eSafety FOI 26056
Document 1 of 11

Australian Government
Australian Institute of Family Studies

AIFS

Ethics application for higher risk projects

This amendment form is to be completed with reference to Guidelines for AIFS Ethics Review of a Research Project, Guidelines for Preparing an Ethics Application, Guidelines for Preparing an Application for Non-Ethics Committee Review, Child-safe research policy, National-Statement-Ethical-Conduct-Human-Research-2023, AIFS privacy policy, *Privacy Act 1988*.

Project title

Monitoring and outcome evaluation of the Social Media Minimum Age

Project lead

s 22

Application reference number

2025/06

Project start date

7/11/2025

Project completion date

31/12/2030

Acronyms

Abbreviation	Description
SMMA	Social Media Minimum Age
NAPLAN	National Assessment Program – Literacy and Numeracy
MBS	Medicare Benefits Scheme
PBS	Pharmaceutical Benefits Scheme

s 22

E2.4: How will you manage any risk that linking databases of non-identifiable data could subsequently result in the individuals being identified?

We will engage the Accredited Data Service Providers (ADSPs) at the Australian Institute of Family Studies (AIFS), and will adhere to their expert guidance on linkage protocols and data governance, including the AIFS' Data Confidentialisation and Disclosure Control Policy, as summarised below:

AIFS' Data Confidentialisation and Disclosure Control Policy is designed to manage disclosure risk effectively, preventing re-identification, privacy breaches, and other misuse of data.

Confidentiality Policy and Processes

AIFS' Data confidentialisation and disclosure control policy applies to all staff and contractors handling personal data. This policy ensures that effective and appropriate controls are implemented to mitigate privacy, confidentiality, and re-identification risks. It provides auditable evidence of data confidentiality and disclosure protection controls.

Confidentiality and Output Checking Manual

The policy includes a comprehensive confidentiality and output checking manual that provides guidelines for assessing and treating re-identification and disclosure risk in microdata. It includes strategies for mitigating identification risk in both microdata and disseminated data outputs.

Arrangements for Vetting, Confidentialising, and Monitoring Outputs

We have established detailed arrangements for vetting, confidentialising, and monitoring outputs as part of the policy. This includes:

- **Assessment**: Assessing microdata for re-identification risk and applying appropriate treatments to minimise disclosure risk.
- **Treatment**: Implementing controls to reduce the level of detail in records that present re-identification risk.
- **Review**: Comparing treated data against planned objectives and re-assessing if necessary.

Policies, Processes, and Methodology for Managing Disclosure Risk

The policy outlines various methods for managing disclosure risk and de-identifying data, including suppression, aggregation, and perturbation. These methods are applied based on a detailed assessment of the data and its intended use.

Managing Data Confidentiality Breaches

The policy also includes comprehensive procedures for managing data confidentiality breaches. This involves documenting key confidentialisation steps, retaining evidence of reviews, and archiving as part of the formal review process.

s 22

s 22 [redacted]

E5.3.1: If the survey data is individually identifiable, will personal identifiers be retained or removed over the course of your project? If they are to be removed what process will be used?

SRC will host the survey, collect and clean the survey data, and provide eSafety with raw de-identified datafiles, which will be stored on eSafety's secure IT system. Personal information will only be collected from participants who provide consent to enable data linkage. Personal data will be stored separately by SRC and linked only to the survey responses via a unique identifier. The files (e.g., consent forms) including personal details of participant and the unique identifier will be shared with the data custodians to enable data linkage – this will not include any responses to survey questions. eSafety will not access nor store personal information of survey participants.

SRC will share personal details (e.g., name and email address) with eSafety for a small sample of participants who consent to participate in qualitative research, to enable eSafety to schedule interviews, online focus groups etc. with these participants. This personal information will not be shared in conjunction with any of their survey responses, other than a small number of demographics to ensure a diverse range of participants is represented in this qualitative research. Any personal information that is shared will be stored securely on eSafety's secure servers and will be destroyed at the completion of the qualitative study.

s 22 [redacted]

eSafety FOI 26056
Document 2 of 11

Appendix K – Risk Management

s 22

s 22 [redacted]

4. Participants' confidentiality will be prioritised in data collection to minimise the chance of them being identified by evaluators or other participants:
    - All data will be de-identified in analysis and reporting.
    - Qualitative methods which promote anonymity and confidentiality have been prioritised. This included online-text based focus groups, where participants will be given pseudonyms and will not involve video.
    - Participants will be discouraged from sharing any personally identifiable information throughout the evaluation.

s 22 [redacted]

eSafety FOI 26056
Document 3 of 11

Appendix O – Data Management Plan

REC-0599: Monitoring and outcome evaluation of the Social Media

Data collection

The study will be conducted over an initial period of two years (with potential to extend for an additional three years), and will employ multiple modes of data collection, including:

- Multi-wave online survey
- Qualitative research (i.e., focus groups, diary studies, and interviews)
- Objective data collection (i.e., passive tracking of smartphone usage)
- Data linkage and population-level data

The **multi-wave online survey** will be self-complete, and will primarily collect quantitative data, with some qualitative data collected via free-text response questions. The Social Research Centre (SRC) will host the survey, collect and clean the survey data, and provide eSafety with raw de-identified datafiles, which will be stored on eSafety's secure IT system. Personal information will only be collected from participants who provide consent to enable data linkage. Personal data will be stored separately by SRC and linked only to the survey responses via a unique identifier. The file including demographic details of participant and the unique identifier will be shared with AIFS to enable data linkage – this will not include any responses to survey questions. eSafety will not access nor store personal information of participants.

All **data linkage** activities will be conducted in accordance with strict data governance and privacy protocols to ensure the protection of participant information (see AIFS Ethics Process here). AIFS will provide eSafety with the administrative linked data files, linked through the unique identifier. No personally identifiable information will be included. Access to linked datasets will be managed through secure environments approved by AIFS. Data will be stored on eSafety's secure IT system.

We will collect app usage, device metadata and connection metadata using **passive tracking**. The data will be collected and hosted by Wakoopa. The data will be de-identified and will include a unique identifier to enable the data to be linked to survey responses. No personally identifiable information or details about content or communications will be collected. SRC will be responsible for linking passive data with unique participant identifiers, which will be provided to eSafety and stored on eSafety's secure IT system.

Further details on SRC's and Wakoopa's data management, storage, and privacy practices are provided in Appendix W.

Qualitative data will be collected and hosted on VisionsLive during fieldwork and downloaded onto eSafety secure systems at the end of each fieldwork period. VisionsLive is based in England and is EU Regulation 2016/679 (the General Data Protection Regulation) compliant. VisionsLive data centres are ISO27001 certified. They are regulated by the Information Commissioners Office, registration number Z1315831. The VisionsLive platform is accessible only to research team members with an account and password, and to participants with a link sent to their personal email. Participants surnames will not be shared with VisionsLive. The platform creates a record of the focus group that will then be downloaded by the research team for analysis. VisionsLive stores data securely and purges data every 12 months.

Interviews will be conducted, recorded and auto transcribed using Microsoft Teams. Microsoft Teams is eSafety's professional meetings platform. Microsoft Teams automatically deletes recordings and transcripts after 60 days and eSafety staff are able to delete these earlier as needed.

Transcripts from VisionsLive and Microsoft Teams will be downloaded, de-identified, and saved on eSafety's secure IT system. Once uploaded, recordings and identifiable transcripts will be securely destroyed.

