Contents

1.0 Introduction

During the last two decades information technology, including the use of email and the Internet (especially in the last few years, social media) have had a substantial impact upon the design and conduct of human research across nearly all disciplines and methods (including interdisciplinary projects where the researchers are interested in human-technology interactions).

Reports, such as those released by Sensis (2015) and Cowling (2015) have highlighted the degree to which the majority of Australians have daily access to the Internet and email, and the degree to which it is involved in many elements of our daily lives. The Australian experience echoes international trends with regard to access to technology and the world wide web – in part driven by smart phone, other handheld devices and Wi-Fi (Kemp 2015). The Sensis Social Media Report (May 2015) indicates that 79% of Australians accessed the Internet on a daily basis and 52% of Australians accessed the Internet 5 or more times a day. Discussion about the degree to which Australians access social media on a daily basis can be found at 5.13 of this Booklet. The number of connected devices in Australian households has also increased with a significant shift from desktop computers to laptops and in the last few years to 'post pc-era devices' (e.g. smart phones and tablets).

These trends offer new opportunities across many research areas and endeavours (e.g. in terms of recruitment, data collection, the transport of data, data analysis and retesting). This also provides opportunities for researchers to remain engaged with potential participant pools in a way that would have been impossible only a few years ago. It should however be noted that not all Australians have easy, private access to these technologies with socio-economic status, age, geographic location and other factors having an impact on access. When employees have access to the Internet and email at work there may be restrictions on how it can be used. (e.g. a public sector staff member may only be able to access a small number of web sites that have been authorised by the employer). For this reason researchers should carefully consider the impacts of using such technology in a project (e.g. so a group of potential participants are not excluded and a potentially important perspective is not lost).

The use of such technologies also can involve a number of significant ethical challenges that need to be carefully considered and addressed. Failing to do so might not only be an ethical concern it could undermine the quality and impact of a project.

As is often the case with research ethics challenges they can be avoided, or at least mitigated with some preparation.

This Booklet of the *Griffith University Research Ethics Manual* is intended to assist researchers who are planning and conducting a human research protocol where such technologies will be utilised. It is also a resource for a research ethics reviewer considering a proposed project.

Back to contents

2.0 National guidelines

The *National Statement on Ethical Conduct in Human Research* is the Australian reference for human research ethics matters.

The *National Statement* is largely silent on the ethical considerations for online research and the use of information technology in human research, however the core ethical principles described in Section 1 of the *National Statement* do apply to such research. The discussion about matters such as consent and privacy do apply to online and other computer-based research, but its not without some peculiar challenges.

Back to contents

3.0 Use of computers (desktop/laptop)

Computers can be employed for a wide range of purposes across most research disciplines. If the term computer encompasses tablets and smart phones computers may be involved in most stages of a human research project (see 6.0 for more about such devices). The rapid pace of change makes a complete and up to date discussion in a booklet of the GUREM impractical. The subsequent sections of the booklet discuss some specific issues and the associated ethical considerations (e.g. social media and research at 5.13 and data security at 8.0).

Below are some general ethical considerations for the use of computers in human research. Please forward any suggested additions to this section to the Office for Research (see Contacts).

3.1 Epilepsy and other physiological reactions

Some neurological conditions like epilepsy can be triggered, or otherwise exacerbated, by watching/interacting with a computer screen or tablet. If a project will involve participants watching content on a computer screen, or interacting with a computer the researchers should consider how this risk should be managed. Example strategies include:

i) warning potential participants in the consent (and perhaps recruitment) materials that participants will be watching/interacting with a computer so individuals can self-screen themselves;

ii) whether in addition to the kind of information provided at i) specific reference to the risk of epilepsy and other conditions should be discussed (this might be appropriate where the activities/tests are known to cause such reactions);

iii) whether, in addition to the kind of screening discussed at i) and ii) the potential participant pool should be screened by a tool to identify whether they have a condition that makes participating unwise (this might be appropriate where the potential participant pool is vulnerable, in an unequal relationship, or a researcher feels there are other reasons for additional precautions).

Additional precautions may be required if potential participants do not regularly view similar content on a computer screen (because they maybe unaware that they are prone to adverse reactions). Researchers should be prepared to explain the reasons for the screening and the potential harms (even though in most cases the chance of an adverse reaction may be minimal).

Despite considering the above matters, researchers should have a prepared plan so that in the event a participant has such a reaction (e.g. because of an undiagnosed condition) they will be ready to appropriately respond. Such a plan might include: immediate response and individual care; accessing emergency assistance; arrangement for a safe journey home; and urging an individual to consult a qualified health professional).

This may also be a consideration for members of the research team (i.e. a member of the research team who is supervising the activity having an adverse reaction).

The above matters should be discussed in the application for research ethics review. See Booklet 9 of this Manual for more about risks in research, Booklet 21 for more about recruitment and Booklet 22 about consent.

3.2 RSI and other physical harms

Some testing on a computer can involve quick and/or repeated tasks for a period of time (e.g. clicking a button in response to visual stimuli). It is important to recognise that such activities can be a source of harm (such as repetitive stress injury) – even though in many cases the harm may simply be temporary discomfort that lasts only for a short time.

If a project will involve an activity (such as repeatedly clicking a mouse) the researchers should consider how this risk should be mitigated, for example:

i) warning potential participants in the consent material (and perhaps recruitment material) what participation will involve so individuals can self-screen themselves (e.g. if they have an existing injury or feel they are particularly at risk of such an injury);

ii) whether the design of the equipment is ergonomic or otherwise designed to minimise such physical harms;

iii) whether to modify the testing to minimise the duration of the testing and to provide for sufficient rest breaks;

iv) reinforcing to participants that they should indicate if they need to pause or stop the test; and

v) whether, in addition to the kind of screening discussed at (i) the potential participant pool should be screened by a tool to identify whether they have a physical condition that makes participating unwise.

Researchers should be prepared to explain the reasons for the screening and the potential harms (even though in most cases the chance of an adverse reaction might be minimal). Researchers should remain reflective during testing to consider whether the experience of participants requires any refinement or

change to the test. Concern for participants must be given pre-eminence ahead of the objectives of the research.

The above matters should be discussed in the application for research ethics review. See Booklet 9 of this Manual for more about risks in research, Booklet 21 for more about recruitment and Booklet 22 about consent.

3.3 Consent and emotional responses

Some projects can involve showing participants material such as images or videos with a view to analysing their response. It may be that this content could be highly sensitive or distressing.

If a project will involve showing participants such material researchers should consider how this risk should be mitigated, for example:

i) warning potential participants in the consent material (and perhaps recruitment material) that they will be viewing material that some people might find distressing so individuals can self-screen themselves;

ii) further to (i) researchers should consider whether it is prudent to be more specific about the subject matter of the material;

iii) whether to provide free-to-user appropriate counselling support to participants;

iv) whether to conduct some form of debriefing or other activity to 'extinguish' any negative reactions;

v) reinforcing to participants that they should indicate if they need to pause or stop the test; and

vi) whether, in addition to the kind of screening discussed at (i) and (ii) the potential participant pool

Inset 1 – Inability to respond to the risks - A real Griffith University research project related to risky behaviour, happiness and matters that some people might have found embarrassing. The participant pool was recruited via social media. The data collection method was a survey.

The research team were mindful that some participants might self-edit their responses if they would be identifiable by the researchers (even if they wouldn't be identifiable by third parties).

When designing the project the researchers identified that some participants might be struggling emotionally or dealing with depression. The consent materials provided the details of a free-to-the-user community support service and urged participants to contact that service if they were in need of assistance.

In the survey response of one participant, they indicated they were contemplating suicide in the near future.

If the researchers could identify the individual they would almost certainly have taken prompt action to ensure the individual received urgent assistance – perhaps even going so far to contact the police. Given the actual situation the research team was unable to take any such action.

It is easy with the benefit of hindsight to say this situation was predictable and could have been avoided. There is no way to know where the participant was located, much less who they are. We can only hope that this was prank in very poor taste, rather an actual intent to commit suicide.

There are indeed situations where anonymity may be the only circumstance where participants are truly honest. Even with an apparently innocuous topic, participants might use a research project to make such statements or other disclosures where some form of action would be required.

The consent material did provide details of sources of appropriate counselling support. Perhaps this could have been reiterated at the end of the survey and other more technically involved triggers might have been designed to prompt a participant to identify themselves so assistance could be provided.

As a general principle researchers should always consider this potential shortcoming/failure of de-identified data collection.

In the event of a similar occurrence researchers must promptly notify the Office for Research (see Contacts) and consider debriefing/support for the researchers/others who may have themselves become distressed by the experience

should be screened by a tool to identify if they live with a psychological condition that makes participating unwise).

Researchers should be prepared to explain the reasons for the screening and the potential harms. Researchers should remain reflective during testing to consider whether the experience of participants requires any refinement or change to the test. Concern for participants must be given pre-eminence ahead of the objectives of the research.

It may also be that an emotional reaction may also be a consideration for members of the research team (e.g. research assistants/junior members of the team might be distressed by the materials).

is outside the scope of the University's human research ethics arrangements and so does not require ethical review.

The above matters should be discussed in the application for research ethics review. See Booklet 36 of this Manual for more about the use of audio-visual material in human research, Booklet 9 of this Manual for more about risks in research, Booklet 21 for more about recruitment and Booklet 22 about consent

***Commentary Inset 2* – Administration of incentives and anonymous data collection** - There are in fact numerous ways to conduct anonymous data collection, such as an anonymous computer/web-based survey, administer an incentive. while preserving the anonymity of responses.

A common strategy is outlined below:

1. After completing the survey/test procedures the participants are presented with a separate form to register for the incentive.

2. The registration details are stored in a separate table that is unmatched with the research data.

3 If there is concern about a dependent relationship between the participants and the researchers and if there is concern about the researchers knowing the participatory status of individuals – Someone without a relationship with the participants (e.g. the school admin officer) organises the incentive, without revealing to the researchers the names of the participants.

Such an arrangement can preserve the anonymity of response but allow participants to receive the incentive.

Whatever arrangements are used, these must be explained to the research ethics reviewers (in the application for ethical clearance), and to potential participants (e.g. in the consent materials). In some cases it might be helpful to outline the arrangements in the consent material. The description should clearly explain whether the researchers will know who has participated and what individuals have said.

Example: "Your entry into the prize draw will be stored separately to your test results and there will be no link between the two. The prize draw will be administered by the School Administration Officer. He will keep confidential that you participated in the research. After administering the prize draw he will delete the prize draw entries. This means that the researchers will not know who participated and the Administration Officer will not be able to link your prize draw entry to your test results.

Previous experience has been that, if the arrangements are not explained, some participants may worry that the researchers are not being entirely honest about participation being anonymous.

3.4 Anonymous participation and limited capacity to respond to risks

When a planned research project will explore highly emotive, sensitive or psychologically confronting matters (e.g. illegal behaviour) it may seem advantageous to collect the data in a manner where personally identified information is not collected (e.g. identifying information about respondents is not sought so it is not possible to associate individual participants with individual responses). This may be a risk management strategy (e.g. with the example above, if even the researcher cannot identify individual respondents there would be negligible legal risks to the participants).

It should however be remembered that such circumstances are likely to impede researchers from proactively managing some risks (see Commentary 1 inset for a real example). Before electing to conduct

data collection in a personally de-identified form, researchers should carefully consider its impact upon their ability to manage risks.

This should be discussed in the application for research ethics review and to potential participants (typically in the consent material). See Booklet 22 of this Manual for more about consent, Booklet 40 for more about the exposure of illegal of illegal behaviour in human research and Booklet 9 of this Manual for more about risks in research

a. The participant group can be characterised as vulnerable.

b. The information obtained is recorded in such a manner that participants can be identified, directly or through identifiers linked to the subjects, and that identification is likely to be considered problematic or a cause for concern by the participants.

c. The information obtained is recorded in such a manner that any disclosure of the participants' responses/results outside the research team could reasonably place the participants at risk of criminal or civil liability or be damaging to the participants' financial standing, employability or reputation.

Commentary Inset 3 – Educational value of information technology in the classroom - It is important that we recognise that not everyone believes information technology (e.g. tablets or computers) can make a positive contribution in the classroom.

In recent years a parent raised a concern with the Office for Research with regards to a project that was looking at how tablet computers were being utilised as an embedded component of a sequence of lessons. Her concerns were:

1. The language in the consent material suggested the researcher had prejudged that tablet computers in the classroom were valuable; and
2. The research activity was a distraction from her child's learning.

Parents can sometimes have an existing disagreement/dispute with their child's school and researchers can unwittingly stumble into these disputes, as was the case in the above real example.

