Office of the Information Commissioner
Queensland

Decision and Reasons for Decision

Citation:	***K41 and Griffith University* [2026] QICmr 29 (23 February 2026)**
Application Number:	**318301**
Applicant:	**K41**
Respondent:	**Griffith University**
Decision Date:	**23 February 2026**
Catchwords:	**ADMINISTRATIVE LAW - RIGHT TO INFORMATION - INFORMATION PRIVACY ACT - APPLICATION FOR PERSONAL INFORMATION - DOCUMENT OF AN AGENCY - applicant applied under the *Information Privacy Act 2009* (Qld) for his personal information held by Microsoft - right of access to personal information - meaning of personal information - whether information is about the applicant - whether the applicant's identity can be reasonably ascertained from the information - whether the information is in the possession or under the control of the University - section 12, 13 and 40(1)(a) of the *Information Privacy Act 2009* (Qld) - section 12 of the *Right to Information Act 2009* (Qld)**

REASONS FOR DECISION

Summary

1. The applicant applied[1] to Griffith University (**University**) under the *Information Privacy Act 2009* (Qld) (**IP Act**)[2] for access to five specific categories of *'personally identifying information about* [him] *held by Microsoft'*.

2. The University located documents with respect to two categories of information and decided to release these to the applicant.[3] However, access to the remaining three categories of information was not given on the basis that the information was contrary to the public interest to release, or was nonexistent or unlocatable.

3. The applicant applied for internal review[4] of the University's decision with respect to the three refused categories of information. On internal review,[5] the University affirmed its

[1] Access application dated 5 July 2024.
[2] On 1 July 2025 key parts of the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (**IPOLA Act**) came into force, effecting significant changes to the *Right to Information Act 2009* (Qld) (**RTI Act**) Act and the IP Act. References in this decision to the RTI Act and IP Act, however, are to the those Acts **as in force prior to 1 July 2025**. This is in accordance with Chapter 7 Part 9 of the RTI Act and Chapter 8, Part 3 of the IP Act, comprising transitional provisions requiring that access applications on foot before 1 July 2025 are to be dealt with as if the IPOLA Act had not been enacted.
[3] University's decision dated 22 August 2024.
[4] Applicant's internal review application dated 9 September 2024.
[5] University's internal review decision dated 11 October 2024. This is the *reviewable decision* for the purpose of this review.

earlier decision that releasing the information would be contrary to the public interest and that information could be refused because it was nonexistent or unlocatable.

4. The applicant applied to the Office of the Information Commissioner (**OIC**) for external review[6] of the University's decision to refuse access to two of the three categories of refused information, held by Microsoft.[7]

5. For the reasons explained below, I set aside the University's decision and find that there is no right of access to the information sought on external review under section 40(1)(a) of the IP Act because that information does not comprise the applicant's personal information and / or the documents containing that information are not documents of the University.

6. In making this decision, I have considered evidence, submissions, legislation and other material as set out in these reasons.[8] I have also had regard to the *Human Rights Act 2019* (Qld) (**HR Act**), particularly the right to seek and receive information,[9] and in doing so, have acted in accordance with section 58(1) of the HR Act.[10]

Background

7. The applicant sought access to five categories of *'personally identifying information about* [him] *held by Microsoft'*. Only two of the five categories remain in issue in this external review,[11] namely:[12]

> *(1) Tracking identifiers and relevant logs linked to* [the applicant] *such as cookies, IP addresses, user agents, web browser configurations and other relevant identifiers* **(Category 1)**.
> …
> *(5) All records transferred to Snowflake Inc and/or SCUBA* **(Category 5)**.

8. As the applicant applied to the University for access to information under the IP Act, the University processed the applicant's request for access to the applicant's personal information *collected by* the University[13] - that is, only information '*collected by* [the University] *for the provided staff account and/or devices used by the applicant in their employment at* [the] *University'.*[14]

9. With respect to Category 1, the University provided the applicant with samples of the type of information it located responsive to his request and asked the applicant to provide further information to assist in its searches. The applicant confirmed the samples of information located by the University did not capture the information he was seeking but confirmed he would '*like a list of* ***MUIDs*** [Microsoft User Identifiers]*, and a list of domains each has been associated with..'.*[15] The applicant considered that the MUIDs were available to him under