De-identified transcripts will be uploaded to Condens for analysis. Condens is a qualitative data analysis tool. eSafety has a Business Plan with Condens which has passed an internal government security assessment.

Data storage and associated timelines

All data will be saved onto eSafety's SharePoint within a restricted access section where only research staff will be given access. All information within this SharePoint site is auditable and backed up to ensure information integrity. SharePoint is set up to be limited to be accessible only to eSafety staff and is rated to manage information up to and including Official: Sensitive. The quantitative data will need to be downloaded and imported into SPSS/Q for the purpose of analysis. Once analyses are complete, this will be re-uploaded to SharePoint for storage and version control. Any files will be securely deleted from the desktop.

All research data will be retained for a minimum of 20 years after completion of this study before destruction in accordance with national archives requirements. These set specific data retention periods depending on the circumstances, as follows. The National Archives of Australia's Records Authority 2018/00153827 applies to eSafety records, and states that

records documenting research that gathers unique or original data or offers significant insight into the regulation of the communications and media industry within Australia or internationally, must be retained indefinitely as national archives. These records include data files and tables. It also states that research that does not offer significant insight into industry regulation issues, but informs industry policy or practice, is to be destroyed 20 years after the action is completed.

eSafety's IT security arrangements are in line with the Protective Security Policy Framework, which is the federal government guideline for information handling and security.

Management of personal information

eSafety has a privacy policy outlining how eSafety handles, manages and protects personal information. eSafety handles information in accordance with its obligations under the *Privacy Act* 1988, the Freedom of Information Act 1982 and the Public Governance, Performance and Accountability Act 2013. eSafety only uses or discloses personal information for the purpose for which it was collected or in other permitted circumstances, such as where consent is given for it to be used or disclosed for another purpose. eSafety will not disclose sensitive information about a person unless they agree or in other limited circumstances, such as when eSafety is required or authorised by law.

Under eSafety's privacy policy, eSafety may collect personal information if it is reasonably necessary for, or directly related to, one or more of the Commissioner's functions or activities under the Online Safety Act 2021. One of eSafety's legislative functions is 'to support, encourage, conduct and evaluate research about online safety for Australians.'

Access to the data

SRC and Wakoopa will have access to data that is collected. Suppliers were evaluated, amongst other criteria, on their capacity to comply with the Australian Privacy Act 1988 and, where applicable, other relevant regulatory frameworks such as the General Data Protection Regulation (GDPR), as part of the procurement process. Detailed information on SRC's and Wakoopa's data handling and privacy compliance is provided in Appendix W.

eSafety and members of the evaluation team identified in this application, and members of the Academic Advisory Group, will also be given access to de-identified data to conduct their own analyses and collaborate on publications.

We will be developing a data sharing principles document, which members will be expected to adhere to. This will be shared with AIFS HREC once developed. Members of the

Academic Advisory Group have also signed MOUs which included agreement to act in accordance with Privacy Principles.

Indigenous Data Sovereignty

In this study, we recognise and prioritise the principles of Indigenous Data Sovereignty, which asserts that Indigenous peoples have the right to govern the collection, ownership, and application of data about their communities, lands, and cultures. We are committed to respecting these rights and ensuring that all data activities related to or impacting Indigenous communities are conducted in accordance with their customs, legal frameworks, and data protocols.

Each stage of this study will be guided by the Maiam nayri Wingara Indigenous Data Sovereignty principles, as outlined below. Our co-investigator, s 47F, is also an executive member of the Maiam nayri Wingara.

Principle 1. First Nations people have the right to exercise control of the data ecosystem including creation, development, stewardship, analysis, dissemination and infrastructure.

First Nations Investigators s 47F and s 47F will be involved in the development of research instruments, including survey and focus group protocols, and reporting to ensure that each stage of data collection supports Indigenous leadership and self-determination. They will also lead the analysis and reporting of Indigenous data, ensuring that study creation and development are led by First Nations expertise, and that data is collected in a way that accurately reflects Indigenous lives and values.

s 47F and s 47F will oversee the analysis of data relating to First Nations young people and their parents and caregivers and will lead the interpretation and reporting of findings on experiences and impacts of the legislation for First Nations families (for example in journal articles or conference presentations). They will also be invited to contribute to and review any evaluative conclusions or discussion related to First Nations young people, parents/caregivers and community within any broader evaluation reports authored by eSafety. Additionally, they will support the future engagement of First Nations people in reviewing relevant study outputs, ensuring that First Nations experience controls data analysis and dissemination.

A sub-section of survey participants will be invited to participate in a session to collaboratively analyse and interpret the survey findings after the 24-month follow-up survey. This invitation will be included in that survey. Only respondents who agreed to be re-contacted for this purpose when completing the survey will be invited to attend. The research team will make special efforts to ensure that First Nations participants have substantial input into overall data analysis.

We note that the present study does not focus on a single First Nations group or community and is not singularly focused on the experiences of First Nations trans and gender diverse people. For these reasons, it is not necessary to prioritise First Nations control over data storage and infrastructure.

Principle 2. First Nations people have the right to data that are contextual and disaggregated (available and accessible at individual, community and First Nations levels).

This study aims to recruit a survey sample of First Nations participants that is large enough for meaningful analysis. We aim to ensure the inclusion of people who are both Aboriginal and/or Torres Strait Islander to allow for disaggregation of the data, which in turn can support meaningful reflection on the implications for First Nations policies or programs, led by First Nations researchers and First Nations people with lived experience of the age restriction (i.e., young people and their parents/caregivers).

Data will be analysed and written-up to ensure that study outputs support First Nations self-determination and leadership, and that analysis reflect First Nations lives and values, including contextualising First Nations data when it is presented.

Principle 3. First Nations people have the right to data that are relevant and empowers sustainable self-determination and effective self-governance.

Study design will be informed by the expertise of First Nations researchers s 47F and s 47F. In this way First Nations people will set the agenda and priorities for data gathering. In addition, we will seek to incorporate lived experience review of evaluation outputs from appropriate peak bodies throughout the evaluation, to support interpretation and translation of the findings. First Nations young people, parents/caregivers, and Peak staff who support the review process will be compensated for their time and expertise. This approach has been used in our previous research, including It's More than Fun and Games, Tipping the Balance, and a New Playground.

Principle 4. First Nations people have the right to data structures that are accountable to Indigenous peoples and First Nations.

When they become available, all research reports from this project will be shared with key First Nations stakeholders and organisations, and with all research participants who indicate they would like to receive them during the research process.

First Nations organisations that we work with on the project will be offered a briefing on the report and be made aware that they can contact eSafety to discuss findings and primary data access via email.

A note will be made in the final report that First Nations organisations can contact eSafety to discuss findings and primary data access.

Principle 5. First Nations people have the right to data that are protective and respects our individual and collective interests.

As outlined above, data will be stored securely, ensuring the privacy of First Nations Participants.

The research is not expected to directly involve access to Aboriginal and Torres Strait Islander intellectual and cultural property. The knowledge and experience of Aboriginal and Torres Strait Islander People(s) will be valued and respected in the conduct of research and the presentation of the findings. Some traditional information and knowledge may be culturally restricted (such as information pertaining to sacred sites and objects). This means it is subject to conditions under customary law, and it is not appropriate to disseminate or publish any culturally restricted information unless consent is granted. We do not anticipate that culturally restricted or sensitive information will be gathered as part of the study. However, if during the course of the project any culturally sensitive information is recorded (e.g. in open text responses) and is identified as such, this information will not be included in the research findings.