Even though the above matter was mediated and resolved, it does highlight the importance of recognising that there are differences of opinion on questions like "is a tablet computer in a classroom anything more than a bit of fun for the children?"

d. The research deals with sensitive aspects of the participants' own behaviour, such as sexual preference, illegal conduct, use of alcohol, drug use, or includes information about health status.

3.5 Anonymous participation and incentives

In some cases potential participants will be offered an incentive for participating in a project (e.g. all participants will be entered into a draw to win $100). In cases where the data collection measures will not collect identified data it may seem that the process for entering into the prize draw (e.g. a student entering their name and email as their entry into the draw and the system knowing they have in fact participated) will undermine the anonymity of participants.

Two common solutions to this problem are discussed in Commentary 2 inset). The approach selected by a researcher should be discussed in the application for research ethics review and in the consent materials for potential participants.

See Booklet 21 of this Manual for more about the offering incentives to encourage participation and Booklet 22 for more about consent.

3.6 School-based work and educational value

When planning research in a compulsory education context (e.g. with Grade 1 school students) researchers should carefully consider:

i) Whether the research activity is to be conducted as part of normal classroom activity;

ii) whether the research activities will impact upon regular school activities or otherwise distract students from their regular learning; and

iii) ?be aware that not all parents or other members of the school community will agree that computers (e.g. tablet devices) being in the classroom is a good thing (see Commentary 3 inset for further discussion on this matter).

This should be explained discussed in the application for research ethics review and to potential participants (typically in the consent material). See Booklet 22 of this Manual for more about consent and Booklet 24 for more about research with children and young people.

Back to contents

4.0 Email

Anecdotal evidence suggests that, thanks to 'free' email services like Hotmail and GMail, the number of Australians with at least one email address is greater than the levels of people with regular/home Internet access. For this reason, it can often be sensible, cost effective, and efficient for a researcher to use email during the conduct of a research project.

Some of the more typical uses of email during the recruitment, consent, data collection and other interactions with research participants, is discussed below, as well as some of the ethical issues associated with those uses.

It is important for researchers to bear in mind that email is not secure (see 4.10 for a discussion on why this is the case). The potential for email communications not to be secure should be borne in mind for all of the matters discussed below.

4.1 Identification of potential participants - Email list

One way in which a researcher can find or identify potential participants is by accessing an email list (e.g. one way of identifying the staff of a business to approach about participating in a research project could be to access a list of employee email addresses).

An important ethical, and indeed in some cases regulatory, consideration is the degree to which the list is publicly available. This may raise considerations such as respecting the privacy of the individuals who appear on the list, and the degree to which the individuals have a legally protected right of privacy. These issues can be even more important for personal, rather than public/professional, lists (e.g. access to a public list of work email addresses might be considered to be less of a concern than access to a list of email addresses of persons who are members of a social group - even if the holder of this list provided the information to the researchers). These issues can become acute when the list relates to sensitive personal matters (e.g. a list of email addresses of persons who live with a chronic medical condition – this could be a legal concern even if the custodian of the list provides it to the researchers).

Regulatory privacy considerations mean that, even when a researcher has authorised access to a list for another purpose (e.g. for teaching purposes), they may not be able to use that list to identify potential participants for research purposes.

There can be appropriate strategies (e.g. the holder of the list distributing recruitment material on behalf of the researchers) to enable the use of email lists. However, these will need to be identified, discussed and endorsed during the research ethics review of the project.

See Booklet 21 of this Manual for more about the appropriate identification of potential participants and Booklet 23 of this Manual for more about ethical and regulatory privacy considerations.

4.2 Initial contact with potential participants - Email lists

In addition to lists of email addresses being useful to identify potential participants in research (see 4.1), such lists can also be useful to enable researchers to make initial contact with those potential participants (i.e. by sending them an email about the research project).

The same ethical and regulatory privacy issues that were identified at 4.1, also apply to researchers employing email lists in this way.

In some cases, a specific approval will be needed from the custodian of the list to use it for the purpose of initial contact with potential participants.

As per provision 5.2.23 of the *National Statement* the text for this first contact email must be submitted for prior approval. In many cases, this text can be approved by the Office for Research, but in some cases (i.e. where there are serious risks or very significant ethical issues), the text will need to be reviewed executively (by the Chair or Deputy Chair of the Griffith University Human Research Ethics Committee (GUHREC)) or even at a meeting of the GUHREC. Ideally, the text for this initial contact text should be provided as an attachment to the application for ethical clearance.

4.3 Initial contact with potential participants - Email group addresses

An email group address or listserv address refers to a single email address (such as users@communityorganisation.org.au) which delivers to multiple people.

One distinct advantage of the use of a group address is that the researchers will not know the individual email addresses of the potential participants, which removes the ethical and regulatory privacy concerns that relate to the use of lists of email addresses (see above).

In most cases, a specific approval will be needed from the custodian of the group address to use it for initial contact with potential participants (e.g. the approval of the head of academic element is likely to be required for the research use of a group address that delivers to all higher degree students in that academic element). This approval is likely to relate to governance considerations (e.g. is the element satisfied with the list being used for research purposes, are there any duty of care considerations, what else is going on in the element at the moment?).

As discussed in 4.2, a copy of the text that will be sent to the group address will need to be reviewed and approved prior to its use.

The provision of a copy of the approval for the use of the group address for the particular research is also likely to be a condition of ethical clearance for the project.

4.4 Email and consent

A key element of the design of ethical human research is the mechanism to ensure that potential participants are afforded the opportunity to make an informed and truly voluntary decision about their participation in the research. You can find more information, discussion and guidance about consent in Booklet 22 of this Manual.

There must be an appropriate consent mechanism for email-based research. However, there are a number of appropriate consent mechanisms to chose between, and the selection of a mechanism for a project must be based upon the specifics of the research, the potential participant pool, the context and the preferences of the research team.

One of the most common approaches is for the information sheet to be sent to potential participants as an email, and the individuals respond with an email back to the researcher(s) to indicate that they understand what their participation will entail and that they consent to participate in the research. If participation is otherwise to be anonymous (i.e. not even the researchers know who is participating, and they cannot associate data with individuals), the information sheet might direct them how to participate

Commentary Inset 4 – Identifying information embedded into electronic files - Some software, such as the components of the latest Microsoft Office suite embed personal information when a file is saved (including the name of the registered user and the designation of the computer used). The information can be retrieved with two mouse clicks.

When researchers will be receiving electronic files from participant (e.g. a survey completed in MS Word) there is at least the potential for the respondents to be identified.

For many research projects, being able to assign a name to a response may not in practice be enough to identify a participant (because the size of the potential participant pool is so large and/or does not include persons who are known to the researcher). In other cases, the subject matter of the project might make potential identification not a significant concern.

However, for some projects the potential identification of respondents could be a real and serious concern.

For example: A lecturer knowing which of their students from a course they are coordinating have participated might represent at least a perceived pressure for students to participate - because they might worry that it could impact on how the lecturer regards/grades them.

Another example: If the respondents are disclosing illegal behaviour in response to an apparently anonymous survey, the fact that the researchers (or perhaps an enterprising law enforcement agency) could glean the name of respondents, could represent serious risks to the participants.

There are measures to address these issues, such as: printing the attachments as soon as they are received and deleting the electronic copy; or there are methods (**see this article about removing the hidden personal information from MS Office files**) by which either the responding participant, or the receiving researcher, can strip the 'hidden' properties of some types of files.

When researchers will be receiving electronic files from participants, and the potential for the identification of individuals may be a concern, the researcher(s) must:

1. Consider this in the design of the research, and consider what (if any measures) can and should be undertaken to address this situation - so the reviewers are aware of both the existence of the issue and the plans of the researcher(s);

2. Identify, discuss and justify in the application for ethical clearance for the project the existence of the potential issues, the measures to address any risks or concerns, and the degree to which the remaining situation can be considered ethically justifiable; and

3. Explain the situation to potential participants and the researcher's approach to the situation - so the potential participant can make an informed decision and (in the case of more computer savvy potential participants) perhaps have more confidence in the researcher(s)

(completing and returning the survey) and indicate that by completing the task/participating the individual is indicating their consent.

4.5 Email and the distribution/return of surveys

A common use of email in research is to distribute surveys to participants (either at the same time as the recruitment and/or consent information, or after the participants have expressed their consent to participate).

In some cases, participants will be asked to complete the surveys and post them back, but in many cases, the participants will be asked to complete the survey electronically and email their completed survey back to the researcher(s).

Such mechanisms are appropriate, but if the survey is intended to be anonymous, it will be necessary to take some additional steps, such as:

- if the survey is an attachment (such as a word processor file), when the researchers receive the response, researchers should immediately separate the attachment from the email, so it is no longer possible to associate the response with an individual (see the Commentary 4 inset for a discussion about the need to also remove the imbedded identifying electronic information and its implications for very sensitive research); or
- if the survey responses are in the body of an email, then the email should be immediately printed, and the header and footer of each page of the printout (where the identifying information about individuals is likely to appear, e.g. their email address) deleted - thus rendering the response as de-identified.

Commentary Inset 5 – The implications of monitored email communications - Many people are aware that their email communications may be monitored - especially when it comes to email accounts provided by their employer. USA Today reported on a 2007 study where 55% of survey employers monitored the email of employees. See this article for an Australian employer perspective on such monitoring (as presented by the online Human Capital Management publication).

Such monitoring can include manual 'random' inspection of emails sent or received, as well as automated 'sniffers' that monitor all emails for certain key words, or emails sent to certain email addresses and then flag the email that meet those criteria for review (by an officer in the organisation's HR department).

The existence of such monitoring might introduce a range of significant risks if the researcher(s) will be corresponding with participants using email.

In practice, it might be considered that the risk of harm to participants is low, but depending upon the area being explored in the research, it is still a factor to consider (e.g. if employees will be commenting on their behaviour that might be contrary to the policies of their employer).

Furthermore, post 9/11, many countries afford their law enforcement agencies a range of powers in terms of the monitoring of emails handled by mail servers in their jurisdiction. There is also commentary that suggests that some countries routinely monitors email traffic for references that the ruling powers in that country believes to be subversive or otherwise undesirable.

Once again, in practice, given the topic of the research and where it is to be conducted, the chance that this will be an issue for most research projects may be very low. Nevertheless, it is still a factor that should be considered (e.g. for email-based research where the subject matter might be considered to be critical of an oppressive regime.

In situations where there is a chance that email monitoring may be a concern, the researcher(s) must:

1. Consider this in the design of the research, and consider what (if any measures) can and should be undertaken to address this situation.

2. In the application for ethical clearance for the project the existence of the potential issues must be identified and discussed, the measures to address any risks or concerns outlined, and the degree to which the remaining situation can be considered ethically justifiable. This is so the reviewers are not only aware the existence of the issue but also the plans of the researcher(s). Without such a discussion the reviewers might conclude that an applicant is unaware or indifferent to the issues.

Continued over leaf

The consent materials should explain the above mechanisms.

Experience suggests that the provision of such information can address the apprehensions of potential participants and is likely to increase the number of individuals who agree to participate in the research. Conversely, failure to both address these issues, and to explain this to potential participants, may not only reduce the number of individuals who agree to participate, but also introduce or compound risks to the participants (e.g. exposing them to legal risks).

Refer to Booklet 22 of this Manual for more about consent, and Booklet 23 of this Manual for more about privacy issues.

Commentary Inset 5 – (Continued from previous)

3. Explain the situation to potential participants and the researcher's approach to the situation. So the potential participant can make an informed decision about their participation and (especially in the case of more computer savvy potential participants) perhaps have more confidence in the researcher(s).

In practice, where monitoring is an issue, the only solution might be to change the method of communication between the researchers and the participants.

For example: The employees of an organisation might be asked to participate using a private/home email address, via a web site (rather email) or to send their data/response offline.

Of course, such precautions might have an impact on participation rates. In practice, there will need to be a reflection on the risks (e.g. in terms of chance of incidence and significance of harm) and for this to then be weighed against
any potential impact upon participation rates.

The discussion of these issues, and the reflections of the researcher(s) may be an important element of the application for ethical clearance for a project and possibly in the consent materials"

4.6 Email and the results of the research

Generally speaking, participants should be offered access to an appropriate summary of the results of the research (as a component of a researcher project's adherence to the ethical principles of 'respect for persons' and 'beneficence'). This summary should be available in a timely manner and the language/complexity of the summary should be appropriate for the participant pool (e.g. it is generally neither timely nor appropriate to provide participants with copies of a publication arising from a research project).

Where the researcher knows who participated, and has individual email addresses for those participants, it may be appropriate to email an appropriate summary of the overall results of the research to participants (or to those participants who have requested the summary). When the research involves highly sensitive matters or may otherwise be embarrassing to participants it may not be appropriate to email participants the results of the research.

