UNIVERSITY OF TECHNOLOGY SYDNEY

Professor Kathryn McGrath
Deputy Vice-Chancellor (Research)
15 Broadway, Ultimo NSW 2007

PO Box 123
Broadway
NSW 2007 Australia
www.uts.edu.au

UTS CRICOS PROVIDER CODE 00099F

September 14, 2022

Office of the National Data Commissioner (ONDC)
By Email: information@datacommissioner.gov.au.

UTS Response to the Data Availability and Transparency Data Code 2022 Consultation

The University of Technology Sydney (UTS) welcomes the opportunity to comment on the Data Availability and Transparency (DAT) Code 2022 Consultation paper August 2022" published by the Data Commissioner at Consultation and Engagement | Office of the National Data Commissioner.

UTS values the important work and effort to increase the availability and accessibility to data held by public sector agencies. The DAT Code must continue to enable research activities that support and deliver value to industry partners, create knowledge with our students, inform public policy and generate real impact in our communities.

General comments on the Data Availability and Transparency Data Code

Impacts on University research in the application of the Act

Universities have existing arrangements in place with government agencies for the provision of data that supports research and development activities. These existing data sharing arrangements should continue to remain in place with the introduction of the Data Availability and Transparency Act. UTS was advised in an information session, that the code is not designed to restrict existing arrangements but to serve as an alternate pathway to access data from agencies and government departments covered by the Act. UTS would welcome clarity on the application of the Act to ensure there are no adverse impacts on the ability to conduct research, recognising the robust governance and legislative requirements already in place.

Impacts on Accredited Data Users

Universities would benefit from increased clarity on the impact on Accreditation in the event of a data breach, by a subunit or area that is not involved in research and development activities. Assuming each sub-unit has been assessed against the criteria, and then any decision to suspend or cancel that accreditation should be independent of the broader institutional accreditation, even where an investigation is required to understand any broader, systemic issues that may have resulted in the data breach.

In the unlikely event a University is denied accreditation when seeking to become an Accredited Data User (ADU) or Accredited Data Service Provider (ADSP), clarity is required as to whether existing data sharing arrangements with relevant departments would continue as if accreditation had not been applied for. This would be consistent with the above section (*Impacts on University research in the application of the Act)* that ensures existing research is not impacted by the introduction of the Act.

Response to specific Questions outlined in the Consultation Paper

1. Is the approach to weighing arguments for and against the project serving the public interest appropriate? If not, how else could entities assess whether a project for the purpose of informing government policy and programs, or research and development, serves the public interest?

It does seem to put the onus on Universities to determine if the research meets the public interest test, without sufficient guidance. It is far easier to identify the public interest factors, but the factors to determine which has more weight can sometimes be difficult and time consuming.

Universities in NSW have similar obligations under over Government Information (Public Access) Act (the GIPA Act) which is our Freedom of Information legislation. There is "guidance" on public interests in favour of the release of information and consider anything that supports release; but under GIPA, there are prescribed factors against release and only these factors can be applied and used. There are similar obligations for documents that are conditionally exempt under the Cwlth Freedom of Information (FOI) Act. In these cases, there are legislative protection in place for agencies in making such decisions.

The Code should recognise the additional responsibilities for handling and accessing Indigenous Data, acknowledging and highlighting that there is a greater requirement for use than "public interest" in line with The AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research.

The Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989 (Cth), section 5, C.ii gives the responsibility to AIATSIS to provide leadership in ethics and protocols for research and activities relating to collections about Aboriginal and Torres Strait Islander peoples. The Code should make greater reference to the Principles outlined in the AIATSIS Code, in particular Principle 2 Indigenous Leadership and Principle 3 Impact and Value (pp.17-21) when assessments about the use and benefit of sharing the data are being made. This is especially because the AIATSIS Code refers to the use of existing data, like Principle 1 Indigenous Self-Determination 1.11 a & c (p.16), which should be highlighted and used when making such assessments.

2. If yes to the above, are the requirements of what entities must do, to weigh up arguments for and against the project serving the public interest, clear and unambiguous, and is this list proper and pragmatic? In your response, please provide reasons.