Appendix W – SRC and Wakoopa Data Management Plan

REC-0599: Monitoring and outcome evaluation of the Social Media Age Restriction

The Social Research Centre

Privacy, data security, and compliance

All aspects of this research will be undertaken in accordance with ISO 20252:2019 Market, Opinion and Social Research Standard, The Research Society (formerly AMSRS) Code of Professional Behaviour, the Australian Privacy Principles and the Privacy (Market and Social Research) Code 2021. The Social Research Centre (SRC) is accredited under the ISO 20252:2019 scheme (certification number MSR 20015, first issued by SAI Global, on 11 December 2007 and recertified on 24 November 2022 by ISO Experts for a further 3 years to 2025).

SRC's data security protocols are articulated in a Secure Information Policy – the SRC has been accredited to ISO 27001:2013 certification and hosts web applications at Amazon Web Services in Sydney (AWS), a cloud service provider that is certified by the ASD on the Certified Cloud Services List (CCSL).

All senior staff are full members of the Research Society with either Qualified Practicing Researcher (QPR) status or professional accreditation relevant to their role. The SRC is also a member of the Australian Data & Insights Association (ADIA) and bound by the Market and Social Research Privacy Principles/Code.

The SRC is committed to protecting participant privacy and upholding ethical research practices. SRC's standard processes fully comply with the following:

- Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs)
- All applicable state/territory privacy and health records legislation
- Privacy (Market and Social Research) Code 2021
- The Research Society Code of Professional Behaviour
- The ADIA Trust Mark.

The APPs form the foundation of SRC's data privacy practices. SRC's Audit, Risk, and Privacy Committee meets monthly to ensure SRC's procedures are aligned with current privacy best-practice, including the upcoming proposed reforms to the Privacy Act in 2024.

SRC's certification to ISO 20252 aligns with the APPs and along with SRC's other obligations they:

- maintain a publicly available Research Information Privacy Policy (RIPP) that is regularly updated. The RIPP outlines SRC's data handling practices, including details on collection, use, disclosure, access requests, complaint processes, data disposal, website visitor data collection, and information security
- maintain a comprehensive inventory of all information SRC handle (stored, processed, and transmitted) including location, security and access controls
- obtain fully transparent and informed consent from participants before they participate in SRC's research
- provide privacy training to all permanent staff every two years
- implement robust data security measures to minimise the risk of data breaches and to maintain a data breach response plan to effectively address incidents
- conduct security-risk vetting of all subcontractors and suppliers and have formal agreements in place for personal information destruction to ensure information is disposed of securely.

All projects undergo a Privacy Risk Assessment (Threshold Privacy Assessment) during the planning stage. This review process identifies all potential impacts the project may have on individual's privacy and the degree of risk associated with these impacts.

The assessment informs processes and procedures for managing, minimising, or eliminating potential privacy risks. It also determines whether we would recommend that eSafety undertake a formal Privacy Impact Assessment (PIA) in relation to this research.

Secure data storage and handling

The data security procedures adopted by the SRC comply with Research Society Code of Professional Behaviour, ISO 20252:2019 standards, the Australian Privacy Principles and the Privacy (Market and Social Research) Code 2021.

All of the SRC's business critical servers are backed up daily to storage located in AWS' Sydney data centres. The SRC utilises AES-256-bit encryption for all data backups by default. Data from different servers is segmented within AWS to ensure continued security should a storage account credential be compromised.

The SRC maintains a dual fibre-optic AWS Direct Connect links to the Sydney data centres and all backup data flows over this link. No data ever transits over public internet links. All workstations run commercial virus protection and firewall software. Virus definitions are updated hourly.

All workstations run commercial virus protection and firewall software. Virus definitions are updated hourly.

All staff may work from home at any time by connecting through VPN to our Sophos XG Firewall. If connecting from their SRC laptop, normal access to the office network is given. If connecting from a personal PC, they are only able to connect via Remote Desktop. All

VPN connections require Multi Factor Authentication (MFA) in addition to their unique username and password. Remote access to VPN or Office 365 if blocked by default from IP addresses outside Australia.

All sensitive data transferred to and from the SRC is undertaken via Citrix ShareFile. All data uploaded to the platform has an automatic expiration date of 7 days, and access is granted via security groups. The data security procedures adopted by the SRC comply with Research Society Code of Professional Behaviour, ISO 20252:2019 standards, the Australian Privacy Principles and the Privacy (Market and Social Research) Code 2021.

All SRC IT systems that store sensitive information comply with security requirements outlined in the Australian Government Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and follow the Commonwealth's Essential 8 strategies to mitigate cyber security incidents. SRC's data collection platform, Forsta HX is hosted at Azure Sydney using a single-tenant model where Forsta HX servers are dedicated to the SRC. Azure regularly undergoes independent third-party audits to provide assurance that control activities are operating as intended. More specifically, Azure is audited against a variety of global and regional security frameworks dependent on region and industry. Azure participates in over 50 different audit programs.

To further strengthen SRC's cybersecurity posture in 2019, the SRC has become accredited in ISO 27001 at their Melbourne office.

Data Security practices employed by the SRC include:

- physical security (storage of confidential information in locked cabinets / in locked rooms)
- use of multi-level password protection on all electronic storage systems
- limited access to information (i.e. access limited to the project team and other agreed persons on a 'need to know' basis)
- deidentification of the data at the agreed completion of the project
- system cleansing at the conclusion of the project
- cross-cut shredders to destroy in-confidence material
- storing all sensitive information (e.g. the names and contact details of selections) on segregated and encrypted server drives where backups are overwritten every 30 days
- deployment of commercial UTM (Unified Threat Management) devices to protect the internal network from the public network. These devices provide firewall protection, intrusion protection, virus scanning, online content filtering and manage multiple WAN connections.
- cloud hosting of web services at AWS Sydney
- cloud hosting in an ISO 27001 certified Tier 4 Data Centre.

The SRC wherever possible, removes points of failure in server and network designs.

The SRC full Secure Information Policy can be provided on request.

Cloud security at AWS is a shared responsibility with AWS controlling security 'of the cloud' (hardware, infrastructure and virtualisation software providing compute, storage, database & networking) and SRC IT is providing security 'in the cloud' (server, application, encryption, access rights and data). As such, the SRC is addressing all the security risks highlighted in ASD's paper "Cloud Computing Security for Tenants" with AWS recommended solutions highlighted in "Understanding the Australian Cyber Security Centre's 'Cloud Computing Security for Tenants' in the Context of AWS".

Data breach response plan

SRC's Data Breach Response Plan outlines the steps to take upon suspecting a data breach. Employees must immediately report a suspected breach to supervisors and the Data Breach Management Group (DBMG). An incident report template helps gather details about the breach, including the type of personal information involved and how it occurred (malicious attack, human error etc.). If the suspected breach involves a potential information security compromise, the Security Incident Policy is actioned alongside the Data Breach Response Plan. This ensures a comprehensive response that addresses both data protection and information security concerns.