Where the researcher does not know who participated, but has authorised access to a group email address (whether directly, or by asking an authorised person to conduct the broadcast), it might be appropriate to distribute the summary of the overall results of the research to all of the potential participants, irrespective of whether they actually took part in the research.

In some cases, the consent materials will indicate that individuals let the researchers know if they would like to be added to a list of people who will be sent the summary of results.

4.7 Email and debriefing

In addition to offering participants with an appropriate summary of the overall results of the research (see 4.6), there can be circumstances where the researcher can communicate individual results/findings to individual participants, and where it is reasonable to assume that the participants might be interested in learning their own results (e.g. learning that they have a specific genetic marker that the research indicates could be a predictor of a risk of later developing a disease or illness; or that the literacy of their daughter or son is below average; or that the individual's business is not complying with a regulatory requirement).

In some cases the provision of such feedback/debriefing may be the only tangible benefits for participants. There can also be situations where results should, or even must, be communicated.

As discussed in Booklet 22 of this Manual, the researcher will need to consider whether there should be a mechanism where participants indicate if they want to be told about their individual results.

There should then be consideration of who should provide this de-briefing to those participants. In many cases, the amount of information required, and the need to provide further clarification and support to participants, means that it might not be appropriate to provide this de-briefing via email. Furthermore, there might be privacy and other concerns associated with delivering a de-briefing via email (see 4.10). Nevertheless, there will be situations (especially where the likely impact of the results for participants is considered to be relatively minor) where it is appropriate to provide a de-briefing to participants via email.

Commentary Inset 6 – Email, the identification of individual participants and risk - The implications of the researcher(s) being able to associate a response/data with an individual participant, or the chance that a third party could theoretically do so, should be considered in terms of whether this creates a degree of risk. Sometimes the mere fact that the researcher(s), or a third party, will know who participated could constitute a risk.

Example: A research team has been commissioned by Queensland Police to collect data about violence against officers during arrests. An element of the survey that will be sent by email to current officers is the degree to which they themselves have used excessive force. The responses will be returned to the researchers via email but does not seek any identifying information from respondents.

Issues to consider during the design of the research, when preparing the application for ethical review, and seeking consent from potential participants include:

1. The data is quite sensitive in that it involves possible illegal behaviour, where if an individual was associated with a response that disclosed legally questionable behaviour, the individual could face legal, professional, social and other risks.
2. If the survey responses are to be returned via email this means that, at least for some time, the researchers could correspond responses to individuals.
3. If the completed surveys will be returned as electronic attachments, potentially identifying may be embedded as 'hidden' data in the file.
4. If QPS is given a report that indicates that some excessive force is being used, they may feel it important to try to work out who participated and how they were acting inappropriately.
5. The legal representative of an individual arrested during the conduct of the research might seek access to the information above to see whether the arresting officer is someone who indicated they had used excessive force.

Consequently, the research team needs to carefully consider how to ensure that the surveys are genuinely anonymous.

4.8 Email and maintaining contact with participants

In addition to offering participants with an appropriate summary of the overall results of the research (see 4.6) and/or potentially debriefing on their individual results (see 4.7), some research projects will use ongoing email communication to maintain contact with participants.

The use of research updates, newsletters or other communications can be a positive way to maintain contact for projects where participation is extended over a long period of time and/or where the researcher(s) hopes to ask the individuals to participate in subsequent work (whether in a phase of the project or other future projects).

In most cases, the ethics reviewers will not ask to receive, with a view to reviewing and approving, these ongoing communications (though in the case of highly sensitive research topics they may decide this is necessary). However, it is prudent that copies of these materials are sent to the Office for Research (see contacts) so they can be placed on the research ethics file for the project.

4.9 Email and exclusion of some participants

Even though the number of Australians with access to at least one email address appears to be quite high, the demographic information reported by bodies such as the Australian Communications and Media Authority (ACMA) suggests that access to the relevant technologies is lower amongst certain age groups (e.g. persons aged over 65), people living in very remote locations, and persons living in lower socio-economic circumstances.

Furthermore, even for those people who have access to an email address, there can be privacy issues (see 4.10) or other reasons (see Commentary 5 and Commentary 6 insets), which mean that they are unwilling or unable to use that email address to participate in research.

The above issues can be even more significant in developing countries or in situations where statutory/regulatory body monitor email and Internet activity by citizens.

As a consequence, the exclusive use of email for a research project, might serve to exclude some people from the participant pool. Such exclusion might impact upon the validity of the data collected and the findings of the research (because the data collected excludes sections of the potential participant pool). This can raise research ethics and research integrity issues if the research is claiming results that are relevant to the entire potential participant pool. Furthermore, the practical exclusion of some participants (because they do not have access to the necessary technology/services) could raise distributive justice issues (e.g. if the exclusion of some potential participants from the research denies them access to a benefit that they might view as desirable).

When planning a research project that will involve email, researchers should carefully consider these matters and ensure that their reflections are made clear in the application for research ethics review for the project.

4.10 Email and privacy

Email is not a secure method of communication because messages are not normally encrypted, and so at least theoretically, can be 'sniffed'. In an earlier edition of this booklet it was observed that, in practice, such interception was unlikely for mail sent via private email addresses. Recent revelations about the activities of some intelligence agencies and global media corporations have suggested that this may no longer be the case – especially for research in some fields (e.g. religious fundamentalism) and/or with some participants (e.g. political figures).

In the case of emails that are sent via an organisational server (such as the mail server of the employer of a potential participant) these could be intercepted and read by that organisation (and some employers can even set for email traffic through their server to be searched for keywords and then sent for review by an

organisational officer). The security of email can also be compromised because many computer users are not careful to 'lock' their machine/log out of their email account when they leave their machine unattended, consequently their emails could be read by third parties.

Despite the above, the sheer volume of email traffic in Australia still makes it unlikely that private email will be intercepted. However, email that is sent to work addresses, and other organisational addresses, might be intercepted.

Researchers should also carefully consider the risks associated with having participants send data (e.g. questionnaire responses) back via email. See Commentary 6 inset for an example and further discussion on this issue. Furthermore, researchers should reflect on whether there is a need for steps to protect the privacy of participants if the researcher's receipt of data via email (e.g. arrangements to ensure that the email account can only be accessed by authorised persons, and checking what copies of emails are kept by their mail server).

The chance that harm might occur, and the implications of that risk, might be considered to be higher where the nature of the research means that there might be discussion about illegal behaviour or the research is critical of the organisation whose mail server is to be used for the email communication between participant and the researchers.

It can often be important to include a discussion on these issues in the consent materials - if only to give potential participants greater confidence in the steps that will be taken to protect their privacy if they elect to participate.

Of course, it should be noted that the contemporary concern about online security and identity theft not withstanding, the issues discussed above are probably no more acute for email communications than they are for hard copy communications (e.g. the same careful consideration, precautions and discussion in consent materials, might be required if data critical of an employer will be sent through the postal office of that employer).

Back to contents

5.0 The World Wide Web

The World Wide Web based research is still relatively new (Battles 2010) but is already a very useful tool for some researchers in that it offers:

- practical advantages (e.g. it often being quicker, cheaper and easier to reach a larger group of people over a wider geographical area, compared to other approaches),
- methodological advantages (e.g. it being easier to embed into the data collection screening criteria, validation, etc.); and
- ethical advantages (e.g. being able to make participation truly anonymous and to potentially even conceal the participatory status of individual from the researchers).

Online research however can still raise significant ethical considerations. In this section some of the more typical uses of, and challenges arising from, the Internet in human research are discussed.

In 5.0 you will find:

Commentary Inset 7 – Assessing the ethical use of information published on the Internet - One of the considerations when deciding whether it is ethical to use information that has been published online, and whether to consider this to be human research that requires ethical clearance, is the degree to which the author and/or subject of the publication has themselves posted the information (e.g. on their own web site or they themselves submitted it to an online publication.

In such cases, if the data / document is on a public web site, it may be appropriate to consider the document / data as being appropriately on the public record and so it's use may not need consent.

The next consideration is the degree to which the subject matter is contentious and/or the individuals named / discussed in the online material are likely to be concerned by the research use of the material.

For example: An online article about the record of a how a politician has voted in parliament on an issue might not have been written by the politician themselves, but he / she is unlikely to be concerned by the research use of this information.

Whilst the research analysis of information like a politician's voting record is arguably human research, it is not an activity which requires ethical review.

Alternatively an online and unauthorised biographical piece about the troubled youth of a politician might require ethical clearance, even if the piece is on a public web site (especially if there might be ethical concerns about the manner in which the information was collected).

5.1 Is online content analysis human research?

Some research will involve access to and then analysis of, or other research uses of, web pages and other online content. The question of whether research, that only involves the research use of web content, should be considered human research that requires research ethics review will depend upon:

i) the degree to which the material should be regarded as being 'on the public record' (e.g. that it is in a location which can be accessed by general Internet users - rather than requiring some sort of password/access credentials); and

ii) whether the 'subjects' of the content are the persons who placed the material online/operate the web site, or the degree to which the subject matter should be considered to be contentious/of concern to the 'subjects' (see Commentary 7 inset).

When the web content is publicly available and the content was either made available by the 'subject' or it involves negligible risk and the research use of the content is not likely to be of concern to the 'subject' then this work need not be considered to be human research that requires research ethics review. In practice researchers may need to confer with a Research Ethics Adviser or the Office for Research (see Contacts) when making this assessment. Further guidance with regard to social media can be found at 5.13.

5.2 Web surveys

Web surveys are an increasingly popular tool for human research. Buchanan EA (2009) conducted a survey of 750 Institute Review Boards (IRB) and 94% of which reported "growing prevalence of this methodology for academic research".

Surveys that are placed online have many advantages, these include:

- being a cheaper way of delivering surveys to a large number of people;
- making it quicker and easier for participants to access, complete and submit the survey;
- being able to add validation to the survey (e.g. checking that certain questions have been answered, and checking that if a question is supposed to be answered with a number, that the respondent has in fact provided a number;
- being able to make some elements of the survey dynamic (e.g. setting so a group of questions from the survey only appear if an earlier 'trigger' question is answered in a particular way (see Commentary 8 inset for an example); and
- making possible to make the survey even more anonymous.

Commentary Inset 8 – Dynamic survey design - In a regular survey, each question from the survey appears on a web page. The participants move through the various questions in a very similar way they would a paper and pen survey.

In a dynamic survey, all of the questions do not appear, but instead what appears depends upon the participant's earlier answers.

For example: A survey might include the question - "Are you employed (Yes/No)?" In a dynamic survey, if they answered that question Yes, they might then be asked "What are your working arrangements (Fulltime/Part Time / Other)? If they answer Other they might be presented with "Please describe".

Whilst setting up a dynamic survey is undeniably more work, they have the advantage of appearing shorter and avoid the participants having to wade through probing questions that are not relevant to them.

However, in addition to the issues discussed at 5.11 and 5.12 it is important to remain mindful that the use of online surveys can raise ethical and methodological challenges, such as:

i) ensuring that an individual only completes a survey once[1];

ii) applying the intended screening criteria (e.g. the exclusion of persons under a certain age, because the subject matter is not considered to be appropriate or their experience is unlikely to be relevant); and

iii) the researchers not being able to refer a participant to a support service if they become distressed or if the nature of their responses warrants some kind of intervention.

[1] A common solution to this challenge is through the use of cookies. Where they are utilised the consent material should discuss that cookies are being utilised, the reasons why, and whether they enable the researchers to identify respondents. Applicants for ethical clearance must disclose to review bodies if cookies are to be used to collect data (such as other websites the participant has viewed). See Booklet 22 of this manual for more about consent and Booklet 23 for more about privacy.

The IRB respondents to the survey by Buchanan EA (2009) noted these and other ethical considerations (e.g. consent and secure data storage) can often not be adequately addressed by the design of human research projects that include web surveys. The advice provided in 5.0 are intended to assist Griffith University

researchers avoid some of the more common difficulties (in the design, research ethics review, conduct and reporting the results of such research).

The matters discussed above might also apply to surveys administered in other ways (e.g. over the phone, via email, or via the post), but these matters may be especially acute for online surveys.

5.3 Web tests

Rather than an online survey (see 5.2), some Internet-based research can involve the administration of tests for participants. The exact nature, administration and participant-experience in these tests can be quite diverse. The strengths and challenges for such research are often similar to those discussed above for online surveys (see 5.2).

An important technical, and participation, consideration can be the degree to which the testing back-end requires the potential participant to be using particular Internet browsers (or generation of browser), for them to have particular plug-ins installed (e.g. a Flash player) or certain Internet security settings in place (e.g. java enabled and cookies allowed). If the above technical requirements are not considered then some potential participants may be unable to access the test, or they may receive a warning message that causes them concern.