An entity attempting to identify what is in the public interest will be challenging. Consideration to the existing freedom of information (FOI) legislation would be of benefit given significant work has been done in this space, whilst acknowledging these laws generally cover release to the pubic generally, not necessarily sharing under any restrictions.

3. Is the list of projects that do not serve the public interest able to be practically applied? What, if any, further guidance is required to support entities consider when a project does not serve the public interest?

The list at 7.5 could be misapplied without further guidance from the Commissioner. To provide an example (noting that other cases may not be as clear), section 7.5 (a) and (b)

imply that using government data to inform research on water & waste management in Kiribati *could* be ruled not in the public interest. Universities often conduct research on a global scale to address global problems and in this case, the national public interest includes the resilience of our Pacific neighbours. In more complex research projects, it may not be reasonable to expect data custodians to possess the expertise to judge such requests. This also goes to question 14 – is the reasonable person test adequate? The terminology in 5 (d) (“the project is *merely* of interest to the public", emphasis added) could also lead to requests being rejected. An example could be a researcher looking into trends relating to public education having a request rejected due to the data provider not deeming the research to have substantive "benefit" beyond being "merely interesting". A method for recourse or greater clarity about what would constitute a project that "is merely of interest" is required.

Possible mitigations could include

a) The provision of guidance via illustrative examples;
b) Category 1 grant research projects have already passed an expert-informed public interest test and should be weighted more favourably; and
c) An appeal mechanism for rejected requests.

4. Are the notes contained in this section helpful, and would this section benefit from other illustrative examples provided as notes? If yes, what examples and under which subsections?

Yes, as per response in Question 3

5. Under the draft data code, entities must have regard to any process of ethics applicable. Do you have any comments about this approach?

This approach seems reasonable as universities already have considerable experience in dealing with questions of ethics and integrity, and handling sensitive information in research. Research in Australia is governed by the *Australian Code for Responsible Conduct of Research* and its accompanying guidelines.

- The Australian Code guideline for ‘Management of Data and Information in Research’ provides an outline of individual and institutional responsibilities for managing research data, which would align well with the accreditation process.
- The National Statement on Ethical Conduct in Human Research outlines requirements for the collection, use and management of data relating to human participants
- Frameworks to support the use of Indigenous data should be considered, e.g. AIATSIS Code of Ethics, as described in the response to question 3
- The new Guidelines to Counter Foreign Interference in the Australian University Sector consider issues of cyber-security and the appropriateness of data sharing with foreign interests.

6. Is the note provided to assist entities identify ethics processes helpful? Why, or why not?

Yes, it is helpful in that it clarifies the circumstances under which ethics approval might or should be sought, and provides appropriate cross-reference to the two key ethics guides referred to above in response.

7. Are the requirements of this element of the people principle clear and unambiguous? What, if any, further details or guidance could assist?

Yes, the requirements of this element are clear. The onus of both identifying and managing any conflict of interest that arises at any stage during a data sharing agreement is on the accredited entity, or 'collector' as referred to in the Act. Accredited users will need to ensure that their processes for disclosing and managing conflicts of interest are fit for purpose for accreditation under the DATA Scheme.

UTS, like most universities, has existing mechanisms in place for disclosing and managing conflicts of interest, which apply to all staff within the UTS Code of Conduct, and to all researchers (including HDR students) within the UTS Research Policy. It is envisaged that these existing process will align with, and can be referred to, as part of becoming an Accredited User under this Scheme.

Clauses 8 and 9 in the Exposure Draft address the expectations around conflicts of interest. Referring again to conflicts in the following section on Appropriate Persons (Section 10(4) (a-d) becomes somewhat circular and confusing. It may be helpful to refer to these examples of conflicts within People Principle 8 (subsection 3) rather than as relevant affiliations for appropriate persons.

8. Is the example provided under this section helpful? Why, or why not?

The example provided is useful, however could be enhanced in two ways, namely (a) by outlining the ways in which the conflict of interest is problematic, and (b) by giving an example of the controls that can be applied once the conflict arises.
This section might also be enhanced by including additional examples, for example a situation where a researcher or person accessing the shared data might have a financial or commercial interest (akin to the relevant affiliations referred to in Section 10(4) (a-d)).