The plan then focuses on containing the breach, recovering lost information (if possible), and assessing the risks. This includes evaluating the potential for serious harm to affected individuals, such as financial or reputational damage. Legal advice is strongly recommended throughout this process. A collaborative decision is made on whether notification is required under the Notifiable Data Breaches (NDB) scheme or deemed appropriate as a voluntary measure. If notification is necessary, the plan outlines the process for notifying affected individuals, law enforcement (if required), and relevant authorities. Finally, the plan emphasises taking steps to prevent similar breaches in the future.

In situations where a potential information security compromise has been identified, the SRC's Information Security Incident Response Policy has five distinct stages: containment, notifying business owners of impacted systems, collection of data relating to information security incidents, remediation of affected services and escalation.

Containment can include disabling access to SRC networks to contain a security incident, disabling system access by locking an account, isolating and temporarily impounding the affected computer and isolating subnetwork access to the network and internet gateways.

Notification requires making attempts to notify the owners of the information systems that are impacted by or suspected of being impacted by an information security incident. Where there are reasonable grounds to believe that criminal or other charges may be laid in relation to the incident, it will be referred to the Chief Operating Officer and then legal counsel.

Data relating to information security incidents will be collected and handled by the CIRT in a way which will allow the Company to use it as evidence in judicial or administrative proceedings if it chooses to do so.

Remediation of affected services involves the return service of disabled services in a manner such that the incident does not recur once the service is resumed.

Escalation ensures accountability. An Information Security Incident Report will be provided to the Chief Information Officer by the Computer Incident Response Team. The report will provide root cause actions taken and any further recommendations. The Chief Operating Officer will report high risk incidents to the Audit & Risk Committee for inclusion into Risk Mitigation Strategies.

SRC will notify eSafety in writing as soon as reasonably practicable after becoming aware of a breach and will take all reasonable steps to minimise the breach, in keeping with s 35 of the Telecommunications Regulations 2021.

SRC will also notify the OAIC and affected individuals regarding eligible data breaches under the Notifiable Data Breach scheme (also Privacy (Market and Social Research) Code 2021 s 28(3)). Under the Privacy (Market and Social Research) Code 2021 s 28(3), we must also notify the Code Administrator (ADIA) of breaches reported to the OAIC. Notifications to affected individuals will include recommendations about the steps they should take in response to the data breach.

Procedures for secure data deletion

The SRC de-identifies any personal information as soon as is reasonably practicable and as soon as that information is no longer relevant or required in identifiable format for the primary purpose of conducting the research according to the research brief provided by eSafety. This is done in a comprehensive manner that ensures that it is not possible to re-identify individual information from any aggregate records. Any files related to SRC's projects are deleted pursuant to SRC's obligations under the Privacy Act 1988 (Cth).

Procedures for ensuring only data necessary for the study is collected during passive tracking

The passive tracking provider (Wakoopa) will not receive any identifiable information. The passive tracking data is a list of events, dates, and times. The passive tracking provider at no point has respondent contact information and restricts information collection to the bare minimum specified by eSafety. At the completion of data collection SRC will provide the IDs to Wakoopa for de-activation. Wakoopa then stops the data capture for those devices. At the same time SRC and non-probability-based panels will send communications to panellists regarding the app uninstallation process, as this must be done by the users themselves. This means if even the user does not uninstall the App, there will not be data going to Wakoopa or SRC.

The basic steps in the passive tracking are as follows:

- Consent is gained
- SRC load unique SRC IDs to the Wakoopa tool
- Wakoopa tools generate a unique passing tracking link specific to each ID
- SRC sends the passive tracking link to consenting research participants
- Research participants install the passive tracking App
- SRC download the passing tracking data.

Procedures for secure collection and transfer to data custodians of consent forms for MBS/PBS and NAPLAN data linkage

SRC anticipate that transfer of consent forms will use secure file exchange protocols; either those of the data custodian or the SRC. Detail of SRC's secure file exchange platform are provided below.

To maintain the principle of separation, the linkage consent will be programmed as a separate survey to the survey data collection with individual-level permissions applied in SRC's data collection platform (Forsta) and storage systems to ensure that staff with access to the personally identifying information used for the data linkage key do not have access to survey data and vice versa. All IDs will be linked by a 'key' so that survey data and PII cannot be matched.

The SRC uses Citrix ShareFile as a secure file exchange facility. ShareFile is an enterprise secure, cloud-based solution which enables SRC to deliver a robust data sharing service, and provides industry-leading security, auditing capabilities, and compliance controls for safe content sharing, allowing the SRC and its clients to safeguard data, documents, content, users, and devices with one solution.

The SRC can control, authenticate, track, and report on who accesses, views, shares, edits, deletes, downloads, and uploads files based on user location, role, and device criteria.

All sensitive, secure and personal identifiable data shared via ShareFile will be stored in Sydney, Australia, at Amazon Web Services EC2 data centre, which has implemented and effectively operates applicable ISM controls relating to the processing, storage and transmission of UNCLASSIFIED (DLM) Australian Government data, and will comply with key industry standards for security, reliability and confidentiality, such as ISO/IEC 27001, SOC 1 and SOC 2, and IRAP.

This facility incorporates the following features:

- Multilayer Security: Granular controls protect encrypted data at rest (with AES), in transit (with SSL), and during access and use.
- Enterprise Key Management (EKM): Company-owned encryption keys allow organisations to safeguard data within private on-premises and cloud repositories.
- Information Rights Management (IRM): The authentication process follows the file itself, ensuring secure access to sensitive content only by intended recipients. Editing, printing, screen capture, and other activities can be restricted, even after the file is downloaded.
- Data Loss Prevention (DLP): ShareFile integrates with existing DLP solutions to restrict access and sharing based on the classification of content inside files, preventing external sharing of sensitive data. DLP helps organisations enforce regulated industry requirements, company governance policies, and security parameters for audit reporting and compliance.
- Security, Global Performance, and Regulatory Compliance: ShareFile ensures reliable performance everywhere and compliance with privacy laws and sensitive data residency requirements (including PCA, HIPAA, HITECH, and SOC-2) in regulated industry sectors.
- SRC does not use customer-managed on-premises Citrix ShareFile storage zone controllers which have been subject to security flaws in the past (for example CTX-CVE-2020-7473).

Subcontractor oversight

Subcontracted non-probability-based panels (Octopus, Thinkfield, Lightspeed, ORU, and PureProfile) abide by industry standards and guidelines as prescribed by the Research Society and the world association of research professionals (ESOMAR). In addition, they hold the following memberships and promote adherence to these guidelines:

- Accredited to ISO 20252.
- Adheres to the ESOMAR guidelines on conducting market and opinion research using the internet.
- Australian Data and Insights Association (ADIA) member.

- Adheres to ADIA privacy principles and fully conforms to the Australian Privacy Principles as detailed in the Privacy Amendment Act (2000).
- Adheres to the Research Society Code of Professional Behaviour and guidelines on the confidential handling and delivery of respondent information.
- ADIA Quality Standards for Online Research (Access panels).
- Adheres to the Australian anti-spam laws.

All subcontractors not certified to ISO 20252 are required to sign an agreement form committing to adhere to the standard. This includes strict confidentiality clauses aligned with the Australian Privacy Principles (APPs), specifically APP 11 for secure storage access, and APP 3 and 5 for consent and participant information management. Additionally, subcontractors must undergo IT compliance checks and, where necessary, IT vetting to ensure APP compliance. SRC's contracts with subcontractors should mirror these requirements, incorporating confidentiality clauses that bind them to APP compliance.

Refer also to Appendix AB - Managing Subcontractors and Suppliers Policy (A.5.22).