Commentary Inset 9 – Ensuring individuals only participate once - In some cases it will be important for the validity of the results of the research to ensure that individuals only participate once, rather than perhaps distorting the results by participating multiple times.

The two most common ways to ensure individuals only participate once in a web-based research project are summarised below:

1. The researcher(s) give each individual participant a unique login credential. The survey back-end only allows an individual to complete the survey once.

2. When accessing the survey, the individual is asked to provide their full name and email, and this combination can only be used once.

With both approaches there would be the option to:

i) Store the login record separately from the data and this information never being made available to the researchers.

ii) As per i) except the researcher(s) are provided with the record of who participated, but this information does not correspond individual responses with individual logins (i.e. the participatory status of individuals is known to the researcher(s), but the survey is still anonymous).

iii) the login and response data are stored in the same table (i.e. the participatory status of individuals is known to the researcher(s) and the survey is not anonymous).

The approach and implications should be explained both in the application for ethical review for the research and in the consent materials.

Experience suggests that it is important for potential participants to have a clear understanding of the implications of the login requirement and the degree to which the researcher(s) can identify who has participated and whether they can correspond data with individuals.

5.4 Consent and the observation of online communities, bulletin boards, YouTube channels, blogs and chat rooms

As was noted previously (see 1.0) the last twenty years has seen a massive increase in the number of Australians who spend significant amounts of time online. The number and duration of visits to online communities (including social media sites), YouTube channels and blogs have massively increase, while the usage of bulletin boards and chat rooms have been largely replaced by similar features on social media sites (Rovics 2014).

See Roberts (2015) for a discussion of the ethical conduct of research within online communities,

Because of the degree to which these online communities and communication applications can facilitate vibrant and unique dialogues, they can be potentially useful sources of data for researchers.

At 5.13 there is discussion about whether sourcing material from social media sites/communities should be considered human research – with the consequence of research ethics review being required.

As discussed at 4.4 consent is a key element of the core ethical principle of respect for persons. In all but very specific circumstances (see Booklet 33 of the GUREM) the design of online research should respect the right of individuals to choose for themselves whether to participate in a research project.

Potential ethical tensions are highlighted by cases such as the 'pro-ana[1]' web site that was actually being managed by a researcher using the web site to conduct undisclosed research (Botsky and Giles 2007).

Research conducted with online networks frequently face three challenges:

i) The fluid nature of participation (in terms of who is participating, and when they start and end participating) in these online network applications (such as chat rooms) can make it impractical to seek the prior consent of individuals.

ii) In many cases participants can be anonymous, being identified only by a screen name, and possibly without an email address or other contact method being available to the researcher(s).

iii) Depending upon the methodology of a project there can be quite a justifiable concern that any mechanism to seek prior consent before the activities could distort the degree to which the discussion can be considered to be natural.

Commentary Inset 10 – Online screening tools - Depending upon the nature of the screening criteria, it may be possible to conduct this screening online. However, when screening is conducted online, some issues to consider are:

1. Are the purpose and implications of the screening test explained to potential participants?

2. Will the system record the answers to the screening test? Will this information be deleted if an individual does not participate? Who will have access to this information, and how will it be used? Is consent sought for this use?

3. Will it be necessary to reconfirm the screening data through offline mechanisms?

4. What will individuals be told if they are screened out of the participant pool? Is there a need for debriefing or a referral to a support service?

5. What will be done if there are more eligible

potential participants than are needed?

[1] A community of mutual support for people living with the anorexia eating disorder.

The University has a mechanism where researchers can seek waiver of the consent requirement for individual research projects (see 7.0 of Booklet 33 of this Manual). It may well be justifiable not to seek consent in situations where the subject matter is not especially sensitive, where there is no risk of identification of participants (whether directly or indirectly) and/or identification of individual participants is unlikely to expose them to significant risks, and the participants are unlikely to be concerned by the research use of data from the community.

Commentary Inset 11 – Keeping a record of consent - It is accepted practice (at Griffith University and many other institutions) for survey-based research to:

1. Provide an information sheet to potential participants; and
2. Accept that if they return a completed questionnaire they have consented to participate.

However, there are circumstances where having a record of the express consent of individuals can be appropriate, desirable or important.

The options and issues associated with seeking an online expression of consent and then a record of that consent are very similar to those discussed at 4.5. The same sort of issues with regards to ethical review, risk and consent also apply.

In practice, the decision of whether to seek a record of expression of consent is likely to be a balance between risks to the participants (including how potential participants might perceive that risk and so perhaps elect not to participate) versus the needs for the researcher(s) to have a participant specific record of consent from individual participants.

But when a waiver of the consent requirement is not obtained, there must be a mechanism to seek consent from the community participants. Some strategies employed by researchers in the past have included:

i) The researcher and/or network moderator posting regular notices about the presence and objectives of the researcher(s), with a link to an information sheet about the project, so individuals can decide whether to post their comments and/or adjust what they say.

ii) After an individual has posted comments which the researcher(s) wishes to use, the researchers then seek the consent of the individual (e.g. via email - if this is possible) for the research use of the comments.

iii) Particularly where the subject matter is highly sensitive and/or seeking consent from individuals after they have posted a comment is not practicable, researchers have themselves set up a web community (e.g. an issue group within Facebook) where seeking consent will be an element of the process of an individual joining the group.

The above examples may not be appropriate, or even possible, for every project. Other strategies, which address the ethical principle of 'Respect for Persons' and adhere to University policy (see Booklet 22 of this Manual for more about consent) may be considered appropriate. Researchers should consult with the Office for Research (see Contacts) to discuss her/his intended strategy.

5.5 Recruitment

The Internet can be a very useful tool that can assist with the identification of, and contact with, potential participants.

Some examples of online recruitment strategies are listed below. It is not intended that this list be considered exhaustive or prescriptive.

i) Banner or other advertising on appropriate feeder web sites (e.g. a graphic link calling for volunteers might be posted on the web site of a community social club from which the researcher(s) are hoping to recruit members).

ii) A notice, article or news item on appropriate feeder web sites that describes the research and calls for volunteers.

iii) A post on an online network (e.g. a social media post) that describes the research and calls for volunteers.

You can find further information about recruitment in human research, and some of the associated ethical challenges in Booklet 21 of this Manual. As per 16.0 of Book 21, any materials or media that will be used for recruitment purposes must be approved

5.6 Screening

As was noted at 5.2, one of the difficulties with web-based data collection is the conduct of screening (e.g. excluding persons who are not members of a particular cultural group, or only including persons who fall within a certain age group).

In most cases, the only screening that can be employed is controlling who are given the URL of the web-test, assigning individual passwords to potential participants (see Commentary 9 inset for more on this method), or relying on potential participants to self-screen on the basis of information provided in the recruitment and/or consent materials.

In some cases where monies and expertise is available, it might be possible to incorporate a screening assessment tool into the web test (see Commentary 10 inset for an example). However, this will not always be helpful or even possible

5.7 Consent and the web*

- The following guidance material relates to web-based tests and surveys and does not relate to consent and the observation of social media, bulletin boards, chat rooms, YouTube Channels or blogs (see 5.4). It also does not allow the research use of content that has been published online (such as on a dedicated web page (which may be more a copyright/authorised use issue than a human research ethics matter – see 5.1).

As is the case with all human research, the normal expectation is that voluntary and consent must be obtained from all participants. However, as discussed at 5.4 there can be circumstances where not seeking consent can be justified and may be considered ethical.

Even when consent is required, the University's policies (see Booklet 22 of this Manual) allow for considerable flexibility in the formulation of a consent mechanism.

A range of valid consent mechanisms are possible options for online research. Some examples of consent mechanisms are listed below. It is not intended that this list be considered exhaustive or prescriptive.

i) Before potential participants access a web survey or test a 'splash page' displays before the survey/tests and describes the project, what participation involves, the rights of participants, and what will happen with their submitted responses/data. The potential participant is invited to print

the splash page for later reference, and they click to indicate that they have read the information and consent to participate. They then are directed onto the survey or test.

ii) A variation of the above is where the potential participants have unique credentials (e.g. a username and password), so the system can log that the individual has consented and date/time stamp this consent. See Commentary 9 inset for a discussion about the strengths and weaknesses of this approach.

iii) An email provides the link to the web survey or test includes (or has it attached) to a description of the project, what participation involves, the rights of participants, and what will happen with their data. The potential participant is invited to print the information page for later reference, and told if they follow the link to the survey or test, and then complete the survey or test, they will be deemed to have indicated that they have read the information and consent to participate.

iv) The consent mechanism could be conducted offline, so that participants are only given the URL of the survey or test once they have consented to participate.

Commentary Inset 12 – Web content and accessibility - A well-coded web site has text where the size of the text can be increased by visitors (e.g. to allow for visitors with some degree of visual impairment) and can be accessed and interpreted by a screen reader (technology used by some people with no visual acuity).

Furthermore, a well designed survey, web test or interface:

1. Will be coded so that it can be accessed and completed via only the keyboard (i.e. rather than requiring a visitor to use a keyboard and mouse.
2. Will use a colour palette that is as 'friendly' as possible for persons who have a colour vision deficiency.
3. Will be compatible with 'screen readers'

The implication of failing to adequately address such issues is to exclude some potential participants because they are physically unable to use the project's web materials.

This not only raises potentially serious issues (in terms of the ethical principles of justice and respect for persons), it could also impact upon the validity of the results of the research (by excluding a group of potentially key participants).

It should be noted that W3C valid design (click here for more) should not add very much time to the development of web materials.

It should be noted that, like other research methods such as paper and pen anonymous surveys, after an individual has participated, it might be impossible for them to later withdraw their consent and data (because the researcher(s) cannot correspond specific data with the person who has withdrawn their consent). If this is the case, it should be clearly explained in the consent materials.

Reflections about whether consent is required should be web site specific and may need to be revisited over time (see Whiteman 2012).

You can find further information about consent in human research, and some of the associated ethical challenges in Booklet 22 of this Manual

5.8 The Internet and research results

As was noted at 4.6, in most cases there must be a mechanism by which participants can access a timely and appropriate lay summary of the overall results of the research.

An advantage a web site has over email is that the summary of the overall results can be posted on a web page, enabling individuals to access and view the results without having to contact the researchers -

potentially preserving their anonymity and concealing the participatory status of individuals. In addition to providing another, and confidential way for participants to access results, such an approach may also facilitate building an ongoing link with participants that could be useful for the future (see 5.10).

5.9 The Internet and debriefing on individual results

Whilst the Internet could be used for the debriefing of participants, this would not completely replace the need for other debriefing mechanisms (see 5.11). Furthermore, if individual results are made available online the page/app will require access controls to ensure third parties cannot view the results of individual participants or indeed participants cannot view the results of other participants.

Such arrangements to protect the confidentiality of participants are not only a matter of respect for persons (see Booklet 26 of the GUREM) it may also be required by privacy regulations (see 5.12).

In most cases it would be inappropriate to communicate an individual's results online if those results could be distressing to some participants, require explanation, or require referral to some form of care/assistance/treatment/support.

Commentary Inset 13 – Intercepts of web-based communications - From the earliest days of the Internet it has been theoretically possible to intercept web-based communications (such as when a user completes and submits a web form such as a survey).

Security vulnerabilities include:

1. Situations where the server where the back-end of the survey is installed being infected with a virus, Trojan or other malicious code, which 'harvests' data and forwards it to an unauthorised third party.
2. As per 1, but it is the 'sending' participant's machine that is infected.
3. As per 1, but it is the 'receiving' researcher's computer that is infected.

The Internet itself is not especially secure and is at least theoretically vulnerable to attack. The HTTPS protocol (a commonly used security protocol) is more secure, but is not invulnerable to attack (evidenced by the recent successful attack on the Adobe client database).

Information communicated online, without such encryption may, in certain circumstances be especially vulnerable to interception (e.g. if staff of an organisation will be using their employer's web server to access a web-based survey or test).

In the recent past the sheer volume of Internet traffic has afforded some degree of protection (unless the communication was likely to be especially attractive / apparently valuable) but the rapid increases in the processing power of relatively inexpensive computers has diminished the protection 'afforded by the herd'.

Allegations of illegal intercepts by a major news corporation and leaks of intercepts by intelligence agencies have demonstrated that any electronic communication is vulnerable to intercept.

Consequently during the design of a project researchers should carefully consider the degree to which the topic, potential participant pool, the issues explored and context make the data attractive to would be hackers, the potential harms if the data is intercepted, and the relative vulnerability of the participants.

