Throughout fieldwork, incentives were increased to encourage a greater response rate.

## 2.2.10 Fieldwork metrics

The below tables show the projects fieldwork metrics and the number of days the app was active across the 104 successful completes.

**Table 3: Fieldwork metrics**

	Total
Completed recruitment questionnaire	870
Downloaded and installed the app	180
Kept app active for at least 7 days	104

**Table 4: Number of days the app was active across the 104 successful completes**

Number of days	Sample
7	2
8	3
9	2
10	97

Note: see Section 2.2.11 and 2.2.12 for details of the final reporting sample of 97 children. Changes were made following quality assurance checks to exclude participants who exhibited suspicious behaviour.

## 2.2.11 Quality checks

Included within the data processing stage, we conducted quality checks on the data collected, looking specifically to ensure that the captured web browsing behaviour of the 100 participants looked to be child rather than adult behaviour.

Our checks flagged suspicious behaviour if participants spent:

- 1hr+ on reward sites
- 20+ minutes on real estate sites
- 14+ minutes on job searches
- 30+ minutes on government services searches
- 10+ minutes on gambling

We looked at time spent on these categories alongside age data to make a judgement on whether the behaviour looked more adult than childlike.

This quality check identified 18 participants from the 104 sample, who exhibited suspicious behaviour. On balance, we considered they were likely to be adults and were therefore not comfortable including them in our sample.

In collaboration with the ASA, it was decided that we would replace these participants with 11 respondents who did not show signs of suspicious behaviour, but who had the app installed for fewer than 7 days. We came to this decision as it was agreed that it was better to under-report child behaviour, than to report behaviour that was potentially of an adult as that of a child.

Following these amends, our final achieved sample is 97 children.

## 2.2.12 Defining the monitoring period for Ad Metric analysis

The below table shows the number of days the app was active, for our final 97 participants.

**Table 5: Number of days app was active, for our final 97 participants**

Number of days	Sample
7+ days	86
6 days	2
5 days	2
4 days	2
3 days	3
2 days	2

To ensure a consistent approach when selecting the 7-day monitoring period for those participants who had the app installed for 7+ days, we used days 2-8 inclusive for the core analysis. It was decided to take the beginning of the block rather than the days towards the end to have fewer days over the school Easter holiday period.

## 2.3 Step 3: Capturing Ad Exposure

Below we detail what was captured on the panellists' Android device during the 7-day monitoring period.

### 2.3.1 Approach to collecting Digital Behaviour

Digital behaviour collected via the Kantar Scope meter involves tracking the apps used and websites visited, including the adverts served during this online activity.

For this study, Kantar Scope, including RealityMine’s metering technology, was installed on the main Android device (smartphone/tablet) used by the participating child aged 11-17. They were asked to install the app on their own device, specifically the one they used most often, allowing the meter to capture advertising during their online activity. This included advertising in specific apps as well as advertising from general web browsing, covering video as well as static images and animated gifs.

## 2.3.2 Coverage across operating systems

We chose to focus our sample on Android users only, because greater coverage is possible on Android devices than iOS. At the time this study ran, it was possible for RealityMine to capture social media coverage across Facebook, YouTube, Instagram, and Twitter. The below table illustrates this.

**Table 6: Coverage across operating systems**

Platform	Android App	Android browser	iOS App	iOS browser	Laptop browser
YouTube	Y	Y	Y	Y	Y
Facebook	Y	N	N	N	N
Instagram	Y	N	N	N	N
Twitter	Y	N	N	N	N
Other Apps	Some, but limited	N/A	Some, but limited	N/A	N/A
Other Websites (not encrypted)	N/A	Y	N/A	Y	Y

As the table above indicates, at the time of preparing to conduct this study, greater social media coverage was possible on Android devices than iOS devices due to an additional method of data collection being possible on those devices. We therefore made the decision to focus our target audience on those who have their own Android device (smartphone/tablet).

Focusing on Android devices, the table below illustrates the ad exposure we were able to capture over the course of this study.