---

[6] External review application dated 5 November 2024.
[7] On external review, the applicant confirmed he no longer sought access to the remaining category of information.
[8] Including footnotes.
[9] Section 21 of the HR Act.
[10] OIC's approach to the HR Act set out in this paragraph has been considered and endorsed by the Queensland Civil and Administrative Tribunal in *Lawrence v Queensland Police Service* [2022] QCATA 134 at [23].
[11] In the applicant's external review application dated 5 November 2024, the applicant advised OIC he did not seek access to the remaining category of refused information. As such, it does not form part of this decision.
[12] During the initial access request, the University provided the applicant access to '*History of non-Microsoft links that* [he had] *clicked/accessed in Microsoft Teams & Microsoft Outlook*' and '*Logs and timestamp of* [his] *online activity in Microsoft Teams'*.
[13] Under section 12 of the RTI Act, which applies by virtue of section 13 of the IP Act, an applicant is entitled to access documents *'in the possession, or under the control, of the agency…'*. The University advised the applicant that copies of information collected and retained by Microsoft associated with his University provided staff account are available for access on https://account.microsoft.com/account/privacy.
[14] Submissions from the University provided to OIC on 16 January 2025 (**Architecture Brief**), page 5.
[15] Applicant's submissions to the University dated 8 August 2024, provided to the University during its processing of the applicant's initial access request. Throughout this decision, references to 'MUID', 'MUIDs' and 'MUID information' all refer to Microsoft User Identifiers as sought by the applicant with respect to Category 1. For more information, see paragraph [35] below.

the IP Act as these were '*identifiers that can be used to identify* [him]*, such as the MUID…*[and that this is his] *personal information as* [he] *can reasonably be identified by it'.*[16]

10. In its searches for documents containing information responding to Category 1 of the applicant's request, the University located two excel spreadsheets/logs containing 'IP Logs'[17] and 'Successful Authentications'[18] (**located logs**).[19] The University refused access to the located logs on the basis that it was contrary to the public interest, finding that it was '*unable to provide this information on the basis that doing so could pose a security issue to the University/impact the privacy of others'.*[20]

11. With respect to documents containing Category 5 information, the University requested further information from the applicant relating to Snowflake Inc (**Snowflake**)[21] and SCUBA.[22] When doing so, the University observed '*Snowflake is a data hosting and analysis service provider. Copies of all records or data transferred to a particular data service provider would not be within the* scope *of an RTI/IP Act request as it is too broad*.'[23] In response the applicant advised that '*my concern is that Snowflake is being used to share "anonymised" or "masked" (often just pseudonymised) PII to third parties outside of* [the University]*, Microsoft and Snowflake using "data clean rooms" and "data exchanges", two of Snowflake's major offerings…I would like to confirm if my pseudonymised PII, or PII that has gone through a "data clean room", "data exchange" or similar mechanism'.*[24] The University refused access to documents containing the Category 5 information on the basis that it was nonexistent or unlocatable by the University as it was not the collecting 'agency' for this information.[25]

12. The applicant sought internal review[26] of the University's decision. On internal review,[27] the University affirmed its original decision in relation to Category 1 information (although it did give different weight to certain factors favouring nondisclosure of the information).[28] The University also affirmed its original decision in relation to Category 5 information.[29]

13. On external review, the applicant sought review of the University's decision to refuse access to the Category 1 and Category 5 information. Throughout the external review, the