In light of the above matters, and the risks are considered of sufficient concern, it might be necessary to collect the data in a de-identified form, not to

communicate the data / materials to others in an identified form, and/or to consider the degree to which Big Data (see 7.0) could be used to identify individuals.

Consequently, the use of a web-based debriefing mechanism is rare - though not impossible, if the matters discussed above are satisfactorily addressed.

5.10 The Internet and maintaining contact with participants

A potentially extremely useful, but often neglected, way for researchers to utilise the web is as a mechanism to remain engaged with participants (e.g. with a newsletter about progress with the research and activities once the data has been collected).

A common criticism from 'highly researched' populations (e.g. people who live with chronic medical conditions) and people whose historic experience of research has not been positive (e.g. Aboriginal and Torres Strait Islander people) is that they have frequently been the 'subject' of research, but rarely learned much of the outcome, felt connected to how their participation made a contribution to knowledge or practice, and very rarely felt they have any role in the next stages. Having established some degree of Internet presence, whether initially only to recruit and/or collect data, researchers might usefully decide to use the web site to provide ongoing updates about the progress of the research, as well as deliver a summary of the results of the work (see 5.8).

Such an Internet presence could be used to acknowledge the contribution of participants, share information about action arising from the research, and discuss upcoming phases of the project or related research.

Another advantage of this kind of strategy is that it might not only foster an ongoing positive relationship with individual participants, groups, organisations and communities, it can also provide an ongoing pool of persons who are more likely to be enthusiastic participants in future related work.

Commentary Inset 14 – Physical security considerations - In addition to digital security matters discussed above there can also be more physical matters to consider.

Examples include:

1. If there are potential risks to individuals if they elect to participate in a project, could they be observed participating? Were this to be the case, potential participants might be usefully encouraged to take steps to conceal their participatory status. It may be necessary to modify the design of a project to better conceal the participatory status of individuals.

2. Similar considerations apply if there could be risks to individuals if they are observed to not participate in a project.

3. If there are risks (if only in terms of humiliation) associated with individuals undertaking some of the questions, tasks, etc. in a project (e.g. because of answers to some trigger questions it is considered that the individual warrants further enquiry that other participants did not) similar precautions to 1) may be required to ensure they are not observed (e.g. by other participants who may realise the significance of the extra tasks

4. If there are risks (e.g. social, economic or legal) associated with third parties knowing an individual's results (if the research design means that there are individual results and these will be communicated to the participants), similar precautions to 1 may be required.

In light of the above it might appear at first glances that the simplest approach would be to always conduct web-based (and email based or even computer based) research without collecting personally identified data, but it should be noted that:

1. This may not be possible, desirable or appropriate for some methodologies, issues or participant pools.

2. Issues 1 – 3 (above) may still apply even if no personally identified data is collection (Example: It may still be deleterious if a person is physically observed to be participating in a project – even if no personally identified data is collected).

3. Receiving personal feedback on their performance/results

may be an important benefit of the research.

Continued overleaf

5.11 The World Wide Web and the exclusion of some potential participants

Even though recent years has seen increasing general usage of the Internet across Australian all age groups, and despite some of the practical advantages of conducting research online, it is not always appropriate. In the case of some potential participant groups, the conduct of a research project online (or at least exclusively online, without offline alternatives) can:

- (depending upon whether the design of the web-based materials comply with the Web Content Accessibility Guidelines) exclude persons with a degree of vision impairment, in some cases auditory or speech impairment, or fine motor control impairment. See Commentary 12 inset for a further discussion on this issue.
- exclude, or at least be less accessible, to –
    - older Australians
    - persons living in lower socio-economic circumstances
    - persons living in especially remote locales;
- be inappropriate when conducting research involving some international jurisdictions (e.g. where an oppressive regime has made it unlawful for residents to access anything other than sanctioned content);
- raise additional privacy concerns when the potential participants will be utilising Internet services at their workplace (that might be monitored by their employer, but could be the only Internet access some individuals have), or using services that might monitored by third parties (e.g. law enforcement agencies) - see 5.12 for more about privacy considerations; and
- (depending upon whether the design of the web-based materials comply with the Web Content Accessibility Guidelines) exclude persons with a degree of vision impairment, in some cases auditory or speech impairment, or fine motor control impairment. See Commentary 12 inset for a further discussion on this issue.

Commentary Inset 14 - (Continued from previous)

4. As discussed earlier in Inset One an important limitation of collecting de-identified data is that it can prevent researchers from acting upon an individual's need for some form of intervention / support.

Instead researchers should consider what arrangements to manage the above are appropriate (e.g. keeping the various pages of the survey / test relatively low key so it is not obvious to an observer what they are doing) and whether it would be useful to give participants some guidance with regards to their own privacy (e.g. not using a desktop computer in a high traffic location).

The approach to these matters must be outlined in the application for ethical review – if only to indicate why it was considered unnecessary to take any precautions (because of the nature of the participant pool, the issues, or the location where data collection will occur).

It may also be useful for these matters to be discussed with potential participants (e.g. in the informed consent materials), if only to make it clear to potential participants that the researchers are aware of the issues and have considered what approach is best.

5.12 The World Wide Web and privacy

Similar privacy issues that were identified at 4.10 relating to email-based research also apply to web-based research. If the web survey or test is located in a secure host with a current security certificate it is less likely that a third party (even an employer whose Internet server and connection is used) could intercept and

access the participant's data. However, many Australian employers do monitor the web sites accessed by staff. In some international jurisdictions, some oppressive regimes do conduct similar monitoring.

Where the collected data is located online, the researchers must consider the security of this storage and how authorised access to the data is controlled (8.0 for more on data security).

Researchers have important ethical and regulatory privacy obligations to participants.

Consequently, researchers should carefully reflect upon the risk that the data submitted by individual participants could be intercepted or otherwise accessed by parties other than the researchers and/or the risk that third parties are in a position to identify the participatory status of individuals, where there are risks associated with that knowledge (see Commentary 13 inset for more and Commentary 14 inset for more about physical security threats to the privacy of data).

This may require additional precautions or a change to the way in which the online components of the research will be conducted. There should also be reflection upon how these matters are to be explained to participants, if only to allay any apprehensions.

See Battles, HT (2010) for an example of a web-based qualitative research project involving highly sensitive information and the approach taken to data collection, analyses and reporting of research outcomes.

At 3.0 of this booklet there is discussion about matters such as privacy and the administration of incentives and the capacity of the researchers to assist a participant who is deemed to be 'at risk'. Those matters should be: considered during the design of an online project; discussed in the application for research ethics review; and possibly explained in the consent materials for the project.

In circumstances where content, comments or personally identified data is sensitive or there are risks (e.g. social professional or legal) researchers might consider strategies to conceal the identities of individuals. However in the case of some web-based content (e.g. blogs) there may be authorship and attribution considerations that make removing the identity problematic (Buchanan 2011 pp102-103). The rules of some social media platforms might preclude researchers editing comments/posts (see 5.13.6.2).

Henderson et al (2013 pp552-554) discuss 'traceability' – the degree to which separate posts, comments, usernames and other data can be used to identify individuals and private information. As the functionality of social media platforms and search engines progress, and the sheer volume of online data about individuals increase, it is likely that identification of individuals (and potential exposure to risk) will become more likely.

See Booklet 9 of this Manual for more about risks in human research, Booklet 23 for more about privacy issues, and Booklet 22 for more about consent.

5.13 Social media and human research

Social media has become a widely used, and perhaps arguably only partially understood term (see 5.13.3). Very little has been written about the complex ethical challenges confronting researchers who intend to use social media – such as for recruitment or data collection purposes (Henderson et al 2013).

As of October 2015 Facebook had around 14 million Australian subscribers and Twitter around 2.8 million Australian subscribers (Cowling 2015). In August 2014 the world wide base of social media users exceeded two billion. A significant component of this growth can be attributed to mobile devices utilised in developing countries (Kemp 2015).

Although it may be a surprise to current users, the first social media web site Six Degrees was launched in 1997, but social media grew in its user base and influence in 2003 with the introduction of MySpace and then in 2005 and 2006 with the establishment of Facebook and then Twitter as publicly accessible platforms ("The History of Social Media").

5.13.1 IS IT HUMAN RESEARCH?

Initially this might appear to be a straightforward question and a subset of the question about published web contact discussed at 5.1. As such it might purely be considered in terms of whether posts/comments on a social media platform should be considered as being already published and publically available. If the answers to those questions are yes, it might seem to be the case that even if it is human research it will probably be exempt from research ethics review as per provision 5.1.18 and 5.1.23 of the *National Statement*.

While technically (dependent upon the privacy settings of a person's account) a posting to social media site might be published and on the public record, a not unreasonable probing question might be: did the author of the post appreciate that their information might be analysed or otherwise used for research purposes? Recent research published in the UK (Evans H, et al 2015) suggests that in many cases the answer is likely to be: probably not. Similarly, Boyd and Crawford (2011) question whether social media users are really cognizant of the potential research use of the information the information they post online. Consequently, Griffith University requires most research involving the analysis of social media comments to be submitted for research ethics review.

This section suggests some practical considerations for the ethical design and conduct of social media research.

5.13.2 IDENTIFIED PERSONAL INFORMATION/SENSITIVE PERSONAL INFORMATION

Identified personal information refers to information of a personal nature that can be linked to an individual (whether a participant or a third party). The information may be relatively innocuous or can involve more serious matters that might represent a risk to the identifiable person (e.g. exposure to a social, professional or legal harm). An opinion expressed by an individual is personal information.

The term sensitive personal information has a legal definition which includes: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices; criminal record; health information about an individual; genetic information about an individual that is not otherwise health information; biometric information that is to be used for the purpose of automated biometric verification or biometric identification; biometric templates. When identified personal information is sensitive additional legal requirements apply with regards to consent, use, its secure storage, and disclosure/sharing with others.

An ethical challenge for social media research, especially when it will involve access to comments/posts is that it can be impossible to know in advance whether the comment will include personal information (or indeed sensitive personal information).

Consequently the design of a project involving access (see 5.13.3) to social media posts/comments should ordinarily presume at the very least that personal information could be involved. It may be prudent to also approach the design from a 'just in case' perspective: because the information included in the

posts/comments might include sensitive personal information the design should treat all of the information as sensitive until it has been assessed to determine if it is sensitive.

In light of the matters discussed at 5.13.1 and 5.13.3 Griffith University researchers must obtain prior consent (see 5.13.4) for the research use of social media comments/posts even if it is believed that the information is already on the public record. Alternatively the researchers will need to seek a waiver of the consent requirement (see 7.0 of Booklet 33). Different arrangements might apply to 'brands' e.g. celebrities, politicians and CEOs (see 5.13.4.1)

See Booklet 22 of the GUREM for more about consent and Booklet 23 for more about privacy in human research.

5.13.3 USER AND COMMUNITY ATTITUDES

Research ethics can often involve speculating on the expectations, needs and aspirations of the potential participants and/or the wider community. While the work was conducted in the UK the Evans H, et al (2015) report on research ethics in social media research provides an interesting insight to perspectives of both social media users and non-users.

In summary the report recommends that:

i) researchers must obtain consent for **access** to and use of social media posts/comments even if the material will be analysed in an aggregate or in an otherwise de-identified form;

ii) it is not sufficient to rely on the platform's terms and conditions as being an expression of consent for research, even if the terms and conditions specifically discuss research – see 5.13.5.5 for a case discussion of a project that did rely solely on Facebook's terms and conditions;

iii) the use of the opt-out approach is sufficient but express consent is considered preferable (see 5.13,4) for more about approaches to consent for social media research;

iv) specific express consent (see Booklet 22 of this Manual) must be obtained for verbatim quotation from a post/comment on a social media web site;

v) some people may wish to be identifiable, or perhaps insist upon it, and their decision should be respected; and

vi) researchers should make information available online about their ongoing social media research.

The report noted social media users had a degree of distrust about social media research and researchers with (perhaps counter-intuitively) that distrust being more significant among regular social media users.

5.13.4 Approaches to consent

Based upon experience and feedback from participants/researchers, and in light of the Evans H, et al (2015) report, Griffith University has adopted the following for social media research.

i) Ordinarily express consent should be sought for research access to and analysis/use of social media posts/comments, alternatively a waiver of the consent requirement should be obtained (see 7.0 of Booklet 33) or unless the 'brands exception' (see 5.13.4.1) applies.

ii) In some cases (e.g. subject to the qualifying criteria discussed at 18.0 of Booklet 21) the opt-out approach can be used in lieu of express consent.

iii) Express consent must be obtained for verbatim publication/reporting of a social media post/comment.

iv) **Griffith University researchers should never rely purely upon a platform's terms and conditions as consent for a human research project.**

v) Griffith University researchers are encouraged to make available online information about their ongoing social media research.