**Table 7: Possible Android coverage**

Platform	Android App	Android browser
YouTube	Full coverage of video ads (pre, mid, or post-roll)	Full coverage of video ads (pre, mid or post-roll)
Facebook	All sponsored/promoted ad formats (note: for Accessibility to collect all the Metadata, it needs to be visible on screen, on the device)	N
Instagram	Sponsored post only – not Stories (note: for Accessibility to collect all the Metadata, it needs to be visible on screen, on the device)	N
Twitter	All sponsored/ promoted ad formats (note: for Accessibility to collect all the Metadata, it needs to be visible on screen, on the device)	N
Other Apps	Some, but limited http advertiser domains	N/A
Other Websites (not encrypted)	N/A	Y

### 2.3.3 How Android data collection works

There are two methods of data collection on the Android Operating System – Accessibility and On-Device VPN. The below table explains how both work.

**Table 8: How Accessibility and On-Device VPN data collection works**

Accessibility	On-Device VPN
<ul style="list-style-type: none"> <li>• Accessibility is the primary method of collecting behaviour from in-app usage for specific apps</li> <li>• Accessibility is a service designed to call out on-screen text for visually impaired users of the mobile phone</li> <li>• Rules are in place to capture the text from specific Accessibility fields to report what was on screen within the app - for example, the sponsored posts and promoted tweets from social media adverts.</li> </ul>	<ul style="list-style-type: none"> <li>• The VPN is primarily used to intercept traffic from web browser sessions.</li> </ul>

Alongside Accessibility and On-Device VPN, we used two additional methods to collect digital advertising creatives:

1. Capturing requests to ad broker/ mediation platforms
2. Image capture

The below table explains how both work.

**Table 9: How Ad Broker and Image capture methods work**

Capturing requests to ad broker / mediation platforms	Image capture
<ul style="list-style-type: none"> <li>• We used deep packet inspection of websites visited to capture the data</li> <li>• Deep packet inspection is a mechanism to capture the payload data transmitted between the user's device and web server. This technique of data capture is used very selectively, only targeting traffic explicitly deemed to be of interest. In the case of ad intelligence, this is limited to predefined known ad servers.</li> <li>• We worked with a 3<sup>rd</sup> party to parse html/ java script/ json to extract the ad metadata, including the campaign landing page and rich ad content (including html5). This is a deterministic way of capturing ad content.</li> <li>• This approach is limited to collection from Mobile Web Browsers.</li> </ul>	<ul style="list-style-type: none"> <li>• We captured images which were served from content servers flagged by ad blocking lists as servers known to host ad content</li> <li>• This method does not include any ad related metadata so we had to use other means to identify the content, starting with Google Vision. Google Vision returns information on the contents of the Image including reference to brand logos.</li> <li>• This is a non-deterministic way of capturing ad content as it does not include non-ad content</li> </ul>

## 2.3.4 What RealityMine Meter technology collects

**Table 10: Top-level view of what RealityMine Meter collects**

App collects	App does not collect
<ul style="list-style-type: none"> <li>• App usage and web browsing</li> <li>• Time visited and duration spent on web pages and within apps</li> <li>• Ads served within apps and online</li> </ul>	<ul style="list-style-type: none"> <li>• Financial information such as credit card details or online banking</li> <li>• Personal information such as:               <ul style="list-style-type: none"> <li>○ Location</li> <li>○ Telephone numbers</li> <li>○ Email addresses</li> <li>○ Passwords</li> <li>○ SMS/calls</li> <li>○ Conversations with others</li> </ul> </li> </ul>

Breaking down what is collected by the app in more detail, the app collects both non-personally identifiable information and personally identifiable information. Examples are outlined below and relate to clickstream data.

Clickstream data is information generated while surfing the internet and interacting with various sites, services, apps and device functions. In greater detail, the app collects the following types of information:

- **Online browsing:** This includes the sites visited and apps used, including social media networks, and reflects how the child uses them. We do not collect information such as email addresses or passwords
- **Online activities:** This includes the search terms entered and the results of such searches, the videos viewed, the products shopped for online, the ads served, information and content on sites or apps visited or used and with which the child interacts
- **Information on secure pages/apps:** This includes information and content from protected or secure pages or apps that the child accesses, such as the adverts seen within a social media platform, even if the service makes this information unreadable to others. We do not collect account information e.g., online banking or messages/conversations with others
- **System information:** This includes information about the device and system the child is using, including unique identifiers that may be stored in their device's operating system such as their device's unique identifier. We do not collect location information
- **Mobile device usage information:** This includes information about the child's use of their device. This information is collected and transmitted to us "in the background" and does not require any further activation on the parent or child's part. We call this "passive tracking". This can include the following types of information:

- Information about the child's usage of other apps and features on their device, including the identity of the apps and features, when they downloaded them, how often they use them and for how long. This includes things like their use of the camera(s) - although we do not have access to or collect their photos.
- Information about the type of device the child owns, when and for how long they charge it, its battery status, whether it is switched on, off or in a stand-by or "Airplane" mode.
- Information about which mobile network the child uses, which Wi-Fi networks they connect to, and at what times – we do not have access to or collect network passwords.
- Information about the volume of data downloaded to the child's mobile device, the times that they download that data and the method of connection they use (Wi-Fi or mobile network).

## 2.3.5 What was possible to capture across the four social media platforms

### YouTube

We were able to capture YouTube Video Ad Collection using both Accessibility and On-Device VPN methods.

The predominant way to use YouTube on an Android device is via the YouTube app. In this instance we used Accessibility to capture the following:

- Title and Description (if populated in call to action and overlay cards)
- Channel
- MediaID

Not all fields of MediaID, Title, Description and Channel were populated for every ad collected.

If participants accessed YouTube via the browser app, we used the VPN method to capture URLs. This was possible when a YouTube video was embedded.

### Social Media

Social Media Ad Collection is only possible on Android devices using Accessibility to collect data from app usage of Facebook, Twitter and Instagram.

Using Accessibility, we were able to capture:

- All sponsored/promoted ad formats across supported social media platforms
- Metadata, where it was visible on screen, on the device

Where we had text for Facebook and Instagram ads, the Facebook Ad Library was a resource that could be used to identify the campaign/ creative.



## Ad Blockers

It is important to note that it is not known whether a child had ad blocking or filtering software installed on the device which was monitored. If they were using an ad blocker or similar type of software on their device during the monitoring period, no advertisements were collected from that device.

## 3. Processing the data

The eContext service (<https://www.econtext.ai/>) was used to categorize text (both from websites and description metadata), to help identify the category of advertisements. This allowed the identification of potential prohibited categories for closer inspection. It is possible for multiple category outcomes to be seen and therefore an approach was used to evaluate the main category that had the highest dominance.

We used eContext to attempt to identify the main category of the advert by classifying the:

1. Description text from YouTube ads
2. The metadata captured from social media ads
3. The text from the landing page of ads captured via the Ad Broker method
4. The metadata from images processed via the Image Capture method

## 4. Achieved sample

The below table shows the demographic breakdown of the final 97 sample.

**Table 11: Demographic breakdown of the 97 children**

Demographics		Achieved fallout %
Gender	Male	61 (63%)
	Female	36 (37%)
Age bands	11-12	38 (39%)
	13-15	38 (39%)
	16-17	21 (22%)
Region	North East	4 (4%)
	North West	9 (9%)
	Yorkshire and The Humber	7 (7%)
	East Midlands	7 (7%)
	West Midlands	14 (14%)
	East of England	6 (6%)
	London	15 (15%)
	South East	9 (9%)
	South West	13 (13%)
	Wales	2 (2%)
	Scotland	10 (10%)
Northern Ireland	1 (1%)	

## 5. Usage data

In addition to the ad monitoring data, we also provided data on each child's online behaviour across the week. We provided the following usage metrics:

- Top app usage – frequency and duration
- Top domain visits – frequency and duration
- Time of day usage for YouTube and social media apps (1-hour slot breakdown)
- Top all app categories being used
- Top domain categories being used
- Total device usage

The usage data shared was based on:

- The same 7-day period used for the ad analysis. Where we had 10 days monitoring, we considered days 2-8 inclusive. It was decided to take the beginning of the block rather than the days towards the end to have less days over the school Easter holiday period.

- For those participants with less than 7-days monitoring, it was decided not to weight the data to keep comparability between the usage and ad data and to not infer behaviour of the 11 participants.

## 6. Optional follow-up survey

Following the completion of the 7-day period with the app installed on their device, we invited the participants to take part in an optional, post-fieldwork questionnaire to gain an understanding of whether participants enjoyed taking part in the research and whether having the app installed on their device altered their behaviour/ device usage.

