Privacy Impact Assessment (Condensed report)

July 2026

Evaluation of the Social Media Minimum Age scheme

Research and Evaluation

Australian Government
eSafety Commissioner
esafety.gov.au

Contents

1. Executive summary 3
Background 3
Findings 3
2. Scope and methodology 4
Scope 4
Methodology 4
3. Project description 5
Overview of the evaluation 5
The parties involved 5
The information involved 6
4. Information flows 7
5. Analysis of privacy issues 9
6. Recommendations 13

1. Executive summary

Background

From December 2025, new laws restrict children under 16 from holding accounts on age-restricted social media platforms. To understand what effect these restrictions are having, the Office of the eSafety Commissioner (eSafety) is undertaking a two-year study – the Social Media Minimum Age (SMMA) evaluation – following more than 4,000 children aged 10 to 16 and their parents and caregivers over time.

The evaluation looks at a broad range of outcomes, including children's wellbeing and mental health, their exposure to online risks and harms, their social media use, and their family and school life. It draws on several sources of information: surveys across five waves, interviews and group discussions, opt-in tracking of smartphone use, and – for participants who agree – the linkage of their responses with existing health and education records. Its findings will be a key source of evidence for the independent review of the SMMA scheme.

Because the evaluation involves children and a significant amount of personal and sensitive information, eSafety undertook a Privacy Impact Assessment (PIA) to examine how that information is handled and to confirm that it is handled consistently with the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs). This is a condensed version of the full assessment, prepared for publication given the strong public interest in the scheme and its evaluation.

Findings

The evaluation handles personal information in a way that is consistent with the Privacy Act and the APPs, and it is intentionally designed to protect the privacy of participants.

The central feature of that design is the separation of participants' identities from their research data. Information is held against a participant identifier rather than a name, the ability to reconnect that identifier to a real person is confined to a single provider, and eSafety itself works only with de-identified data. The more sensitive components of the study – passive smartphone-use tracking and the linkage of health and education records – are entirely opt-in, and the linkage is carried out by an accredited government integrating authority so that no single party holds the complete picture in identifiable form.

The evaluation is nonetheless a substantial and sensitive undertaking – longitudinal, involving children, sensitive information and multiple parties, and conducted under close public attention. Two matters were identified where privacy assurance could be strengthened over the life of the study:

- **Security** – Establish a process to periodically review and assure the security arrangements across the project (**Recommendation 1**).
- **Retention** – Agree a clear, project-specific retention and de-identification protocol with the primary service provider (Social Research Centre) (**Recommendation 2**).

2. Scope and methodology

Scope

This PIA assesses the handling of personal information involved in eSafety's evaluation of the SMMA scheme. It maps the personal information flows across the evaluation, assesses the handling of that information against the Privacy Act and the APPs, and makes recommendations to address any identified privacy risks.

The PIA covers all information handling conducted as part of the SMMA evaluation, including by the Social Research Centre (SRC), Netquest and the Australian Institute of Family Studies (AIFS) on eSafety's behalf. eSafety's panel-based research projects more broadly are out of scope.

This is a condensed version of the full PIA, prepared for publication given the public interest in the SMMA scheme and its evaluation. It omits confidential and operational detail (including specific security configurations) but reflects the findings and recommendations of the full assessment.

Methodology

The PIA was prepared by eSafety and independently reviewed by IIS Partners, a privacy and data protection consultancy.

In undertaking the assessment, the following steps were taken:

- Reviewing documentation about the evaluation and the personal information involved;
- Consulting with eSafety's Research and Evaluation team, eSafety's Data and Information Governance team, the Social Research Centre and the Australian Institute of Family Studies;
- Mapping the personal information flows across the evaluation;
- Analysing the information handling against the Privacy Act and the APPs, having regard to relevant guidance and privacy better practice; and
- Preparing this assessment, including findings and recommendations.

3. Project description

Overview of the evaluation

eSafety is undertaking a two-year longitudinal study to evaluate the impact of the Social Media Minimum Age (SMMA) scheme. The study follows more than 4,000 children aged 10 to 16 and their parents and caregivers over time, using surveys, interviews and group discussions, opt-in privacy-protected smartphone-use tracking, and the linkage of population-level health and education records.

The parties involved

A number of parties are involved in delivering the evaluation on eSafety's behalf, as set out below.