5.13.4.1 'BRANDS'

Some social media user accounts/pages/activities relate to what might usefully described as 'brands'. Typically a 'brand' will have thousands of followers, will be confident social media communicators and be well accustomed/able to look after their own interests online.

Examples of 'brands' are:

- established commercial products/services;
- the CEO/spokesperson for a large company;
- celebrities/entertainers; and
- political representatives/activists.

Such people/bodies will probably be unconcerned by the research use/verbatim reporting of their comments, indeed it might be welcomed. Their status as a brand might make an opt-out approach to consent the most appropriate strategy. Researchers who are unsure whether an individual/body is a 'brand' are encouraged to consult with the Office for Research (see contacts). Despite the fact that a potential participant is a 'brand' the work may still require consent (see Booklet 17 of the GUREM for more about the scope of the University's research ethics review arrangements). All participants in Griffith University human research should be treated with respect (see Booklet 26 of this Manual).

5.13.5 Facebook

Around 93% of Australian social media users have a Facebook account, on which they spend an average of eight and half hours per week (Sensis 2015, p3). Internationally the Facebook platform "dominates the social media landscape" with 1.133 billion users – 83% of whom access the platform through mobile devices (Kemp 2015).

5.13.5.1 PRIVACY SETTINGS

Facebook has changed its privacy policies on a number of occasions and the latest changes permit the social media platform to share the personal data of users with third parties (Munson 2015). So it is perhaps not surprising that Evans H, et al (2015) found that users are confused about the privacy settings of their social media account and are distrustful of their information of third parties accessing their personal information.

Currently by default the posts of many Facebook users will be visible to the entire Facebook community, and potentially beyond even that to other Internet users. Even if privacy is set so posts are only visible to friends it may be possible for those friends to inadvertently share that post with the world.

In light of this and given the reported comments of a group of social media users in the UK (see 5.13.3) Griffith has decided to treat social media research as human research requiring research ethics review and upon the consent policies described at 5.13.4.

The uncertainty about whether a Facebook will have understood the implications of their privacy settings is also why express consent must be obtained for any verbatim publication/reporting of a Facebook post/comment.

In light of this and given the reported comments of a group of social media users in the UK (see 5.13.3) Griffith has decided to treat social media research as human research requiring research ethics review and upon the consent policies described at 5.13.4.

The uncertainty about whether a Facebook will have understood the implications of their privacy settings is also why express consent must be obtained for any verbatim publication/reporting of a Facebook post/comment.

Where there are potential risks (such as social harms) associated with a comment/post Griffith University researchers should consider whether it is possibly to conceal the identity of the author or aggregate the views of several authors. The ethical principle of beneficence requires that any risks in human research be justified by the benefits. See Booklet 9 of the GUREM for more about risks and benefits in human research.

Commentary Inset 15 – The 'overheard in the coffee shop approach' - Imagine you were a researcher who was interested in how ordinary members of the public talk about climate change and other environmental matters. You are aware a group of people meet at a local coffee shop to discuss current events, government policies and news about such matters. You plan to sit in the coffee shop, listen to the comments, take notes and audio record exemplar comments. Later you intend to analyse your notes and recordings to identify themes and make observations about the way in which the topics were discussed. This might then be published as a paper reflecting on the degree to which community campaign messages have been adopted and resonate in the community.

Chances are you would correctly consider such an activity to be human research requiring research ethics review.

Similarly you would hopefully also think about what consent strategy is appropriate, possible and respectful, or whether to seek a waiver of the consent requirement needs to be sought.

Such an approach can be useful when thinking about a Facebook discussion between friends. To a certain extent it is immaterial whether the information is published/on the public record. Instead we should recognise that the individuals intended their comments only for their friends not for use in a research project As such, the use of their comments is human research and maters such as consent, privacy and beneficence should be considered.

5.13.5.2 POSTS WITHIN COMMUNITY OF 'FRIENDS'

As noted at 5.13.5.1 Facebook posts that are ostensibly shared only with friends/family can distribute through the networks of friends of those friends and onward. Furthermore, some Facebook users (see 5.13.3) may not appreciate the degree to which their comments/posts may be viewed by any Facebook user.

When a researcher wishes to analyse/use a comment/post of a person, they often know it is good practice and courteous to first seek the consent of that person. An opt-out consent mechanism may be a valid alternative to express consent.

In the case of a Facebook user who a researcher does not know, rather than approach the matter in terms of "has this information been published/is is publicly available?" the 'overheard in a coffee shop' approach (see Commentary 15 inset) should be used instead.

See 5.13.4 for more approaches to consent in social media research.

5.13.5.3 PRIVATE MESSAGES

Private messages within the Facebook platform should only be analysed/used with the consent of the author (and possibly the recipient). This is the case, even if a researcher is one of the parties to the conversation.

5.13.5.4 VERBATIM CONTENT

Verbatim content from Facebook comments, posts or private messages may serve as exemplars, illustrative references and powerful evidence of a claim in a research output. Nevertheless, there is good reason to believe that Facebook users only believe they should be used with the express consent of the author (Evans H, et al 2015). Researchers should carefully consider to which verbatim content might still be potentially identifiable if only be family, friends, colleagues and peers and even if information such as the name of the author has been removed. There may also be risk and privacy issues to consider – that might extend to identifiable third parties.

5.13.5.5 CASE: EMOTIONAL CONTAGION

Research conducted by Kramer, Guillory and Hancock (2014) has generated significant commentary in the press (e.g. Chambers 2014) about the inadequacy of relying on Facebook's terms and conditions as consent for research. It also serves as a practical example of community attitudes to the ethics of social media research. The comments in the media on this case are consistent with the work conducted by Evans H, et al (2015). As noted at 5.13.1 Griffith University research with Facebook comments/posts is considered human research and must be submitted for research ethics review. The terms and conditions of the Facebook platform would never be considered to be a satisfactory consent mechanism for Griffith social media research (see 5.13.4).

5.13.6 Twitter

Even though it has a much smaller user base than Facebook (see 5.13.5) the Twitter platform is used by 2.8 million Australians (Cowling 2015) and 284 million people globally (Kemp 2015). Recent reports suggest the number of Australian users of Twitter is dropping and more people are now using other platforms such as LinkedIn, Instagram and Google+ (Sensis 2015). Nevertheless, there are features of the Twitter platform that make it attractive to some groups of users or for some purposes (see Barthel et al 2015, Coyne 2013, Granahan 2013, Walton 2015).

5.13.6.1 PUBLICATION

In its report on research ethics and social media research Evans H, et al (2015) suggests that while users are likely to consider Twitter posts as having been published, courteous and responsible practice would be to seek consent (see 5.13.4) for their research use. This is particularly the case if the author is to be identifiable (see 5.13.6.2). The Griffith University policy on the research use of Twitter posts is to treat it as human research that will require review via one of the University's review pathways.

5.13.6.2 DE-IDENTIFICATION, PLATFORM RULES AND COPYRIGHT

Twitter's usage policies require that any publication of a tweet must list the username and the full text of the post. In addition to this being a usage policy matter this is also a potential copyright matter. The requirement to print in full and identify the author is not in line with the research ethics requirements (e.g. concealing the author's identity to manage risks and changing the text to reduce the possibility of identification by inference). This is another reason why Griffith University researchers must either seek consent for the publication/reporting of posts or request a waiver of the consent requirement (see 5.13.4).

5.13.6.3 RETWEETS

An often used element of the Twitter platform is users 'retweeting' the posts (tweets) of other users they are following or otherwise become aware of. As tweets trend (because of high numbers of retweets within a group, topic or geographic region) the Twitter platform can recommend them to other Twitter users. This can result in a post 'going viral' and very rapidly grow in the number of views/retweets. Further to 5.13.6.1, the analysis and/or reporting of retweets is human research. If the text of the original post is used (see 5.13.6.2) the consent of the original author should be sought (see 5.13.4). If any comments have been

appended to the original tweet and the researcher wishes to use those appended comments the consent of the appending author should be sought. If the providence of appending comment cannot be identified it may be necessary to seek a waiver of the consent requirement (see 7.0 of Booklet 33). An aggregate analysis of the retweeting of a post is likely to still be considered human research requiring research ethics review (especially if the original post is reported) but it may not be required (or realistic/possible) to see the consent of the retweeters.

5.13.6.4 DELETED TWEETS

Perhaps one or the more controversial of the recommendations of the report by Evans H, et al (2015, p58) is that if a tweet is deleted from the Twitter platform it should be treated as if the author has withdrawn consent for the research use of their comment. This can obviously create some practical publication difficulties for researchers. In the event a researcher becomes aware/is notified (perhaps by the author) that a tweet has been deleted he/she should contact the Office for Research (see contacts) to discuss the options and best approach.

5.13.6.5 CASE: SHAMING AND THE SOCIAL MOB

Even though the link to human research ethics is not obvious, Ronson (2015a) discusses a number of sobering examples of how one thoughtless tweet can rapidly snowball into very public shaming and serious life-long consequences. For this reason researchers should carefully consider the risks associated with Twitter research, especially when the the individual author of a comment will be identifiable. It is important to consider the degree to which the potential benefits of the research justify the risks. Also see Ted Ronson's (2015b) TED Talk on the same topic.

5.13.7 OTHER SOCIAL MEDIA

Since 2010 there has been a surge of other social media platforms. If you include subscriptions and comments on YouTube posted videos as social media then YouTube is in close second with 13.9 million Australian users in October 2015 (Cowling 2015). If you include WordPress pages, blog posts and comments on posts as social media then WordPress is third with 5.7 million users. Instagram, Tumblr and LinkedIn each had more Australian users in October 2015 than Twitter (Cowling 2015).

Internationally platforms such as Qzone (China) and VKontakte (Russia) dominated regional patterns of social media usage (Kemp 2015).

The matters discussed at 5.13.5 and 5.13.6 may be useful starting points for reflections about other platforms. Please contact the Office for Research (see contacts) to request the inclusion of advice regarding another platform here.

5.13.8 SOCIAL MEDIA RESEARCH AND THE UNINTENDED EXCLUSION OF POTENTIAL PARTICIPANTS

A review of the publicly available Australian usage patterns of social media (Sensis 2015) reveals that almost 50% of users access a social media platform at least on a daily basis (up from around 30% in 2011), just over 30% never use social media and that the rest access one of the platforms somewhere between 'most days' and less than weekly. This suggests that recruitment or data collection via social media will exclude almost one third of Australians with that impact being greater for some demographics (e.g. Australians who are aged over seventy). Even though this exclusion might not impact upon whether it is possible to recruit the desired number of participants or sufficient data, but it may distort the data or otherwise represent a limitation to the quality/impact of the outcome of the research.

5.13.9 SOCIAL AND OTHER RISKS

As noted at 5.13.6.5 comments and posts on social media can result in shaming, humiliation and other risks (such as impacts upon employment and professional reputation). The nature of comments and posts, especially when they are reported verbatim may be very hard, or even impossible, to genuinely de-identify. In many cases the removal of an individual's name or other obvious personal identifiers may be insufficient to prevent identification by inference by family, associates, colleagues or peers (sometimes termed 'internal identification' see Tolich, 2004). See two Zimmer papers listed in the 'Other recommended reading' section of this booklet for more about such identification and its consequences.

Any identification may also represent other risks such as legal or even physical (because of reprisals against an identifiable individual).

Social media might also include the risk of psychological harm (e.g. because of the extremely distressing nature of the subject matter).

Griffith University researchers must always take care to identify the risks in a human research project, design and conduct the work in a way that mitigates the risks, and carefully reflect upon the degree to which the potential benefits of the work justifies the risks. These matters will be considered during the research ethics review of the proposed project. Refer to Booklet 9 of the GUREM for more about the ethical principle of beneficence.

5.13.10 YOUNG PEOPLE

The rules of many social media platforms permit users aged under 16 years of age and for them to set up user accounts and comment/post. Furthermore, the information accessible to a researcher might not enable the reliable screening of young people on the basis of age (unless they themselves honestly self-identify their age and/or self-screen themselves for the potential participant pool). The current algorithms to extrapolate age are not always reliable or helpful (Evans H, et al 2015).

This may require Griffith University researchers and research ethics reviewers to reflect upon the possibility that the potential participant pool for a social media research project might include young people aged much younger than expected.

5.13.11 PUBLIC DISCLOSURE AND OTHER RECOMMENDED PRACTICES

As was noted at 5.13.4 Griffith University researchers are encouraged to maintain a web-based public disclosure of current and ongoing social media research, especially if the opt-out approach or a waiver of the consent requirement has been obtained.