Of the 97 children who took part in our research, 64 went on to complete the follow-up survey. The demographic breakdown of the 64 children who opted to take part in the follow-up survey is outlined in the below table.

**Table 12: Demographic breakdown of optional follow-up survey**

Demographics		Achieved fallout
Gender	Male	40 (63%)
	Female	24 (38%)
Age bands	11-12	26 (41%)
	13-15	25 (39%)
	16-17	13 (20%)
Region	North East	4 (6%)
	North West	6 (9%)
	Yorkshire and The Humber	5 (8%)
	East Midlands	5 (8%)
	West Midlands	10 (16%)
	East of England	4 (6%)
	London	10 (16%)
	South East	5 (8%)
	South West	7 (11%)
	Wales	2 (3%)
	Scotland	5 (8%)
Northern Ireland	1 (2%)	

## 7. Data protection

Data protection law requires every organisation processing data to assess whether this activity represents a high risk to a data subject's rights. This particularly applies to the use of new technologies and methodologies processing large amounts of Personal Data or profiling, or when technologies are updated or changed.

Kantar was required to conduct a Data Protection Impact Assessment (commonly referred to as a DPIA) to identify and minimise the privacy risks on the 100 Children Report. This project qualified for a DPIA due to the methodological approach of passively metering children.

Kantar conducted a DPIA which was approved by Kantar's Data Protection Officer (DPO) before fieldwork commenced.

## 8. Appendix

### Appendix A: Example email invitation to download and install app

"Hi {#FIRSTNAME#},

You've recently agreed for your child to download and install a Reality Mine meter software, which will capture their digital behavior and clickstream, through identifying digital ad exposure across apps and websites used, across a 10-day period.

Your child needs to click on the below link using their Android Mobile device which will re-direct them to the app store where they can download the app. They should use the below username for registration, password is not mandatory.

<https://play.google.com/store/apps/details?id=com.qmob.kantarscope>

Username – XXXX

Here you can download/check a step-by-step guide for installing the app:

<http://p.kantar.com/kantarscope/install/android/>

Privacy Policy

<http://p.kantar.com/kantarmedia/ASA/privacy/>

FAQs

<http://p.kantar.com/kantarmedia/ASA/faq>

Instructions to remove

<http://p.kantar.com/kantarscope/instructions/>

By installing the app **on your child's device** and keeping it active for 10 days you will qualify for your LifePoints reward, which will be credited to your account within two weeks of completion.

To start the 10 days, please download the app now.

### Appendix B: Example reminder email to download and install app

Hi {#FIRSTNAME#},

You've recently agreed for your child to download and install a Reality Mine meter software, which will capture their digital behavior and clickstream, through identifying digital ad exposure across apps and websites used, across a 10-day period. We've noticed that you've not yet installed the app, so here is a reminder of what you need to do:

# KANTAR

Your child needs to click on the below link using their Android Mobile device which will re-direct them to the app store where they can download the app. They should use the below username for registration, password is not mandatory.

<https://play.google.com/store/apps/details?id=com.qmob.kantarscope>

Username – XXXX

Here you can download/check a step-by-step guide for installing the app:

<http://p.kantar.com/kantarscope/install/android/>

Privacy Policy

<http://p.kantar.com/kantarmedia/ASA/privacy/>

FAQs

<http://p.kantar.com/kantarmedia/ASA/faq>

Instructions to remove

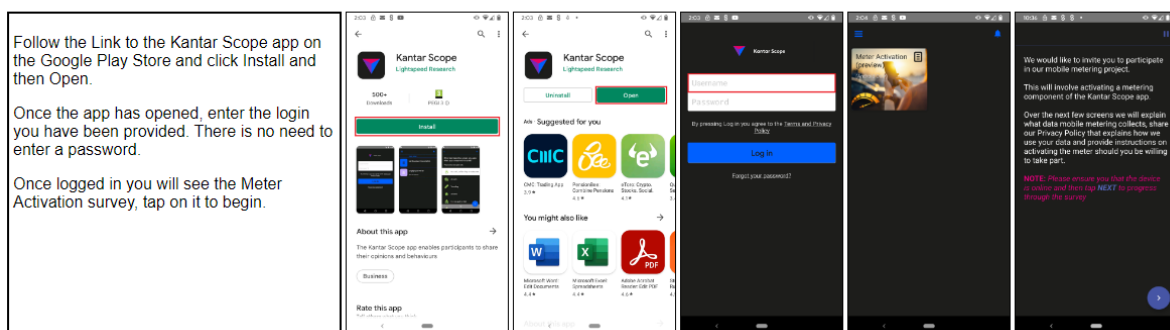
<http://p.kantar.com/kantarscope/instructions/>