Wakoopa

Privacy, data security and compliance

As a GDPR-compliant and ISO 20252 certified provider, Wakoopa adhere to strict data protection and privacy standards that align closely with the principles of the Australian Privacy Act 1988 (including the Australian Privacy Principles, or APPs). While GDPR and the Privacy Act are not identical, GDPR compliance generally meets or exceeds the requirements of the Australian framework, particularly in areas such as transparency, data subject rights, purpose limitation, and security safeguards. Refer to Appendix AC - Technical and Organisational Measures (TOM) for how Wakoopa meets its obligations under Art 32 of GDPR – this attachment is commercially sensitive and is provided only for internal use and not intended to be shared without Wakoopa's authorisation.

SRC will work with eSafety to ensure that any information held by Wakoopa, acting as a data processor, complies with the requirements of Australian Privacy Principle 8 (APP 8) regarding cross-border disclosures. This typically involves one or more of the following measures:

- Ensuring that overseas data recipients are subject to privacy protections similar to those under the APPs
- Obtaining express and informed consent from survey participants for the overseas disclosure of their information; and/or

- Requiring Wakoopa, through contractual obligations, to handle personal data in accordance with the APPs.

Data access

Only the Wakoopa Platform team (6 people) has access to the raw data and the cryptographic keys, usage is logged by AWS and cannot be altered. Access is required for monitoring and reacting to alerts 24x7.

Wakoopa is a data processor, so under legal terms (according to GDPR and equivalent regulations), a data processor may only access and process data in the following cases:

- Based on documented instructions from the data controller: The data controller provides explicit instructions for the data processor to access, process, or consult personal data (Legal basis: Article 29 GDPR — "The processor and any person acting under its authority who has access to data shall not process those data except on instructions from the controller.")
- For the performance of the contracted service:
    - The processor may access data only to the extent necessary to deliver the contracted service, such as technical maintenance, customer support, hosting, or data processing.
    - This must be clearly defined in the Data Processing Agreement (DPA) between the parties.
- For technical or security purposes (Always under prior instruction or authorization from the controller, and only for the time strictly necessary):
    - Access may occur when needed to: Resolve technical or operational incidents, ensure service continuity or Perform maintenance or error detection tasks.
- Due to a legal obligation: In exceptional cases, the processor may be legally required to provide access to competent authorities (e.g., under a court order or regulatory request). However, the data processor must inform the controller before doing so, unless the law prohibits such notification.
- When involving authorized sub-processors: If the processor uses sub-processors (e.g., hosting providers), they may access data only if authorized by the controller and bound by the same contractual safeguards.

As a data processor, Wakoopa couldn't:

- Use the data for its own purposes or those of third parties.
- Share it with other clients or partners. Data collected is not available to any other customers of Wakoopa
- Analyse, enrich, or process it beyond the controller's instructions.

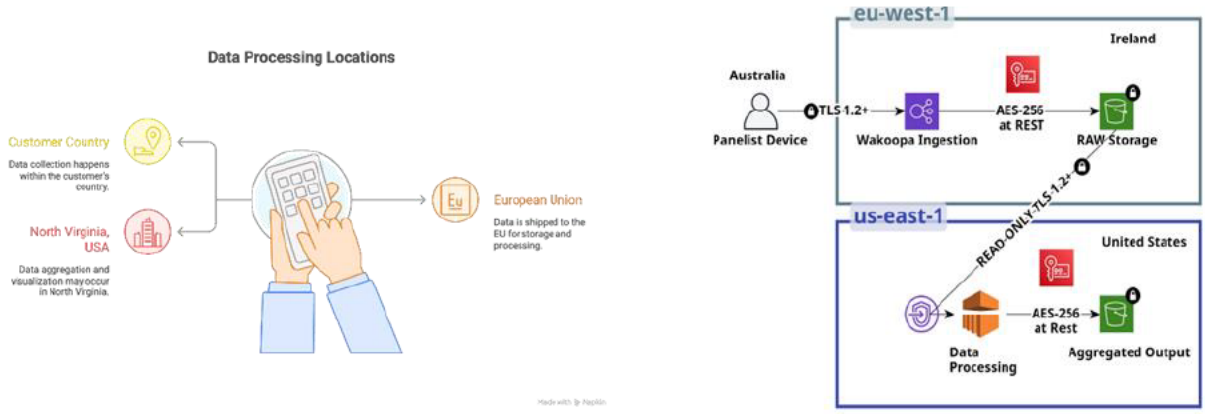
Data transfer

All collected data is sent to Wakoopa via https. Https is a communication protocol for secure communication over a computer network. The data is sent encrypted over the network. For an outsider it is not possible to decode the message.

Data storage

Data is encrypted using AES-256 on-the-fly and at-rest. Collection points are located in the customer country; data is then shipped to the EU for storage and further processing. Some data aggregation and visualisation may occur in North Virginia, USA. See Figure 1 for a visual depiction of this process.

Figure 1. Wakoopa data transfer and storage protocols



Safeguards to ensure passive tracking app does not collect unnecessary or intrusive data

ProxyPlus platform stores only a pseudo-anonymised id of the device, timestamps, telemetry data, plus FQDN/URL and User Agent of the device. TLS decryption is used only to get the URL, other sections regarding the request content are automatically discarded to ensure no other PII is collected, neither accidentally. For the purpose of this study, we will not be capturing URL, as an additional privacy preserving measure.

Data deletion

Data deletion of device related data follows the EU's GDPR ruling for timings and procedures. Once deleted, data is also overwritten as storage consolidation occurs. The default deletion timeline is 12 months after project completion, but earlier deletion is possible if requested.

Data collection will cease for any participants who withdraw from the passive tracking or from the study. At the time of withdrawal participants can also request that their historical data be deleted.

App removal process

The communication regarding a panellist uninstalling the apps used will be SRC's responsibility. From Wakoopa, we can stop tracking the device, but we cannot uninstall the apps.

At the completion of data collection SRC will provide the IDs to Wakoopa for de-activation. Wakoopa then stops the data capture for those devices. At the same time SRC and non-probability-based panels will send communications to panellists regarding the app uninstallation process, as this must be done by the users themselves. This means if even the user does not uninstall the App, there will not be data going to Wakoopa or SRC.