If using a social media platform for recruitment and/or data collection individuals should be reminded about the privacy settings of the project's pages (e.g. perhaps reminding them not to disclose personally identifying information about themselves of others).

A social media page for the project can be a helpful way to keep participants informed about developments, distribute updates, provide a lay summary of the overall results of the work, and generally remain usefully engaged with the participants.

5.14 COMPUTER SCIENCE/COMPUTER SECURITY RESEARCH

Buchanan et al (2011) provides a useful discussion about the human research ethics considerations for computer science research. Computer science refers to work with electronic devices such as smart phones (see 6.0) but can also devices such as geostationary satellites, identification chips and associated "algorithmic processes".

Computer security research is a subset of computer science research "is defined less precisely than the larger realm of CS, and intersects a variety of disciplines, such as applied security, cryptography, number theory, psychology, and law" (Buchanan et al 2011, p73). An example of such work that might be considered human research requiring research ethics review might be testing, surveys and interviews relating to phishing.

Historically such research did not obviously include human research components and did not require research ethics review, but in recent years this has been changing with work such as transaction log analyses blurring the distinctions between computer science research and human research.

The international experience with the research ethics review of computer science research has been problematic (e.g. determining how to usefully apply expectations such as consent and privacy to Google Earth images is far from straightforward).

The Chapter by Buchanan et al (2011) discusses a number of considerations for the ethical design and conduct of such research as well as guidance for the appropriate/useful research ethics review of computer science research. Also watch Golbeck J (2013, October) for practical examples of the ethical challenges raised by computer science research.

Griffith University researchers planning to conduct computer science research that may have human research components are urged to consult a Research Ethics Adviser and the Office for Research (see Contacts).

5.15 INTERNATIONAL CONSIDERATIONS

The nature of online research, and the growing proliferation of internet access (see Kemp 2015), means that researchers should, to varying degrees, reflect upon international considerations when planning, design and conducting web-based research. Below is a discussion of some of the more common international considerations. These considerations may also be a factor the analysis of data, the production of research outputs and the storage of materials after the conclusion of the research.

See Booklet 39 of the GUREM for more about research that is conducted in other jurisdictions.

5.15.1 GEOGRAPHIC LOCATION OF POTENTIAL PARTICIPANTS

When planning online research, it is important to reflect upon whether it is intended that at least some of the potential participants will reside outside of Australia, whether it does not matter where the potential participants reside, or whether all participants need to reside in Australia. In practice this may require some form of screening mechanism and purposive recruitment strategies.

Griffith University researchers should carefully consider whether there could be risks and other ethical sensitivities (e.g. cultural, religious, legal) for participants who reside in other countries and whether special strategies are required to address the risks/ethical sensitivity (see 5.15.3 for more).

A common consideration for overseas research (see 12.0 of Booklet 39 of the GUREM) is whether (for access and language reasons) the consent mechanism should provide a local contact person for concerns and complaints about the ethical conduct of the project. However in the case of online research there may be a credible argument that providing the email address for the Griffith University standard contact person (the Manager Research Ethics and Integrity see 7.13 of Booklet 22 of the GUREM) is appropriate.

5.15.2 DATA SECURITY

The use of cloud-based storage platforms (such as Dropbox) might means that the data is being stored in an unknown country and subject to terms and conditions or security vulnerabilities outside the control of the researchers (Buchanan 2011). The specifics, such as the security of the stored of the stored data and third party/service provider access, might change over time.

In light of the above it may be unwise for researchers to use a commercial cloud-based service for the communication of data between collaborators/sites or for the storage of data – especially if the data is personally identified and is sensitive/there are associated risks (such as social or legal risks).

Griffith University has established a secure service for the storage of data during the conduct of a research project. Griffith University researchers (including HDR candidates and support staff) can use this service without any fee and external collaborators can be provided with access to the stored data. Details of the service (including a FAQ) can be found at https://research-storage.griffith.edu.au/. **All Griffith University researchers are urged to use this service, which is hosted by the University.**

Similar matters to those described above might apply to cloud-based applications.

See Booklet 23 of the GUREM for more about privacy in human research.

5.15.3 ADDRESSING RISKS

The ethical principle of beneficence (NHMRC 2007) requires human researchers to minimise risks and that, for project to be considered ethical:

i) any risks should be appropriately addressed;

ii) the risks must be justified by the benefits of the research; and

iii) the consent sought from participants must appropriately disclose the risks.

Griffith University researchers must always carefully consider these matters during the design and conduct of online research, and discuss these matters in the application for research ethics review. This includes reflecting upon the risks that might exist, or be more serious, overseas.

The ability to minimise, manage or otherwise mitigate the risks may be more difficult for some research designs (see 3.4 for an example).

See Booklet 9 of the GUREM for more about the ethical principle of beneficence.

Back to contents

6.0 Handheld/wearable devices

During the last decade the emergence of powerful smart phones and tablet computers have had a transformative effect on how many Australians access the web, undertake a wide variety of work and recreational tasks and run apps. The introduction in the last few years of smart watches, fitness tracking devices and computer-connected glasses have further transformed the way in which people interact with the Internet and apps.

The significance in Australia of genuinely mobile computing is evident in the available metrics and analysis (see Cowling 2015 and Sensis 2015). The Australian experience reflects the international trend towards mobile computing (Kemp 2015).

Such devices can play a valuable role in research, offering efficiencies, options and possibilities that were previously unavailable to researchers, but they do also raise ethical challenges.

The guidance provided previously in this booklet can usefully be applied to the research use of handheld devices:

i. for the administration of surveys, tests and other research activities and research apps loaded onto the device (see 3.0);

ii. for the sending and receipt of emails (see 4.0); and

iii. for the administration of web surveys, tests and other research activities and research apps which are accessible via the World Wide Web (see 5.0).

Commentary Inset 16 – Backing up data: what, where and how often? - As with any computing it may not be always obvious why regular backups are important – especially if it is viewed as a distraction from actually conducting the research.

Of course, when there is a major hardware or software failure, a good backup strategy can make the difference between such a failure being an inconvenience or it being disastrous.

With that in mind, researchers are urged to have a thorough backup strategy that might include:

1. Backups to a drive / device other than the device being used in the field. There are excellent software solutions (e.g. Time Machine for OSX) that allows for backups to be automated, for incremental backups (as individual files are updated) and for password protection. If backups are not incremental they should be at least daily.

2. Periodic backups to a secure online service (there are several reputable services available) that provide similar functionality as 1) but protects the data from misadventure at the physical location of the onsite back up e.g. because of fire).

Ideally backups would be made of primary data, notes and other material, informed consent and other research ethics documentation, as well as such other supporting documentation that a researcher feels important to the project.

The same security and privacy expectations apply to backups as does to the original data and materials (e.g. password protection and access control, especially for personally identified and sensitive data).

If the data is coded, the data and the code key should be stored separately and with different passwords.

Special care may be required if the backup is transported (e.g. on a storage media – such as a USB memory drive).

Once analysis, write up and reporting / publication / outcome phases of a project are complete Corporate Archives & Records Management Services (CARMS) has established a process to enable elements to transfer eligible data formats to a third party off-site storage provider - ensuring appropriate recording and tracking of the records. Further information on how to arrange for off-site storage of your research data is available from the CARMS website at https://intranet.secure.griffith.edu.au/records-management/team-resources/business-processes/businessprocesses/offsite-storage-of-research-data

In addition to the above, such devices can also be utilised by researchers to: communicate between members of a research team; track important dates, record contact details and handle other administrative matters; access data; the storage/transport/sharing of collected data; and many other tasks.

Below is some commentary on common ethical issues for handheld devices. The nature and pace of change of these devices, their capabilities and uses means that while this booklet may be periodically updated the below should not been considered inclusive or exclusive. While not strictly speaking a handheld device, this discussion could be applied to netbooks, notebooks, Macbooks and other mobile computing devices.

Researchers who plan to use a handheld device and are unsure on the ethical issues and appropriate strategies to meet those challenges should discuss this with either their local Research Ethics Advisor or the Office for Research (see Contacts).

6.1 Stolen, lost and broken devices

The portability of such devices means that they are more vulnerable to theft, being lost and accidental damage. A thief is likely more interested in the monetary value of the device rather than the data it contains (and so will probably quickly delete all data and settings). Nevertheless that doesn't make the realisation that the device has been stolen any less a potential ethical concern. This concern might be especially acute if the data is identified personal information and even more serious again if that identifiable data is sensitive. This may expose participants (or named third parties) to harms that might otherwise not been a factor.

The following is recommended as a way to mitigate the consequences of a theft of, loss of, or broken device:

1. Ensure the device has an access / lock screen password.
2. Make frequent back ups of data, notes and other information from the devices to a secure location (see Commentary 16 inset for guidance on how frequently this should be done).
3. Ensure that any databases, logs and other systems the device remotely accesses are secure and have separate passwords.
4. Depending upon the devices, ensure it has an appropriate security suite installed.
5. Take normal precautions in terms of the security and safety of the device, remembering that its value to you is much higher than 'merely' the replacement price.

See 8.0 for more about data security.

6.2 Unauthorised access

No less ethically troubling than the theft of a device is situations where unauthorised parties access the data on a handheld device. This may occur physically (e.g. when a device is left unattended) or remotely (e.g. using a Trojan or other malicious software to access information on the device). The precautions discussed at 6.1 are useful protections against unauthorised access. See 8.0 for more about data security.

6.3 Lending devices to participants

Though not common, some previous projects have involved lending smart phones to participants for the duration of a project to assess whether the device and/or installed special app has a positive effect for a trial group (compared to a control group who use standard printed materials).

Even though there are obvious logistical matters for researchers to consider (e.g. what happens if a participant loses, breaks or otherwise does not return the device?), the ethical considerations might include:

i. who has paid for the device and, especially if they have been paid for by a commercial sponsor, are there any perceived conflicts of interest to address;

ii. whether the process for selecting the members of the trial and control group are fair and transparent to participants;

iii. whether at the end of the trial, if the benefits of the device is established, will the control group be able to follow the same protocol as the trial group; and

iv. whether at the end of the trial, if the benefits of the device is established, can participants purchase the device?

If the project is a clinical research refer to Booklet 12 of the GUREM for further guidance.

6.4 Devices as incentives

In some cases, researchers may intend to offer devices (whether directly for each participant or as a prize draw), including situations such as 6.3 iv above. Ethical guidance on such incentives can be found in Booklet 21 of the GUREM at 11.0.

6.5 Geotracking

An emergent opportunity made possible (or at least cheaper and more practical) in the last few years is geotracking where there is some form of research analysis of the tracked movements of participants. The most significant changes have been in terms of size / unobtrusiveness, cost and ease of use.

The tracking data may have been collected for other purposes (e.g. a residential care facility monitoring the location of residents who take short walks out from the facility) or specifically for a research project (e.g. tracking the movements of visitors to a national park to compare the areas they later recall visiting as opposed to where they actually visited).

Additional ethical considerations for such data collection include:

i. have the participants consented either for the tracking itself or the research use of tracking data (otherwise either a waiver of the consent requirement must be sought or opt-out consent must be sought – see Booklet 33 of this Manual);

ii. who will have access to the tracking information;

iii. what security arrangements exist to prevent unauthorised access to the tracking information;

iv. could participants be engaged in unsafe, embarrassing or illegal behaviour – if so what will occur if they do;

v. has the device been appropriately assessed and certified in terms of electrical and other safety;

vi. if the device is directly applied to the skin has it been cleaned or free disposal pads used;

vii. how will the tracking information be analysed / reported, and the degree to which individuals will be identifiable if only by inference; and

viii. what information about the device and the above will be provided to potential participants?

See 8.0 for more about data security. Refer to Booklet 9 of this Manual for more about risks in research, Booklet 22 about informed consent, Booklet 24 for more about privacy and Booklet 40 for more about the exposure of illegal behaviour.

6.6 Remote physiological monitoring

Another emergent area for research is the utilisation of data from remote physiological monitoring or biotelemetry devices collecting real time information such as heart rate, oxygen saturation, breathing rate and activity monitoring, with potentially being communicated to a central monitor.

Data of this kind has vast potential applications across many health research methodologies. The same additional ethical considerations discussed above (e.g. at 6.5) are relevant to research with such devices.

Back to contents

7.0 Big Data

The term Big Data is misleading in that, whilst it once referred to data sets so large they required a super computer to process, now even reasonably modest contemporary desktop computers can successfully handle massive data sets. Rather than a connotation of its size, Big Data actually refers to data with high relationality to other data that can be networked to explore connections about individuals, groups, relative comparisons and even the structure of the information being analysed.