Entity	Role
eSafety	Commissions and leads the evaluation. It analyses the data collected to produce the evaluation findings, and conducts the qualitative fieldwork (interviews and focus groups) itself.
Social Research Centre (SRC)	eSafety's fieldwork provider. It recruits participants (including from its own Life in Australia™ probability-based panel and by coordinating the non-probability panels), administers the surveys, coordinates the passive smartphone-use tracking, and manages the consent process for data linkage.
Netquest	Provides the Wakoopa passive-tracking software used, with participant consent, to capture high-level smartphone-use information. Two expert academic collaborators advise on the analysis of this device data.
Recruitment panels	Life in Australia™, Octopus Group, ORU and PureProfile – provide survey participants from their existing panel membership. Of these, only Life in Australia™ and Octopus participate in the data linkage and passive-tracking components.
Australian Institute of Family Studies (AIFS)	eSafety's data linkage provider. It is one of the Australian Government's Accredited Integrating Authorities and Accredited Data Service Providers, and integrates the linked health and education records for the evaluation.
Data custodians	Services Australia (for Medicare Benefits Scheme and Pharmaceutical Benefits Scheme records) and the state and territory NAPLAN authorities – hold and provide the administrative records used in the data linkage.
Australian Institute of Criminology (AIC)	The AIC and DHA each fund a module within the evaluation and receive de-identified outputs relating to their respective modules.
Department of Home Affairs (DHA)	

Stanford University's Social Media Lab	Social Media Lab acts as the Lead Academic Partner and, with an Academic Advisory Group of leading experts, provides independent guidance across the design, analysis and reporting of the evaluation. Both have access to de-identified research data.
Academic Advisory Group (AAG)	

The information involved

At a high level, the evaluation involves:

- **Survey responses** from children and their parents/caregivers about the outcomes being studied.
- **Passive smartphone-use data** (such as apps used and time spent), collected only from participants who opt in.
- **Linked health and education records** (MBS, PBS and NAPLAN), obtained only for participants who opt in to data linkage.
- **Limited identifiable information** – held by the recruitment panels to contact and enrol participants, and held temporarily by eSafety (participant email addresses) to arrange the qualitative sessions.

Most of the information used for the evaluation is held in de-identified form, associated with a unique participant identifier rather than a participant's name. How this information is collected, used and disclosed is described in the next section.

4. Information flows

Personal information is handled across the following stages of the evaluation.

A) Recruitment and enrolment

Participants are recruited from the panels' existing membership, and provide consent (with their parents/caregivers) through the Participant Information and Consent Forms (PICFs). At enrolment, the SRC generates a unique participant identifier, which is used to link an individual's data across sources and across the survey waves. Identity is kept separate from research data: for Life in Australia™ participants, only the SRC can link the identifier back to a participant; for participants from the other panels, no single party can do so – re-identification would require the SRC and the relevant panel acting together (e.g., for mandatory reporting).

B) Survey data

The SRC administers the surveys and records responses against the participant identifier rather than the participant's name, and provides this data to eSafety for analysis.

C) Passive tracking data *(opt-in)*

For participants who opt in, Netquest's Wakoopa software captures high-level smartphone-use information (such as apps used and time spent) against a code only. No personal information is collected by or provided to Netquest. The data flows to the SRC and, in turn, to eSafety, associated with the participant identifier.

D) Qualitative data *(not yet commenced)*

The SRC provides participant email addresses to eSafety to arrange interviews and focus groups, which eSafety conducts itself. The research is intended to capture broad, thematic insights and is not attributed to identified individuals; transcripts are de-identified.

E) Data linkage *(opt-in)*

For participants who opt in, the SRC (and, for its own panellists, the Octopus panel) provides consent forms (including name, date of birth and Medicare number) to the relevant data custodians – Services Australia and the state and territory NAPLAN authorities – and separately provides the linkage identifier to the AIFS. The custodians extract the relevant records and provide them to the AIFS without direct identifiers. The AIFS integrates the records and provides the de-identified linked dataset directly to eSafety. The SRC does not receive any linked data back.

F) Storage

The SRC holds the participant-identifiable information (for Life in Australia™ participants) and the survey and device data; the other panels hold identifiable information only for their own members. eSafety holds the widest range of data for

analysis, but its holdings are associated with the participant identifier only – it does not hold the means to link that identifier to a participant's identity.