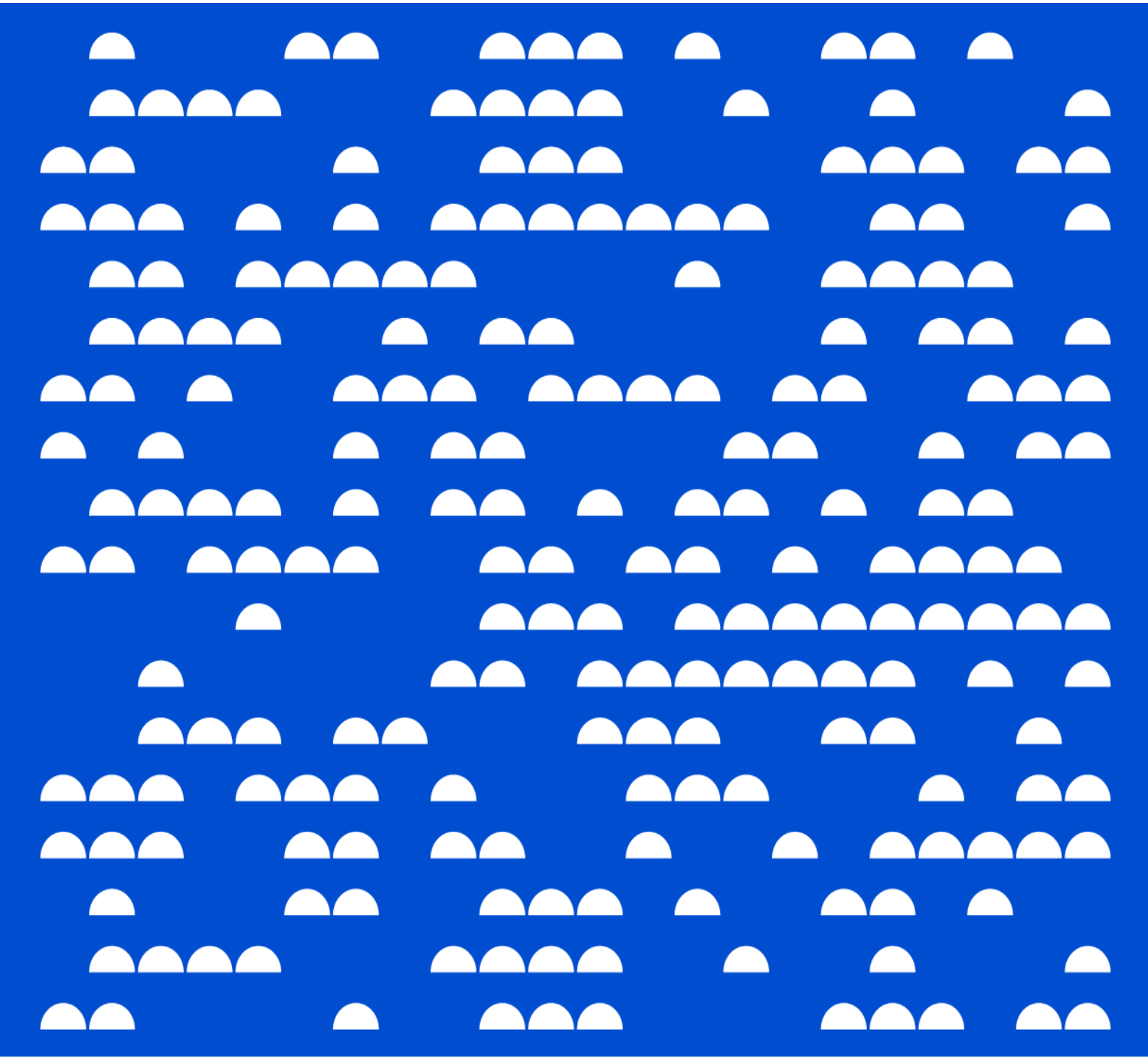
eSafety FOI 26056
Document 5 of 11

Social Research Centre

Evaluation of the Social Media Age Restriction

Proposal

September 2025



s 22

5	Data, privacy and security	Cyber or information security incident; risks linked to linking survey, administrative, and passive data.	Low	Apply stringent encryption, de-identification, and secure local storage protocols. Regular audits against ISO 20252 and Australian Privacy Principles to ensure compliance. Pilot passive data collection to confirm functionality. Limit access to identifiable data.
6	Data quality and integration	Errors or mismatches when combining survey, administrative, and smartphone passive data.	Medium	Establish robust data management and linkage protocols with unique IDs. Use automated validation and cleaning processes. Build redundancy in timelines for integration testing.

s 22

s 22 [redacted]

The SRC de-identifies any personal information as soon as is reasonably practicable and as soon as that information is no longer relevant or required in identifiable format for the primary purpose of conducting the research according to the research brief provided by our clients. This is done in a comprehensive manner that ensures that it is not possible to re-identify individual information from any aggregate records. Any files related to our projects are deleted pursuant to our obligations under the *Privacy Act 1988* (Cth).

The SRC full Secure Information Policy can be provided on request.

s 22 [redacted]

Services Australia Consented Release of Data Request

Office Use Only	**Reference Number:**	
	Date Received:	

Services Australia and the Department of Health and Aged Care are committed to improving Australia's health through the provision of information to health researchers. The *National Health Act 1953* and *Health Insurance Act 1973* include provisions that enable the Australian Government to disclose some health-related claiming information for the purpose of health research. Each request for data will be assessed to ensure disclosure would be within legislative requirements. Approved provision of data is undertaken on a cost recovery basis in accordance with the Australian Government Cost Recovery Guidelines.

s 22

s 22

[redacted]

10. Please provide details of how the electronic data and consent forms will be stored. Services Australia will require the study to retain all confidential information as per their HREC approval, this is normally a minimum of five years, or 15 years if a clinical trial, from the publication of the projects' final report or, if ethics approval require another period.

Please ensure that this information is also included on your Participant Information Sheet to provide a clear picture to the participant on retention and storage of their data. Please refer to page 13 of the 'Services Australia Consented Data Release Guidelines for Individuals and Provider Information' document.

Project-related data will be securely stored by eSafety, AIFS Data Linkage and Integrating Authority (AIFS DLIA) and the online research panel provider. The panel provider is responsible for the management of participant contact data and personal information (including data linkage consent forms). AIFS DLIA and the panel provider will adhere to the separation principle and apply data separation throughout the data life cycle, as follows:

- **Storage:** Identifier and content data securely stored in separate databases.
- **Access:** Limiting the number of roles that staff can have at once and limiting the level of access to project data. Staff are restricted from accessing both identifier and content data simultaneously. Access is strictly on a need-to-know basis.
- **Processing:** Compartmentalisation of functional roles in data management and processing.

eSafety will store deidentified linked PBS and MBS data on eSafety's SharePoint within a restricted access section which only research staff and approved personnel associated with the study can access. All information within this SharePoint site is auditable and backed up to ensure information integrity. SharePoint is set up to be limited to be accessible only to eSafety staff and is rated to manage information up to and including Official: Sensitive.

Conventions maintained by the National Archives of Australia (NAA) apply to eSafety records, and are used to determine how long records must be kept, destroyed or transferred, as authorised under the *Archives Act 1983*, as follows:

i. Where the minimum retention period has expired and the records are not needed for agency business they should be destroyed as authorised in this authority;

ii. Records that have not reached the minimum retention period must be kept until they do; and

iii. Records that are identified as 'Retain as national archives' (RNA) are to be transferred to the National Archives for preservation.

Records that are reasonably likely to be needed as evidence in a current or future judicial proceeding or are subject to a request for access under the *Archives Act 1983*, the *Freedom of Information Act 1982* or any other relevant act **must not be destroyed** until the action has been completed.

A number of Records Authorities (RAs) managed by the NAA are used to inform eSafety's retention and disposal activities. RAs pertinent to eSafety's research activities include:

i. The Australian Communications and Media Authority's (ACMA) Records Authority (2018/00153827) was allocated to eSafety by the NAA; and
ii. The NAA's General Records Authority 37 (GRA 37), which provides more detailed information on retention and disposal protocols for research data and records.

eSafety's IT security arrangements are in line with the Protective Security Policy Framework, which is the federal government guideline for information handling and security.