Big Data is increasingly being used across many private and public sectors to describe and evaluate social and economic behaviour, as well as the basis for the design and implementation of programs. Researchers across many disciplines have embraced the use of Big Data because of the deceptively compelling nature of massive quantities of data.

There are however significant ethical challenges for the research use of Big Data. Boyd and Crawford (2011) proposes six provocations to critically reflect on the assumptions and biases that should be considered when working with Big Data – including challenging the assumption that the sheer volume of the data makes it more compelling than data from other sources. As was discussed at 5.13.3 it can be quite convincingly argued that individuals having posted information in the apparently public space of social media should not be deemed to have consented to its research use. The article also discusses issues such as the possibility of re-identifying data that apparently has had the personal identifiers removed and the potential unforeseen consequences of drawing conclusions from Big Data. The fact these issues exist does not mean that it is unethical to use Big Data in research, nor does it mean researchers must obtain consent from everyone who retweets a comment. It does mean that researchers must reflect upon the issues and highlight hem when seeking ethical clearance for such a project.

Back to contents

8.0 Data security

When a project involves the collection of personally identified data researchers have important ethical, and sometimes regulatory, privacy obligations (especially if the data is sensitive and / or if participants have been given an assurance their confidentiality will be protected). Related to the issues discussed in 4.10 and 5.12 researchers must consider the manner in which access to electronic data will be controlled and how assurance to participants about their privacy will be safeguarded.

These privacy responsibilities should be considered and addressed for the following components of a project:

i. Whether the data will remain in a personally identified, coded or de-identified;

ii. If the data is coded, will the code key be stored separately from the coded data;

iii. How the collected data will be stored during the conduct of a project – the security arrangements and how access will be controlled (and potentially logged);

iv. How data will be communicated between collaborating researchers / support persons / advisors;

v. How the data will be stored after the completion of the project;

vi. Whether the storage arrangements discussed above are in a shared space (e.g. a multi-occupant office) and / or on a machine that is connected to the Internet. If so, what are the arrangements to protect the security of the data?

The above matters may still need to be considered even if participants have consented to be identified. There can also by physical security matters that warrant consideration (see Commentary 14 inset).

These privacy considerations apply even if a researcher has authorised access to the information/data for non-research purposes (such as a Griffith University Academic staff member having authorised access to the University's learning management system).

See Booklet 23 of this Manual for more about privacy issues and the responsibilities of researchers.

Back to contents

9.0 Contacts

There are a number of resources available to assist researchers formulate an appropriate response to a question or challenge about the design and/or conduct of a project. This includes the Griffith University Research Ethics Manual and the Human Research Ethics Information Sheet Series. These documents are available from the URL below.

Research students – The first point of contact for research students for advice on any research ethics matter is always your supervisors.

REAs – All academic elements of the University have been asked to appoint at least one member of academic staff as a Research Ethics Advisor. REAs are a local contact for advice, information and suggestions. The contact details of all the current REAs can be found on the URL below.

Office for Research – Staff in the Office for Research (see below) are available to advise with the process of lodging an application or other administrative matters, procedural or policy questions. However, you will be asked what advice you have sought or received already (e.g. consultation with the REA for your area).

Manager, Research Ethics and Integrity

Tel: (07) 373 54375
research-ethics@griffith.edu.au

Policy Officer, Research Ethics and Integrity

Tel: (07) 373 58043
research-ethics@griffith.edu.au

Research Ethics Systems and Support Officer

Tel: (07) 373 5 2069
research-ethics@griffith.edu.au

On the ethics web site you will find:
https://www.griffith.edu.au/research/research-services/research-ethics-integrity/human

(In the intranet section)

- The other booklets of the *Griffith University Research Ethics Manual*
- The *Griffith University Human Research Ethics Information Sheet Series*
- Either downloadable copies of, or links to, the various application forms
- Contact information for the Research Ethics Advisers (REA) and other contacts
- Educational and other resource material
- Useful external links

Back to contents

10.0 References

Barthel M, Shearer E, Gottfried J and Mitchell A (2015) *News Habits on Facebook and Twitter* Retrieved from http://www.journalism.org/2015/07/14/news-habits-on-facebook-and-twitter/ (accessed 7 December 2015)

Battles HT (2010) Exploring Ethical and Methodological Issues in Internet-Based Research with Adolescents. *International Journal of Qualitative Methods* 9(1): 27-39. Available at: http://ejournals.library.ualberta.ca/index.php/IJQM/article/viewFile/5017/6480 (accessed 23 December 2013).

Bender A (2013) Australians use up nearly a day on the Internet every week, *CMO*. Retrieved from http://www.cmo.com.au/article/532079/australians_use_up_nearly_day_internet_every_week/ (accessed 1 December 2015)

Brotsky SR and Giles D (2007) Inside the 'pro-ana' community: A covert online participant observation. *Eating Disorders: The Journal of Treatment & Prevention* 19: 93-109.

Boyd D and Crawford K (2011), Six Provocations for Big Data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, September 2011. Retrieved from SSRN:http://ssrn.com/abstract=1926431 or http://dx.doi.org/10.2139/ssrn.1926431 (accessed 15 March 2015)

Buchanan EA and Hvizdak EE (2009) Online survey tools: ethical and methodological concerns of human research ethics committees. *Journal of Empirical Research on Human Research Ethics* 4(2): 37-48.

Buchanan E (2011) Internet Research Ethics: Past, Present, Future. In Ess C and Consalvo M (eds) The Handbook of Internet Studies. Hoboken NJ: Wiley-Blackwell, pp. 83-108

Buchanan E, Aycock J, Dexter S, Dittrich D and Hvizdak E (2011) Computer Science Security Research and Human Subjects: Emerging Considerations for Research Ethics Boards. *Journal of Empirical Research on Human Research Ethics: An International Journal* 6(2): 71-83

Chamber C (2014, 1 July) Facebook fiasco: was Cornell's study of 'emotional contagion' an ethics breach? *The Guardian*. Retrieved from http://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach (accessed 5 December 2015)

Cowling D (2015) *Social Media Statistics Australia – October 2015* Retrieved from http://www.socialmedianews.com.au/social-media-statistics-australia-october-2015/ (accessed 1 December 2015)

Coyne J (2013) Advice to Junior Academics on How to Get Involved With Twitter *Plos Blogs* posted 9 December http://blogs.plos.org/mindthebrain/2013/12/09/advice-to-junior-academics-on-how-to-get-involved-with-twitter/

Evans H, Ginnis S and Bartlett J (2015) *#SocialEthics: A guide to embedding ethics in social media research*. Retrieved from: https://www.ipsos-mori.com/Assets/Docs/Publications/im-demos-social-ethics-in-social-media-research.pdf (accessed 28 November 2015).

Ronson J (2015b, June). *When online shaming spirals out of control* [Video file]. Retrieved from https://www.ted.com/talks/jon_ronson_what_happens_when_online_shaming_spirals_out_of_control?language=en

Golbeck J (2013) *The curly fry conundrum why social media likes say more than you might think* [Video file]. Retrieved from https://www.ted.com/talks/jon_ronson_what_happens_when_online_shaming_spirals_out_of_control?language=en (accessed 23 January 2016).

The History of Social Media Retrieved from http://www.digitaltrends.com/features/the-history-of-social-networking/ (accessed 1 December 2015)

Kemp S (2015) *Digital, Social & Mobile Worldwide in 2015* Retrieved from http://wearesocial.com.au/blog/2015/01/22/digital-social-mobile-worldwide-2015/ (accessed 1 December 2015)

Kramer A D., Guillory, J E., & Hancock J T (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788-8790.

McGranahan M (2013) *The Academic Benefits of Twitter* Retrieved from http://savageminds.org/2013/05/08/the-academic-benefits-of-twitter/ (accessed 7 December 2015)

Munson L (2015, 2 February) Facebook's got a new privacy policy, and it plans to share your data with partners. *Naked Security by Sophos*. Retrieved from https://nakedsecurity.sophos.com/2015/02/02/facebooks-got-a-new-privacy-policy-and-it-plans-to-share-your-data-with-partners/ (accessed 3 December 2015)

NHMRC (2007) *National Statement on ethical conduct in human research*. Retrieved from: http://www.nhmrc.gov.au/guidelines-publications/e72 (accessed 7 March 2015).

Roberts L D (2015)."Ethical Issues in Conducting Qualitative Research in Online Communities." *Qualitative Research in Psychology* 12 (3): 314-325.

Ronson J (2015a). *So You've Been Publicly Shamed*. UK: Pan Macmillan.

Ronson J (2015b, June). *When online shaming spirals out of control* [Video file]. Retrieved from https://www.ted.com/talks/jon_ronson_what_happens_when_online_shaming_spirals_out_of_control?language=en

Rovics D (2014). *How Facebook Killed the Internet*. Retrieved from: http://www.counterpunch.org/2014/12/24/how-facebook-killed-the-Internet/ (accessed 9 December 2015)

Sensis (2015) *Social Media Report May 2015*. Retrieved from: https://www.sensis.com.au/content/dam/sas/PDFdirectory/Sensis_Social_Media_Report_2015.pdf (accessed 1 December 2015)

Tolich M (2004), 'Internal confidentiality: When confidentiality assurances fail relational informants', *Qualitative Sociology,* vol. 27, no. 1, pp. 101–106.

Walton J (2015) *Twitter Vs. Facebook Vs. Instagram: Who Is the Target Audience?*. Retrieved from: http://www.investopedia.com/articles/markets/100215/twitter-vs-facebook-vs-instagram-who-target-audience.asp (accessed 7 December 2015).

Whiteman N (2012) *Undoing Ethics: Rethinking Practice in Online Research*. London: Springer.

Back to contents

11.0 Other recommended reading

Griffith University Research Ethics Manual (Booklets 1, 2, 17, 21, 22 and 23 are recommended for all researchers).

Markham A and Buchanan E (2012) Ethical Decision-Making and Internet Research Recommendations from the AoIR Ethics Working Committee (Version 2.0). Available at: http://www.aoir.org/reports/ethics2.pdf (accessed 23 December 2013).

NHMRC (2018) *Australian Code for the responsible conduct of research*. Retrieved from: https://www.nhmrc.gov.au/guidelines-publications/r41 (accessed 12 July 2018).

Roberts L D, and Allen P J (2015)"Exploring ethical issues associated with using online surveys in educational research."*Educational Research and Evaluation* 21 (2): 95-108.

Sveningsson Elm M (2009) How do Various Notions of Privacy Influence Decisions in Qualitative Internet Research? In: Markham A and Baym N (eds) *Internet Inquiry: Conversations About Method*. Thousand Oaks, CA: Sage, pp. 69-87.

Zimmer M (2008) More on the 'Anonymity' of the Facebook dataset – it's Harvard College (Updated). Available at: http://www.michaelzimmer.org/2008/10/03/more-on-the-anonymity-of-the-facebook-dataset-its-harvard-college/

Zimmer M (2010) 'But the data is already public': On the ethics of research in Facebook. *Ethics and Information Technology* 12(4): 313-325.

Back to contents

12.0 Glossary

Big Data
- Data with potential for high correlation to other data.

Erganomic
- A system/space designed specifically to minimise human injury

Extinguish (Psychpology)
- A technique/activity intended to resolve egative thought and feelings

GUREM
- Griffith University Research Ethics Manual

IRB
- Institute Review Board (US human research ethics committee)

National Statement
- *National Statement on Ethical Conduct in Human Research*

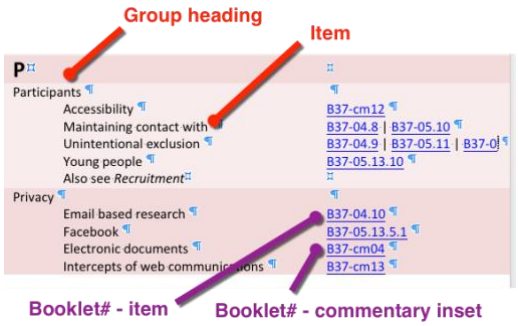
REA
- Research Ethics Adviser

Wi-Fi
- Technology that enables a device to connect to a network/the Internet

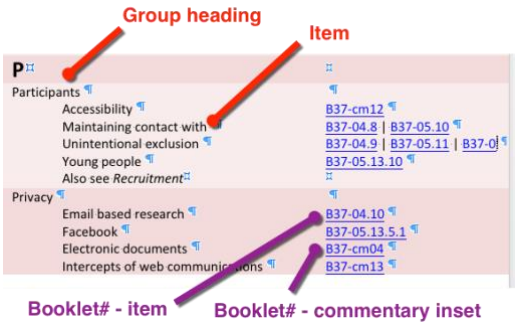
Back to contents

13.0 Booklet Index

Index key



Index key



Click here to access the consolidated index of the entire GUREM.

Back to contents