---

[16] Applicant's submissions dated 8 August 2024, provided to the University during the initial access request.
[17] These logs are '*commonly collected with personally identifiable data points about users that include IP addresses and web browser configurations, however they do not necessarily contain personal and private information about a user as defined in the* [IP Act]. See Architecture Brief page 5.
[18] The '*authentication logs are commonly collected to monitor and respond to malicious attempts to gain access to* [the University] *data via known vulnerabilities.* See Architecture Brief page 5.
[19] The University provided copies of this information to OIC on 24 April 2025. The located logs included information such as IP addresses and the applicant's student identification number. While information has not been released to the applicant, samples of it were provided to him during the processing of the initial access request. See Architecture Brief, page 5. The applicant confirmed on 3 July 2025 that this information '*would not be sufficient for the information that* [he] *requested from Microsoft, as a contractor of* [the] *University'.*
[20] University's decision dated 22 April 2024.
[21] The University proceeded on the basis that the applicant was referring to the cloud services provider (a data host) of the same name. See the Architecture Brief, page 8 and 12.
[22] The University proceeded on the basis that the applicant was referring to the data analysis application of the same name. See Architecture Brief, page 8.
[23] Correspondence from the University to the applicant during the initial access request, dated 8 August 2024.
[24] Applicant's submissions dated 6 September 2024, provided to the University during the initial access request.
[25] Section 67(1) of the IP Act and sections 47(3)(e) and 52(1)(a) of the RTI Act.
[26] The applicant sought internal review on the basis that '*Microsoft* [was] *over-collecting data and disclosing staff and student data to third party data brokers'* and the University's mandated use of '*Microsoft's cloud utilities'* as this could allow the *'collection and potential disclosure of a deep set of information about staff and students…*'. The applicant also submitted that he sought access to his personal information that was disclosed to *'data brokers'* and a '*list of third parties which Microsoft and its subcontractors may have disclosed personally identifiable information via "data clean rooms*"'. Internal review application dated 9 September 2024.
[27] Internal review decision dated 11 October 2024.
[28] I.e. release of the information was contrary to the public interest because it would prejudice the business affairs and security of the University - schedule 4, part 3, items 2, 7 and 15 of the RTI Act.
[29] The applicant's request for his information that had been disclosed to '*data brokers'* and a '*list of third parties which Microsoft and its subcontractors'* was not considered as it was outside the applicant's original request.

applicant submitted that the MUID information he requested in relation to Category 1 comprised his personal information held by the University, as a contractor of Microsoft. The applicant also submitted that the Category 5 information was 'information of an agency' – the i.e., the University – and should have been located by the University. The applicant's submissions are outlined in paragraph [0]-[30] below.

Issues for determination

14. On external review, the University changed the basis for its position on nondisclosure of Category 1 information to the applicant. The University submitted to OIC that the MUID information sought by the applicant should be refused because it did not meet the definition of the applicant's personal information accessible under the IP Act. The University also submitted that it is not information held by the University.

15. In relation to Category 5 information, the University maintained its position that this information was nonexistent or unlocatable because the information was not information held by the University. The University submitted that '*there is no scope for* [the University] *to determine if* [the applicant's] *personal and private information was collected by an application that uses a Snowflake data store or SCUBA service if the applicant does not provide any context*.'[30]

16. The issues for determination in relation to Category 1 is whether the information the applicant is seeking:

    - comprises the applicant's personal information which can be requested under the IP Act; and or
    - is contained in a '*document of an agency'* which can be requested under the IP Act.

17. The issues for determination in relation to Category 5 is whether the information the applicant is seeking is a '*document of an agency'* which can be requested under the IP Act.

18. Although the University processed the application, issued decisions under the IP Act, and released information in response to part of the access application (i.e. two categories of personal information), the threshold issue of whether the request for Category 1 and 5 information can be made under the IP Act remains to be determined in this review.[31]

Relevant law

19. Under the IP Act, an individual has a right to be given access to documents ***of an agency*** to the extent they contain their ***personal information***.[32] The legislation is to be administered with a pro-disclosure bias,[33] however, the right of access is subject to certain limitations, including grounds for refusing access.[34]

[30] Architecture Brief, page 9.
[31] Under section 118 of the IP Act, on external review the Information Commissioner can decide any matter in relation to an access application that could have been decided by an agency.
[32] Section 40 of the IP Act.
[33] Section 64 of the IP Act
[34] Section 67(1) of the IP Act and section 47 of the RTI Act. Those grounds are however, to be interpreted narrowly: section 67(2) of the IP Act.

Personal information

20. The legislative scheme[35] makes a clear distinction between access to personal information under the IP Act, and non-personal information of an individual that can be requested under the RTI Act. '*Personal Information*' under the IP Act is defined as:

> *information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not,* ***about an individual*** *whose* ***identity is apparent, or can reasonably be ascertained****, from the information or opinion.*
>
> [emphasis added]

21. For information to qualify as personal information, two criteria must be satisfied:

- the information or opinion must be *about* the individual; and
- the individual's identity must be *apparent or reasonably ascertainable* from the information or opinion.