AIFS DLIA will store project related data in accordance with AIFS's Information Security Policy. This policy is based on the Australian Government's Protective Security Policy Framework (PSPF), the Australian Signals Directorate's Information Security Manual and industry best practice. AIFS's Information Governance Framework provides a framework for overarching data governance. All access to Institute systems occurs via Institute-owned and managed systems, which have been accredited to hold up to and including PROTECTED data. Thereby, AIFS guarantees a 'safe setting and environment' to the secure storage and handling of data, including sensitive information.

The panel provider will ensure that any identifiable material is stored securely either in e-files which are only accessible to approved project staff. All staff will meet the data security requirements for research by Commonwealth Government agencies. Computing infrastructure will provide high-level security from outside hackers and viruses and robust back up facilities. Privacy policy and security procedures (as documented in ISO 20252 Quality Manual) cover the relevant legislation (including the Privacy Act (1988), Crimes Act (1914)). Protection of "In Confidence" data is in accordance with the relevant standards, covering issues such as:

- Physical security (storage of confidential information in locked cabinets / in locked rooms),
- Data transmission
- Prohibition on copying sample files
- Clear-desk policy
- Use of multi-level password protection on all electronic storage systems
- Limited access to information (i.e. access limited to the project team and other agreed persons on a "need to know" basis)
- Server room security, and
- System cleansing at the conclusion of the project.

Researchers will observe standard procedures regarding the security of any computer-based data, including electronic data files being closed and screen locks being activated when out of the office for short periods, and users logging off the computer when away from the workplace for periods greater than one hour.

The following privacy preserving dataflow will be adopted to facilitate linkage for this Study:

- The panel provider supplies the contact information directly to Services Australia
- Services Australia match the cohort to Medicare and extract the MBS and PBS records
- AIFS receives de-identified MBS and PBS data from Services Australia. AIFS then link the MBS/PBS data back to the survey data using a linkage ID provided to us by the panel provider.
- AIFS provides linked, deidentified dataset to eSafety for analysis.

As described in the Participant Information and Assent/Consent Forms (see **Attachment P, Q, R**), participant contact information will be securely stored for at least seven years by the online research panel provider following the completion of the study. If a participant chooses to withdraw their participate in the study, the study would no longer collect data from them. If they had previously provided consent for data linkage, they would need to explicitly notify the study if they wanted to withdraw consent to any further data linkage. Participant withdrawal consent forms are provided in **Attachments S and T**. Data previously released to researchers would continue to be used and form part of the evaluation study.

s 22

Risk ID	14
Risk status	Active
Date risk identified	9/29/2025
Risk area/ category	Data privacy and security
Description of risk	Cyber or information security incident; risks linked to linking survey, administrative, and passive data
Consequences	Exposure of sensitive and identifiable personal data; breach of privacy and confidentiality; legal and regulatory repercussions; loss of trust among participants and stakeholders; disruption to evaluation activities; reputational damage to the organisation and partners.
Consequence level*	Critical
Likelihood	Unlikely
Risk rating**	High
Mitigation strategies	Fieldwork supplier to apply stringent encryption, de-identification, and secure local storage protocols. Regular audits against ISO 20252 and Australian Privacy Principles to ensure compliance. Pilot passive data collection to confirm functionality. Limit access to identifiable data. Data minimisation protocols in place Adherence to eSafety Research Data Management protocol; consider privacy threshold asssessments/ privacy impact assessments.
Risk treatment option	Avoid the risk
Response action	1. eSafety's Privacy Officer was involved in the procurement and contract negotiation for the fieldwork provider and their subcontractor responsible for passive data collection by; • Reviewing and advising on the Statement of Work with the fieldwork provider, made pursuant to the Commonwealth MAS (Management Advisory Services) Panel Head Agreement which requires service providers to comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) and to ensure that their subcontractors are similarly contractually bound. • Collaborated with eSafety's Data Governance lead to engage the fieldwork provider (including a member of their privacy team) and passive data provider, and reviewing the passive data provider's proposal and documentation. • Reviewing and advising on the Memorandum of Understanding with the data linkage provider, the Australian Institute of Family Studies (AIFS), which is one of the Australian Government's four Accredited Integrating Authorities and Accredited Data Service Providers. This accreditation is granted by the Office of the National Data Commissioner and reflects that the organisation meets stringent legislative and governance requirements set by the Minister for Finance and the National Data Commissioner. • Reviewing and advising on the Human Research Ethics Committee application (which included a data management plan) and all participant and parent consent forms for the study. 2. Technical documentation, data security arrangements ISO 20252 Certifications and whether survey outputs could contain any personal information was considered by the Privacy Officer before the providers and their proposals were approved; based on these above considerations, eSafety's Privacy Officer concluded that a privacy impact assessment (PIA) was not required. 3. eSafety's fieldwork officers completed a privacy threshold assessment (PTA) and concluded that a PIA was not required. 4. eSafety's considerations of privacy risks is ongoing across its operations. eSafety will complete a PIA if considered necessary at a future date.
Mitigation status	In progress

Outlook

Re: Update on consent forms [SEC=OFFICIAL]

From s 22 @aifs.gov.au>
Date Mon 10/13/2025 6:30 PM
To s 22 @eSafety.gov.au>; s 22 @esafety.gov.au>; s 22
s 22 @aifs.gov.au>
Cc s 22 @eSafety.gov.au>

Hi s 22

Below is an extract from the *AIFS Data Confidentialisation Policy*, hope this is helpful. We are just checking with s 22 whether the policy needs to be provided, or if it is sufficient to provide just the extracted info below.

> AIFS' Data confidentialisation and disclosure control policy is designed to manage disclosure risk effectively, preventing re-identification, privacy breaches, and other misuse of data.
>
> **Confidentiality Policy and Processes**
>
> Our Data confidentialisation and disclosure control policy applies to all staff and contractors handling personal data. This policy ensures that effective and appropriate controls are implemented to mitigate privacy, confidentiality, and re-identification risks. It provides auditable evidence of data confidentiality and disclosure protection controls.
>
> **Confidentiality and Output Checking Manual**
>
> The policy includes a comprehensive confidentiality and output checking manual that provides guidelines for assessing and treating re-identification and disclosure risk in microdata. It includes strategies for mitigating identification risk in both microdata and disseminated data outputs.
>
> **Arrangements for Vetting, Confidentialising, and Monitoring Outputs**
>
> We have established detailed arrangements for vetting, confidentialising, and monitoring outputs as part of the policy. This includes:
>
> - **Assessment**: Assessing microdata for re-identification risk and applying appropriate treatments to minimise disclosure risk.
> - **Treatment**: Implementing controls to reduce the level of detail in records that present re-identification risk.
> - **Review**: Comparing treated data against planned objectives and re-assessing if necessary.
>
> **Policies, Processes, and Methodology for Managing Disclosure Risk**
>
> The policy outlines various methods for managing disclosure risk and de-identifying data, including suppression, aggregation, and perturbation. These methods are applied based on a detailed assessment of the data and its intended use.
>
> **Managing Data Confidentiality Breaches**
>
> The policy also includes comprehensive procedures for managing data confidentiality breaches. This involves documenting key confidentialisation steps, retaining evidence of reviews, and archived as part of the formal review process.