By installing the app **on your child's device** and keeping it active for 10 days you will qualify for your LifePoints reward, which will be credited to your account within two weeks of completion.

To start the 10 days, please download the app now. Please be aware that the last date you can start this and qualify for the incentive is 25<sup>th</sup> March.

## Appendix C: App installation guide shared with email invitations

### Step 1



## Step 2

There are 4 steps to activate the meter, click on 1 to begin.

Scroll down to read through the overview.

Confirm you are interested in participating to view the full Privacy Policy.

You can zoom in and scroll through the Privacy Policy.

Select 'Yes' to agree to Activate the Meter.

## Step 3

Click on step 2 to allow the necessary App permissions.

Step 3 is required to download and enable the VPN. For Android version 11 and above there are additional steps required to save and install the VPN CA certificate.

**Please Note:** If your device is on a version below Android 11 please skip to step 7.

## Step 4

Android 11+ devices will see a video showing the steps to save and install the certificate, this can vary slightly depending on manufacturer and 3 examples are provided in the video. A text summary of the general steps is shown on the subsequent screen.

Begin the process to download and save the certificate.

Click OK to Save the certificate.

Click Save to download the certificate to your device.

## Step 5

Click OK to Install the VPN CA Certificate.

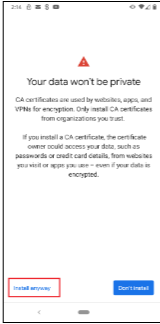
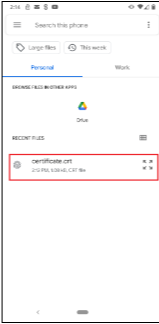
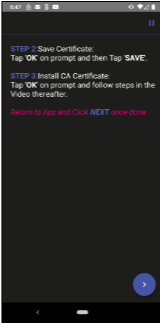


You will be taken to your Security settings, scroll down to Advanced, More or Other settings (will vary by Manufacturer).

Select Encryption & credentials (may be Other security settings on Samsung devices as can vary by Manufacturer).

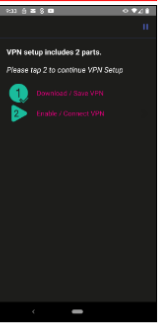
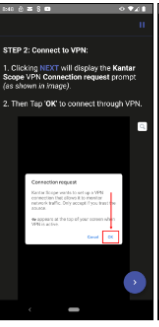
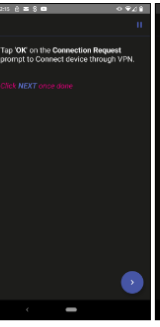
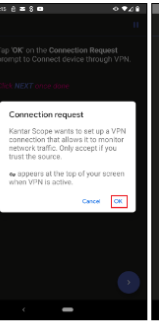
Select Install a Certificate (may be Install from device storage on Samsung devices as can vary by Manufacturer).

Select CA certificate.

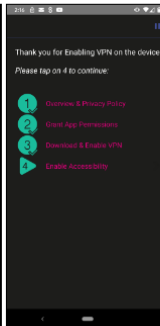
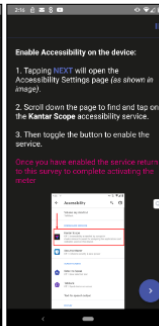
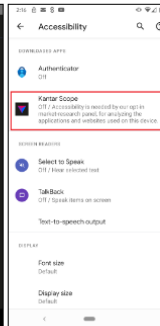
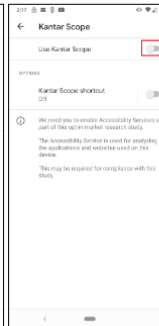
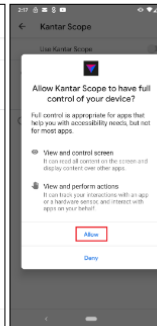
## Step 6