9. Are the attributes, qualifications and affiliations listed in this section appropriate and easy to understand?

These appear to be reasonable expectations of suitably qualified persons.
It is also important to recognise that research conducted within universities will include the training of graduate students, and there may be instances when short-term research projects involving data sets require access by students. Students, as Research trainees, share the same responsibilities as staff under the Australian code for the Responsible conduct of Research, who may not be covered in the same way as academics (employees) of the accredited organisation.

The skills and qualifications of graduate students is being developed and should not preclude the ability to share data where students work on these projects. It would be useful to consider graduate students in the development of more specific guidance around access and accreditation and data sharing for these roles that are integral in the research undertaken at universities.

10. Would this section of the draft data code benefit from other illustrative examples provided as a note? If yes, what examples and under which subsections?

It is beneficial to incorporate examples relating to graduate students, who will have strong support, via supervision, when working on research projects as described in the response to question 9.

11. Is this section adequate in clarifying what are reasonable security standards?

The reasonable security standards appear inadequate as they are very broad and offer limited guidance. Sharing of Australian Government data under this act could benefit from a more precise reference to a relevant security framework. The application of the Protective Security Policy Framework (PSPF) and the data classification and handling requirements contained within that framework, appear suitable as the PSPF would need to be enforced for any data classified at protected and above

There is a strong link with privacy and the relevant security controls to cater for different data classifications. The ability to bring together the privacy and security aspects will ensure appropriate and standard data handling and controls are established.

Consideration of non-technical security standards and activities required by organisations to undertake to improve awareness and education would be a worthwhile inclusion.

12. Would this section benefit from an illustrative example provided as a note? If yes, what are some proposed examples?
The inclusion of examples would be valuable. Examples relating to the different types of data classifications, different levels of aggregation and where data is integrated, via ADSP and contains a mix of data classifications.

13. In practice, this element of the data principle, the privacy protections, and three data services set out in the Act, all work together to provide a framework to appropriately protect data. ONDC acknowledges there is a need to strike the right balance between taking a layered approach and not making the DATA Scheme too complex. Could the draft data code be improved to better assist entities apply this element of the data principle?

There is a need to ensure balance and there is a definite risk that the process becomes too onerous and complex to administer resulting in delays in data access that can fundamentally affect the research being undertaken, if the data provider considers the data should be altered.

The data principle section would benefit from a sensitivity threshold that must be met for sharing to be considered subject to the Code. Data that is classified “public” should be exempted from the Code (for example, data on TERN, GeoScience Australia etc.).

14. Is the ‘reasonable person’ test adequate in this section? If not, how could this section be improved to allow the entities to test whether the data proposed to be shared, collected and used is reasonably necessary to achieve the data sharing purpose?

The reasonable person test may be adequate in most cases, but there may also be cases where a reasonable person cannot reasonably be expected to make a judgement call outside their area of expertise. Such cases may require an escalation mechanism, whether to a peer community, expert panel or the Commissioner.

15. In practice, the output principle requires entities to agree how the accredited user will use shared data. Overall, how could the draft data code be improved to best assist entities apply the output principle?

This section of the Act is quite complex and it is unclear how it will interoperate with other federal government initiatives which regard research data as a research output.
Under NCRIS funding, ARDC and Universities have invested substantially in promoting open publication of research data to improve research integrity, quality and re-use of data ('Open Science'). Some research funders (e.g. ARC, NHMRC) and an increasing number of journals require publication of source and/or derivative data products that may be at least partially sourced from government agencies (e.g. ABS, Geoscience Australia, CSIRO, IMAS, etc.). Consequently, universities have already invested in safe and appropriate data publication, commonly using the five-safes framework. There should be clear criteria determining what data can be safely shared and published to non-accredited users, otherwise the Code may have the perverse consequence of reducing data availability and limit our ability to promote data re-use.

Security Classification could provide a guide to whether derivative data products can be "exited" from the DATA scheme; for example, if a product has been vetted to ensure a security classification of "public" is appropriate. Conversely, an output could be security classified higher than the input with impacts for sharing.

A further complication with respect to Data Sharing Agreements is that additional data publication requirements may arise after the creation of a Data Sharing Agreement (i.e. Publication requirements would not be known this early in a research project). Whilst there are provisions to modify a Data Sharing Agreement, there is presumably no guarantee that this will be agreed by the Data Custodian and presents a risk to the researcher and the research outcome.