Thanks

s 22
---
s 22
Manager | Data Linkage and Integration
Data Linkage and Integrating Authority

Australian Institute of Family Studies
Level 4, 40 City Road, Southbank VIC 3006, Australia
Tel: s 22

General Manager Decision Memo

To	s 22 General Manager, Corporate and Strategy Group
CC	s 22 Executive Manager, Strategy, Engagement and Research
Consulted	s 22 Manager, Data and Information Management s 22 , Legal Services Division
From	s 22
Subject	SMMA Evaluation: Passive tracking technology selection
Purpose	To seek your ag*reement to formally approve* Wakoopa as the specialist provider sub-contracted by the Social Research Centre to provide passive data collection for the SMMA evaluation.
Timing	Urgent
Recommendation	**Agree** that Wakoopa be sub-contracted by the Social Research Centre to provide passive data collection services for the SMMA evaluation.
General Manager	1. Approved / ~~Please discuss~~
Signed and dated by General Manager s 22	Date: 24 October 2025

s 22 [redacted]

The selected technology – Wakoopa

Based on this assessment, Wakoopa was deemed most suitable for this study. Key reasons for selection include:

s 22 [redacted]

- Customisable data capture: The platform can be configured to collect only data essential for the study, ensuring privacy and compliance.

s 22 [redacted]

- Privacy-preserving design: Participants do not provide direct identifiers; instead, they enter a unique key supplied by the panel.
- Regulatory compliance: Wakoopa complies with the EU General Data Protection Regulation (GDPR), which we consider to be substantially similar to the Australian Privacy Principles (Privacy Act 1988) and eSafety's Privacy and Collection Notification Policy. GDPR compliance generally meets or exceeds the requirements

Risks and sensitivities

Legal and privacy risks

The Legal Services Division attended a briefing with Wakoopa and SRC, and have reviewed all relevant materials. They have advised that they are comfortable with the SRC (and Wakoopa as a subcontractor) being engaged through an Order for Services under the Head Agreement. They note the following in their advice:

- the Head Agreement is very robust in terms of privacy and security requirements and ensuring that subcontractors are engaged on similar terms. Importantly, both SRC and Wakoopa will need to comply with the APPs and notify us of any eligible data breach. The Head Agreement provides us with a standard right to terminate our Contract with SRC for default, and to terminate for convenience with 10 business days' notice.
- eSafety has decided that no URLs will be collected by Wakoopa, and therefore Wakoopa will not be collecting or holding any personal information of participants. This is considered to be the most prudent approach and therefore they have concluded that this engagement is very low risk from a privacy perspective. APP 8 (which relates to overseas disclosure of personal information) will not apply in relation to the data collected and handled by Wakoopa as they are not collecting any personal information.

s 22

eSafety FOI 26056
Document 10 of 11

Memo addressing AIFS Human Research Ethics Committee feedback

To: AIFS Ethics Committee Secretariat

From: s 22 Manager, Research and Evaluation, eSafety Commissioner

Date: 29/10/2025

Project title: Monitoring and Outcomes Evaluation of the Social Media Minimum Age

Ethic number: 2025/06

Thank you for your feedback on the Monitoring and Outcomes Evaluation of the Social Media Minimum Age and related materials. This application was considered and given Conditional approval on 23/09/2025, subject to ethical issues and requests for revisions being addressed to the satisfaction of the AIFS HREC.

We have taken the opportunity to consider your feedback and make revisions in response to the Committee feedback. We have noted our specific actions in relation to each item of feedback below.

Feedback/comments	Action undertaken
Clarification required	
s 22	

Feedback/comments	Action undertaken
	s 22
Clarify how the data sent overseas will be stored, managed, retained, and destroyed.	The de-identified data will be securely transferred to overseas collaborators via a shared SharePoint folder managed by eSafety. This controlled-access platform ensures confidentiality and integrity during transfer and storage. To enable analysis using tools such as SPSS and Q, collaborators will temporarily download the data to their secure institutional servers, which have restricted access and comply with institutional data governance protocols. Once analysis is complete, the files will be saved back to the secure SharePoint folder, and the local copies will be securely deleted from the institutional servers to ensure data is not retained beyond its intended use.
Please confirm whether the deidentification process will include measures to protect confidentiality, such as the removal of records with low cell counts. Clarification on this matter is essential to ensure that the data is adequately protected before it is shared with overseas research collaborators.	We can confirm that only de-identified survey data files are provided to eSafety by the fieldwork supplier, and as such, we do not hold any personally identifying information (PII) in the survey files. No PII will be passed on to our collaborators. We understand the concerns around low cell counts, particularly when triangulating multiple data points (e.g., demographic characteristics), which may increase the risk of re-identification. While we are committed to protecting confidentiality, we also recognise the importance of capturing the voices of diverse Australians, including those from smaller population groups. Therefore, we will take a balanced approach: • We will limit the demographic variables shared to only those required for analysis. For example, postcode will be recoded into remoteness and SEIFA categories and then removed from the shared dataset. • Targeted analyses of First Nations participants will be conducted by our First Nations researchers, s 47F and s 47F . Given the higher risk of low cell counts in this subgroup, we may choose not to share this variable with overseas collaborators if cell sizes are too small.

Feedback/comments	Action undertaken
	• We will also consider data reduction techniques, such as combining variable categories, where small cell counts are observed, to further reduce re-identification risk.
s 22	[redacted]

Feedback/comments	Action undertaken
s 22	
Provide the specific protocols and guidance from AIFS for managing the risk of re-identification in linked databases, beyond stating that expert advice will be followed in section E.2.2.	Please find the relevant guidance from AIFS for managing the risk of re-identification in linked databases in Section E.2.4 and copied below of ease of reference: AIFS' Data confidentialisation and disclosure control policy is designed to manage disclosure risk effectively, preventing re-identification, privacy breaches, and other misuse of data. **Confidentiality Policy and Processes** AIFS' Data confidentialisation and disclosure control policy applies to all staff and contractors handling personal data. This policy ensures that effective and appropriate controls are implemented to mitigate privacy, confidentiality, and

Feedback/comments	Action undertaken
	re-identification risks. It provides auditable evidence of data confidentiality and disclosure protection controls. **Confidentiality and Output Checking Manual** The policy includes a comprehensive confidentiality and output checking manual that provides guidelines for assessing and treating re-identification and disclosure risk in microdata. It includes strategies for mitigating identification risk in both microdata and disseminated data outputs. **Arrangements for Vetting, Confidentialising, and Monitoring Outputs** We have established detailed arrangements for vetting, confidentialising, and monitoring outputs as part of the policy. This includes: • **Assessment**: Assessing microdata for re-identification risk and applying appropriate treatments to minimise disclosure risk. • **Treatment**: Implementing controls to reduce the level of detail in records that present re-identification risk. • **Review**: Comparing treated data against planned objectives and re-assessing if necessary. **Policies, Processes, and Methodology for Managing Disclosure Risk** The policy outlines various methods for managing disclosure risk and de-identifying data, including suppression, aggregation, and perturbation. These methods are applied based on a detailed assessment of the data and its intended use. **Managing Data Confidentiality Breaches** The policy also includes comprehensive procedures for managing data confidentiality breaches. This involves documenting key confidentialisation steps, retaining evidence of reviews, and archived as part of the formal review process.
Clearly state that data will be shared with overseas collaborators and explain how it will be stored and managed abroad to ensure informed	We have added the below statement to the Parent PISCF: *"Some of the researchers are based overseas (in the United States and United Kingdom), and de-identified data will be securely shared with them via a protected*

Feedback/comments	Action undertaken
consent (Attachment H: Parent PISCF)	*SharePoint folder. The data will be stored on secure University servers with restricted access and will be deleted once analysis is complete."*
s 22	