G) Use and disclosure

The primary use of the information is by eSafety, drawing the data together to conduct the SMMA evaluation. The other parties handle information in service of that evaluation and on eSafety's behalf. No direct identifiers are disclosed outside this group. De-identified, unit-level data is made available on a controlled-access basis to the AIC and DHA (for their respective funded modules) and to the Lead Academic Partner and Academic Advisory Group, under ethics approvals, data-sharing agreements and institutional arrangements.

5. Analysis of privacy issues

This section sets out the privacy issues identified for the evaluation. Rather than working through the APPs individually, the analysis is arranged thematically – grouping the APPs around the key privacy considerations that arise for a longitudinal study of this kind.

Each issue is described below, together with the relevant finding and, where applicable, a recommendation. The APPs that did not raise distinct issues for the evaluation are addressed briefly at the end of this section.

Issue	Finding
Collection and consent *(APPs 3, 5)* Ensuring the personal information collected is reasonably necessary for the evaluation, that sensitive information is collected with consent, and that participants are notified of how their information will be handled.	The evaluation collects a substantial amount of personal information – including sensitive information about children's health and wellbeing, and in some cases and on an optional basis, their racial or ethnic origin, religion and sexual identity. Sensitive information carries additional protections under the Privacy Act, including that it can generally only be collected with consent. Each category of information collected is tied to a specific purpose within the evaluation, and the study has been designed to avoid collecting more than is needed to answer its research questions. Consent is central to how this information is collected. Because participants are children aged 10 to 16, consent is obtained from a parent or caregiver, together with the child's own agreement expressed in age-appropriate terms. Consent is obtained for each component of the study and renewed as it progresses, so participants and their families retain genuine choice over what they take part in, including the more sensitive components such as data linkage. The PICFs carry the notification required under APP 5 – explaining who is collecting the information, why, how it will be handled, and how to raise a concern – so that consent is informed rather than nominal. **No issues identified.**
Use and disclosure *(APP 6)* Ensuring personal information is used and disclosed only for the purpose for which it was collected, or for a permitted secondary purpose.	The personal information collected for the evaluation is used for a single, clearly defined purpose: to evaluate the impact of the SMMA scheme, including by bringing the different sources of data together for analysis, in line with eSafety's research functions under the *Online Safety Act 2021* (Cth). Because the SRC and the other providers collect and handle the information on eSafety's behalf under binding contractual arrangements, the information they pass to eSafety is properly understood as a use within a single arrangement, rather than a disclosure to an outside party. No participant's identifying

	information travels beyond the group of parties delivering the study. The one circumstance in which personal information might be disclosed outside that group is where the law requires or authorises it – most likely if something a participant discloses triggers a mandatory reporting or duty-of-care obligation. This is expressly permitted under the Privacy Act, is expected to be rare, and is explained to participants and their families upfront in the consent materials. Information shared with funding and research partners (such as the AIC, the DHA and the academic partners) is de-identified, and so does not involve the disclosure of personal information at all. **No issues identified.**
Data linkage Ensuring that the linking of participants' survey data with population-level health and education records is conducted in a controlled and privacy-protective way.	Linking participants' survey responses with their health (MBS/PBS) and education (NAPLAN) records lets the study measure actual health and education outcomes over time, rather than relying on what participants report about themselves. It also warrants careful handling, because combining datasets about an individual produces a more detailed picture than any single source. The linkage has been structured so that no one party ever holds the whole picture in identifiable form. Linkage is carried out by the AIFS – one of the Australian Government's Accredited Integrating Authorities, which conducts work of this kind as a matter of routine under an established Commonwealth framework. The data custodians release the relevant records without direct identifiers, keyed only to a linkage code; the AIFS integrates those records and provides eSafety with a de-identified linked dataset. eSafety receives the linked data associated with a participant identifier, but not the means to connect that identifier back to a person. The result is that the sensitive administrative records are separated from participants' identities at every step, and the linkage is confined to the AIFS. **No issues identified; the linkage is conducted on a de-identified basis under established governance.**
De-identification and re-identification risk Ensuring personal information is effectively de-identified for research use, and that the risk of participants being	De-identification is a key privacy control in the evaluation, and it is what allows the analysis, linkage and academic collaboration to occur without those parties handling participants' identities. Research data is held against a randomly generated participant identifier rather than a name, and only the SRC can link that identifier back to a person – and only for the participants it recruited directly. eSafety holds the widest range of data for analysis, but its holdings are associated with the participant