The Code is a significant step forward in bringing these practices to non-research agencies but it is equally crucial that it supports the continuation of Open Science initiatives *without additional imposts* given that data publication is resource intensive.

16. One of the objects of the Act is to enable the sharing of data consistently with the Privacy Act and appropriate safeguards. Does this part of the draft data code strike the right balance between holding data custodians accountable to seek consent, and providing data custodians with an exception to collect consent in circumstances where it is genuinely unreasonable or impracticable to seek consent? How could the draft data code be improved to achieve the right balance? For example, could the National Health and Medical Research Council waiver of consent guidelines be used here?

Generally the draft code provides the right balance for privacy and Human Ethics National Statement on Ethical Conduct in Human Research (2007) - Updated 2018 | NHMRC? UTS already has HRECs in place and is covered by NSW privacy legislation. There are differences between the draft code and the NSW Privacy legislation. Statutory codes apply covering personal information and health information in research that define our obligations on disclosing/publishing information for research if we are not able to meet the privacy principles generally (for example, if it is not possible to obtain consent). There is a preference in the codes to anonymizing/tokensing/masking data in this respect.

A notable absence in the list of Accredited Data Service Providers (ADSP) services is data linkage by agencies such as CHeReL (Centre for Health Record Linkage) which operate

under the Federal PHRN network. It is common for federal government data (e.g. ABS) and state data to be linked by these agencies for health and medical research. Some of these providers enable a valuable contribution to research and an underrating of how the linked data service applies to ADSPs.

17. Is this part of the draft data code adequate in providing further clarification for what considerations should be taken into account when determining whether it is necessary to share personal information to properly deliver a government service? How could this section be improved?

As above, guidance on the status of linked data involving federal data would be helpful, particularly since linked data may be more identifying despite the removal of sensitive, personal information and unique identifiers.

18. Does this part of the draft data code provide an adequate list of factors for data custodians to consider when determining whether the public interest justifies the sharing of personal information without consent? Would this section benefit from an example provided in a note, and if so, can you suggest one?

The National Statement on Ethical Conduct in Human Research (2018, Section 2) contains helpful advice on risk/benefit evaluation. In evaluating risk to individuals, the distinction between "harm", "discomfort" and "inconvenience" is also very useful to incorporate (Section 2.1).

19. Should the data sharing agreement include any additional details about the designated individual who is a foreign national?

Universities are already regulated around foreign engagements (with compliance obligations articulated through government agencies including DFAT, Defence, Attorney General, and Home Affairs), and have processes in place for risk assessment and due diligence for research involving foreign nationals, either as students or collaborators (staff and honorary appointments). Further information on why this is necessary and whether it is for all data sharing agreements or particular projects will be helpful to understand given the sensitive nature of the information that would need to be collected. It should also be noted that blind Peer Review might involve sharing non-sensitive data with anonymous (possibly foreign) reviewers if data is requested as part of the peer review process.

If additional information is collected on foreign nationals, further guidance on the inclusion of persons who have dual nationalities and are Australian Citizens will be required and consideration to supporting data requests where the data is non-sensitive.

20. This part of the draft data code is informed by the list prescribed in section 130 of the Act. Is this an appropriate approach, and are there any additional details that should be provided to the Commissioner outside of that list?

It would be optimal to incorporate the role of the NDA council and the process for handling and managing complaints in the event data is not shared with an Accredited Data User.

21. Is 31 July an appropriate deadline for data custodians to provide information and assistance to the Commissioner to prepare for the annual report?

This seems acceptable.

22. What additional topics could the data code include to assist the establishment or integrity of the DATA Scheme?

Please provide further details on the review mechanism if a Data Custodian denies a data request. Is there a role for the NDA Council in this?

Potential opportunity to review and suggest areas for improvement before declining an accredited user's request, enabling time to clarify and or refine existing processes, should they be required.

An additional section referencing or listing the range of reference material would be useful, given the wealth of documents (The Australian Code, the National Statement, etc.) that would inform not only the drafting of this Code but also to provide additional guidance to users and entities.

Yours sincerely,

Professor Kate McGrath
Deputy Vice-Chancellor and Vice-President (Research)