	Android 11+ only	Android 11+ only	Android 11+ only	Android 11+ only	Android 11+ only
<p>An Android warning message will be displayed, click <b>Install anyway</b> to proceed with installing the certificate and then click on certificate.crt. This is required for the meter app VPN to be successfully installed.</p> <p>Return to the Kantar Scope app to continue the Meter activation survey.</p> <p>A check will be run to see if the certificate has installed successfully. If it has not you will be taken back a step and asked if you want to see the video again or view a written summary of the instructions.</p>					

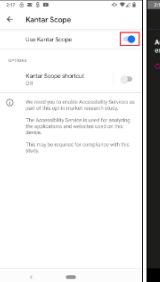
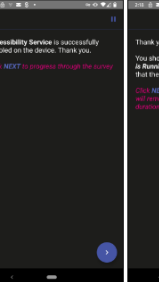
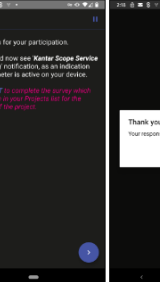
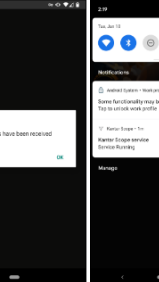
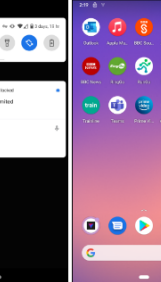
## Step 7

	Android 11+ only
<p>The previous steps to install the certificate are only required on Android 11+ devices. All Android versions require you to connect the VPN.</p> <p>Click OK on the Connection request.</p> <p>A check will be done to check the connection is successful.</p>	   

## Step 8

<p>Continue with Step 4 to enable the Accessibility permission.</p> <p>A display screen will give you some brief instructions.</p> <p>Once you continue, you will be taken to the Accessibility settings on your device, tap on Kantar Scope.</p> <p>Toggle the switch next to Kantar Scope.</p> <p>An Android warning may be displayed, click <b>Allow</b> to continue enable Accessibility.</p>	    
---	--

## Step 9

<p>Once enabled you will see the setting displayed as switched on and the next screen will check if this has been successful. Please note you may need to toggle this off and back on if you receive a notification during the project.</p> <p>When all activations steps are complete the Meter Activation Survey will be submitted.</p> <p>A notification will be present to confirm the Kantar Scope service is running. You will see the Kantar Scope App on your device but there is no need to open it unless you receive a notification.</p>	    
---	--



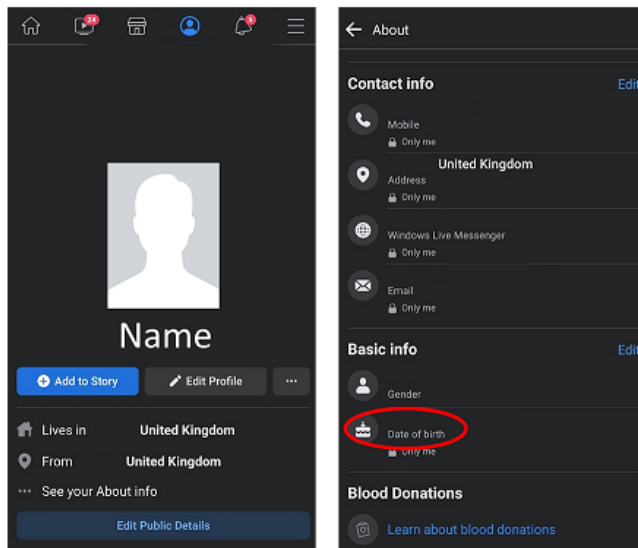
## Appendix D: Survey screenshots to show how to find your registered age on social media platforms

Facebook:

You said you have your own Facebook account.