22. Whether information is a particular individual's personal information will depend on the facts of each specific case.[36] The threshold question to be answered is whether the information is *'about'* the applicant.[37] It is not enough that an individual is identifiable; the information must also say something '*about'* the individual. The words 'about an individual' have been found to direct attention to the need for the individual to be a subject matter of the information. While information and opinions can have multiple subject matters, it is necessary, in every case, to consider whether each item of information requested, individually or in combination with other items, is 'about an individual'. This requires an evaluation of the facts in each case[38] and is a question of fact, to be resolved by reference to the information itself.[39]

23. An individual's identity must be 'apparent' or 'can reasonably be ascertained' from the information.[40] The Information Commissioner has previously considered that the following factors will influence whether an individual's identity can be reasonably ascertained:[41]

- how available the additional information is
- how difficult it is to obtain
- how many steps are required to identify the individual
- how certain the identification will be
- whether it will identify one specific individual or a group of people; and
- whether the individual receiving the information can use it to identify the individual.

---

[35] Prior to the commencement of the IPOLA Act which, as noted at footnote 2 above, remains applicable for the purpose of this review.
[36] *Mahoney and Ipswich City Council* (Unreported, Queensland Information Commissioner, 17 June 2011) at [19] (***Mahoney***).
[37] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4. In this case the Full Federal Court considered the considered the equivalent definition of 'personal information' in the *Privacy Act 1988* (Cth). Like the definition in the IP Act, this definition requires the information to be about the individual who has requested access, and whose identity is apparent, or can reasonably be ascertained, from the information or opinion (see the definition in Part II – interpretation).
[38] *X85 and Economic Development Queensland* [2025] QICmr 26 (22 May 2025) (***X85****)* at [14]-[15], citing *Telstra Corporation Limited.*
[39] *X85* at [15].
[40] Section 12 of the IP Act and *C72 and Queensland Curriculum and Assessment Authority* [2024] QICmr 12 (22 March 2024) at [131].
[41] *Mahoney* at [21] as applied in *Tomkins and Rockhampton Regional Council* [2016] QICmr 2 (22 January 2016) (***Tomkins***) at [16] and *Alsop and Redland City Council* [2017] QICmr 27 (2 August 2017) (***Alsop****)* at [21].

Document of an agency

24. As noted above, section 40 of the IP Act creates a legally enforceable right for an individual to access information about them that is held by Queensland Government agencies. Section 12 of the RTI Act[42] relevantly defines 'document of an agency' as follows:

> *…a document…in the possession, or under the control, of the agency whether brought into existence or received in the agency, and includes –*
> *(a) a document to which the agency is entitled to access; and*
> *(b) a document in the possession, or under the control, of an officer of the agency in the officer's official capacity.*

25. In earlier decisions, the Information Commissioner has found that mere physical possession of a document[43] by an agency is sufficient to meet the above requirements and subject the document to the operation of the RTI Act.[44] Possession does not require formal legal possession nor is it concerned with the means by which the documents came into the agency's possession.[45] However, it is limited to instances where the agency is legally entitled to produce the requested documents.[46]

26. Physical possession is not, however, the sole test as to whether a document is a document of an agency. A document not in the physical possession of an agency will nevertheless be a 'document of an agency' if it is 'under the control' of the relevant agency. This includes documents to which an agency is 'entitled to access'.[47] The Information Commissioner has previously explained that a document will be under the control of an agency[48] where the agency has a present legal entitlement to take possession of the document.[49]

27. If the information sought is not a document of an agency under section 12 of the RTI Act, there is no right of access to it under section 40(1)(a) of the IP Act.

Submissions

Applicant's submissions

28. In the applicant's request for internal review, he explained he was seeking access to his personal information '*held by Microsoft'* because he was concerned that '*Microsoft is over-collecting data and disclosing staff and student data to third party data brokers*'.[50]