re-identified is managed.	identifier only; it can join the datasets together, but cannot on its own identify a participant. De-identification of this kind is not the same as anonymisation. Because the data remains at a detailed unit-record level, some residual risk of re-identification remains – particularly where an unusual combination of characteristics, or a very small subgroup, could make an individual stand out. That risk is low, and a number of controls are applied to manage it: datasets are limited to the variables needed for the analysis, higher-risk variables are recoded into broad categories (e.g., postcode is converted into a remoteness or socio-economic band), small cell counts are suppressed or combined, and additional protections apply to information about groups who may be more readily identifiable, such as First Nations participants. At the end of the study, the participant identifiers are removed, so the research data can no longer be linked back to individuals. **No issues identified; the residual re-identification risk is low and appropriately managed.**
Security *(APP 11.1)* Ensuring personal information is protected from misuse, interference, loss and unauthorised access across all parties involved in the evaluation.	Each party that handles personal information for the evaluation applies its own security controls, consistent with its obligations and, in the case of the government parties, with the Australian Government's Protective Security Policy Framework and Information Security Manual. The SRC, which holds the identifiable participant information, applies access restrictions, encryption, secure transfer and monitoring, and is certified to recognised information-security standards. These arrangements are appropriate to the information each party holds. Given the scale and duration of the evaluation, and the number of parties involved, eSafety would benefit from maintaining a single, overall view of security across the project as a whole – spanning its own environment and those of its providers – supported by ongoing assurance over the life of the study. This would give eSafety, as the agency ultimately accountable for the information, continued confidence that the arrangements across all parties remain effective as the study progresses. **See Recommendation 1.**
Retention and Commonwealth record *(APP 11.2)* Ensuring personal information is retained only for as long as needed, consistent with eSafety's obligations	The evaluation is designed so that identifiable information is held only for as long as it is needed in that form – the SRC will de-identify it once it is no longer required for the research, such as once contact across the survey waves is complete. This limits the period over which participants' identities are connected to their data. Retention is complicated by the likelihood that the evaluation data is a Commonwealth record. If so, its retention and disposal are governed by the *Archives Act 1983* and the applicable

for records that must be kept.	Records Authorities rather than by APP 11.2, and eSafety cannot simply dispose of the information whenever it chooses. A question to be worked through is how the intention to de-identify at the earliest opportunity fits with the retention obligations that apply to Commonwealth records, including for the information held by providers on eSafety's behalf. This is best resolved by settling a clear, project-specific approach with the SRC, so that de-identification and disposal timeframes are agreed and consistent with eSafety's record-keeping obligations. **See Recommendation 2**
Broader considerations Considering whether the project could affect community expectations or cause reputational harm, given it involves children and sensitive information.	The evaluation sits in an area of close public and media attention. It involves children, sensitive information, passive tracking of device use, and the linkage of health and education records – and it concerns a scheme that has itself been the subject of significant public debate. There are strong community expectations that a study of this kind will be conducted carefully and with children's privacy firmly protected. Any privacy failure would carry consequences beyond the individuals affected. These expectations are well served by the way the evaluation has been designed. Participants' identities are separated from their research data, the ability to re-identify is confined to a single provider, the more sensitive components are opt-in, and data shared with partners is de-identified. These features apply throughout the study, not only at its outset. **No issues identified**

Other APPs

A number of the APPs were assessed and found either not to apply, or to be adequately addressed through eSafety's existing privacy practices. Accordingly, they are not discussed above. These include openness and transparency (APP 1), anonymity and pseudonymity (APP 2), direct marketing (APP 7), government related identifiers (APP 9), the quality of personal information (APP 10), and access to and correction of personal information (APPs 12 & 13).

In relation to cross-border disclosure (APP 8), no personal information is disclosed to an overseas recipient as part of the evaluation. While the passive-tracking provider is based overseas, it does not hold any personal information. Elements of the qualitative research component are still being finalised and may involve an overseas platform; eSafety will address any cross-border considerations in a separate assessment before that component commences.

6. Recommendations

This PIA makes two recommendations. Neither identifies a deficiency in the design of the evaluation; both are steps that would strengthen privacy assurance over the life of this long-running and complex study. eSafety's response to each is set out below.

Recommendation	eSafety response
Recommendation 1 Establish a process to periodically review and assure the security arrangements across the project, covering both eSafety's own environment and those of its subcontractors, for the duration of the evaluation.	Agreed
Recommendation 2 Agree a clear, project-specific retention and de-identification protocol with the SRC, consistent with eSafety's Commonwealth record obligations.	Agreed