Following the steps below, please tell us the date of birth that you have registered with Facebook

Profile page -> see your about info -> scroll down to date of birth

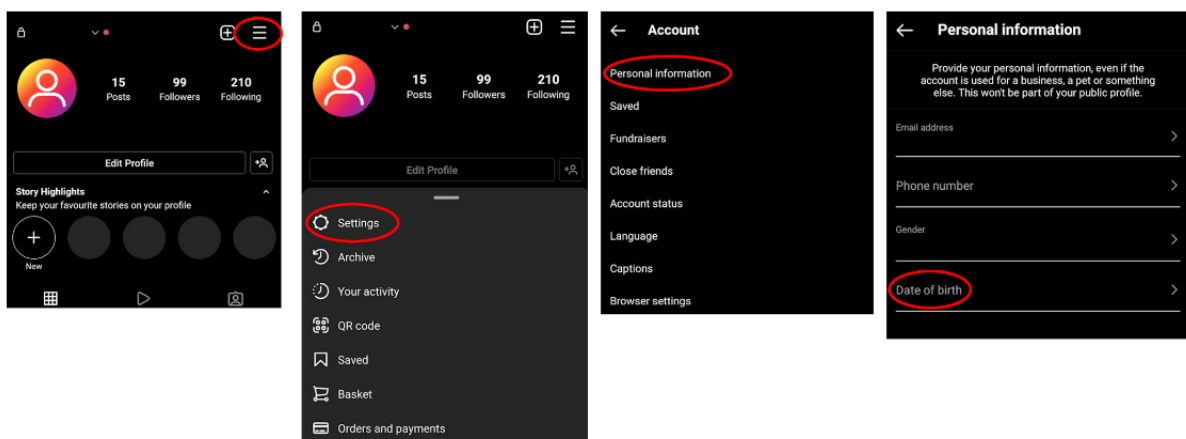


Instagram:

You said you have your own Instagram account.

Following the steps below, please tell us the date of birth that you have registered with Instagram

Profile page -> menu (top right) -> settings -> account -> personal information

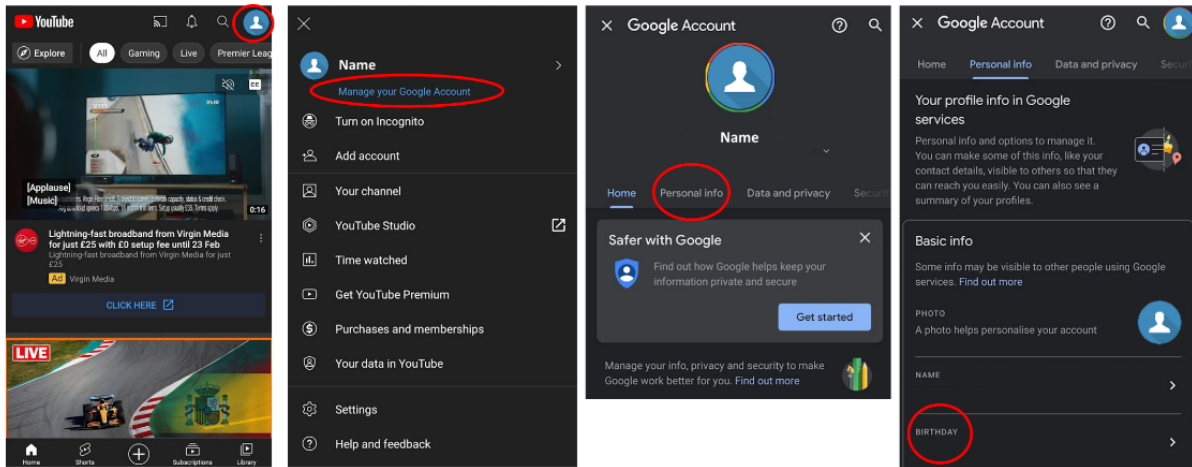


## YouTube:

You said you have your own YouTube account.

Following the steps below, please tell us the date of birth that you have registered with YouTube

Google Account (top right of page you'll see your initials or your profile picture) -> manage Google account -> personal information -> scroll down to date of birth



## Twitter:

You said you have your own Twitter account.

Following the steps below, please tell us the date of birth that you have registered with Twitter

You need to look on your web browser rather than through the app so you may need your login details for this. Click on your Profile picture -> Scroll down menu to "Settings & Privacy" -> "Your Account" -> "Account Information" (enter password) -> Scroll down to see "Birth Date"