---

[42] In conjunction with section 13 of the IP Act.
[43] Including electronic documents. See section 36 and Schedule 1 of the *Acts Interpretation Act 1954* (Qld).
[44] *Kalinga Wooloowin Residents Association Inc. and Department of Employment, Economic Development and Innovation; City North Infrastructure Pty Ltd (Third Party)* (Unreported, Queensland Information Commissioner, 19 December 2011) (***Kalinga***) and *Kalinga Wooloowin Residents Association Inc and Brisbane City Council and Ors* (Unreported, Queensland Information Commissioner, 9 May 2012), each applying *Holt and Reeves and Education Queensland and Ors* (1998) 4 QAR 310 (***Holt***). While *Holt* concerned section 7 of the *Freedom of Information Act 1992* (Qld) (repealed), that provision was framed in substantially similar terms to section 12 of the RTI Act. I am satisfied relevant principles apply equally to section 12.
[45] *Kalinga* at [14]-[15] and [19].
[46] *Carmody v Information Commissioner & Ors (No. 4)* [2018] QCATA 17 at [66] per Hoeben J.
[47] *Queensland Newspapers Pty Ltd and Ipswich City Council* [2015] QICmr 30 (26 November 2015).
[48] Or one which an agency is entitled to access.
[49] *Price and the Nominal Defendant* (1999) 5 QAR 80, at [18] (***Price***). The Information Commissioner went on in *Price* at [33] to explain that the *'…ruling test imposed by the definition of "document of an agency" is comprised in the words "in the possession or under the control of an agency". The remaining words of the definition illustrate, rather than extend, the ruling test'.*
[50] The applicant submitted that this concern stemmed from the following being informed by the '*University Privacy Officer that under the University's agreement Microsoft may transfer/disclose* [his] *information to Snowflake Inc. and SCUBA'* Snowflake and SCUBA '*offer analytics and data brokerage services to Microsoft'*, including '*"data clean room" which allow their clients to share and obtain information on people's activities and preferences, predominately used for behavioural and targeted advertising'.* The applicant also submitted that *'Microsoft's cloud utilities are mandated by the University…allowing collection and potential disclosure of a deep set of information about staff and students…'* and information about how staff or student's typically use '*their workstation could expose them to behavioural targeting from…third-party companies'* '*transparency is really important'* as '*Microsoft is a key vendor to the university with a group number of products through University procurement'.* Further, the applicant submitted that it is '*inappropriate for vendors of the University to expose staff and students to behavioural tracking and disclosure to other third-party complaints outside the control of the University and the Information Privacy Principals…to which it is bound'.*

29. Throughout the applicant's original request and this review, he has submitted he is entitled to the information sought at Category 1 as:

- the University mandates use of '*Microsoft's cloud utilities…',* which allows the '*collection and potential disclosure of a deep set of information about staff and students like when they are online, where they are working from, and potentially even information like what they are working on'*[51]
- '*significant data was being transferred to Microsoft containing usage information seemingly in the style of the Microsoft Clarity product'*[52]
- he is '*seeking identifiers and linked identifiers* [including MUID information]*, which could be used to identify* [him]*…from Microsoft, as a contractor of* [the] *University*',[53] and
- MUID information meets the '*definition of personally identifiable information*' as '*it* "[i]*dentifies unique web browsers visiting Microsoft sites.* [It is] *used for advertising, site analytics, and other operational purposes*"'.[54]

30. With respect to the information sought at Category 5, the applicant has submitted he is entitled to access this information as:

- disclosure (through Snowflake or SCUBA) of information about '*staff or student's typical use of their workstation could expose them to behaviour targeting from…third-party companies*' and he has concerns that Snowflake or SCUBA offer products that '*allow their clients to share and obtain information on people's activities and preferences, predominately used for behavioural and targeted advertising'* ie '*data clean rooms'*[55]
- he '*would like to know if* [his] *personal information is being held by SCUBA and or Snowflake… and if so please provide a list of identifiers and linked identifiers, including but not limited to MUIDs, emails, full name, and hashed/pseudonymised variants of any of those'*[56]
- *'the interpretation that* [the] *University does not have any control or influence by its service provider may be a breach in this instance. It would seem to me that my PII was transferred or disclosed to a separate entity. The University uses terms like "cloud-hosted services" that are irrelevant as they do not recuse the University or its service providers of its responsibilities under the Act'*[57]
- he has gone to '*some length to ensure that* [he does] *not have any relationship with Microsoft "outside" of* [his] *employment'*; [58]and
- he is entitled to this information '*on the assumption that* [the] *University does not consider that a transfer or disclosure has taken place to its service provider in accordance with the IP Act'*.[59]

University's submissions

31. OIC sought further information from the University in relation to its updated position on the information sought at Category 1. In support of its position that the Category 1 information,

[51] Applicant's internal review application dated 9 September 2024.
[52] Applicant's submissions dated 15 April 2025.
[53] Applicant's submissions dated 3 July 2025.
[54] Applicant's submissions dated 6 November 2025.
[55] Applicant's internal review application dated 9 September 2024.
[56] Applicant's submissions dated 3 July 2025.
[57] Applicant' submissions dated 6 November 2025.
[58] Applicant' submissions dated 6 November 2025.
[59] Applicant' submissions dated 6 November 2025.

in particular MUID information, is not the applicant's personal information, nor is information held by the University, the University submitted:[60]

- '[t]*he MUID…is a browser cookie created by Microsoft, to anonymously track user behaviour on all Microsoft domains'* and '*anonymously record all users who interact with Microsoft web services'*
- a MUID '*does not contain personally identifiable information about any user (account name, email address, personal name) and cannot be used to identify a particular individual who interacts with a Microsoft web service*'
- a MUID is a '*Microsoft cookie stored on the browser of the user that interacts with a Microsoft site or service – regardless of whether the user has or is using a* [University] *account or not*' and this is not created by the University
- '*Information related to MUIDs is collected and held by Microsoft*'
- MUIDs '*cannot be associate*[d with] *each other'* as the multiple MUIDs '*located on a user's device for each browser they use cannot be associated each other'* or with a '*particular individual, even if they use the same account'.*
- Microsoft also creates '*a new MUID…whenever a user clears the browser's cache or cookies'* and as user typically '*clear their browser cookies or cache, Microsoft is constantly creating new MUIDs for all internet users'*
- the University '*does not control or have any influence over what data Microsoft collects via the MUID, as this is a Microsoft ID created by Microsoft to collect usage data about how users use Microsoft sites or services – regardless of whether they have or use a* [University] *provided account or not*'
- the University '*does not control what cookies all users of the internet (including the MUID) choose to delete or not from their devices…'*; and
- further, the '*University is a subscriber of multiple services of Microsoft'*. While '*subscribers purchase the right use Microsoft services for the duration of the subscription agreement. This does not mean* [the University] *have any ownership, control, or influence over how Microsoft collects data'*.

32. In relation to documents containing Category 5 information, in response to the applicant's concerns, OIC sought clarifying information from the University about any information that is 'passed onto' Snowflake and SCUBA, and whether the University can search for the applicant's personal information captured by these tools. In response, the University submitted that:[61]

- '[d]*ue to the nature of cloud-hosted services,* [the] *University does not and cannot search or monitor all data hosted by Snowflake. Snowflake is a data hosting platform, not a data recipient*.'
- '*the data host* (such as Snowflake) *only knows what clients use their data centres to host their data. It is the responsibility of the web service or application developer that uses a particular data host to collect and manage personal and private data appropriately*'
- the University '*does not track how a person uses their university-provided email address with external services. If the Applicant has interacted with a third-party service that uses Snowflake,* [the University] *has no visibility into that interaction or the data involved'*
- the University cannot '*search or scan data host external to* [the University] *for any personal information that may have been sent to the that host by the Applicant through a web service or application'*

[60] University's submissions dated 25 October 2025, pages 1-3.
[61] University's submissions dated 8 October 2025, pages 2 and 3.

- *'SCUBA is a software tool used to manage data. It is not a discrete entity, service or destination that data is "captured by/passed on" to'*
- as SCUBA is an analysis software tool, it is not a '*transfer of data; its* [sic] *just a tool being used'*
- '[n]*o relevant context was provided by the applicant to enable* [the University] *to identify a particular interaction, service, or dataset under its control that would relate to the request'*
- this '*request appears to seek information that may or may not exist within infrastructure not managed by* [the University]'; and
- '*external data host (Snowflake) would not be able to satisfy the request without a specific service or context'*.

Findings

Category 1

33. The issue for determination in relation to the Category 1 information is whether the information the applicant is seeking is contained in documents which can be requested under the IP Act. The relevant consideration is whether the information is *'the individual's personal information'* – that is, personal information of the applicant.

34. Throughout the external review, the applicant's submissions about the Category 1 information have related to his concerns that '*Microsoft is over-collecting data and disclosing staff and student data to third party data brokers*'[62] and, accordingly, raised and discussed MUIDs. The applicant described the information sought on external review as comprising … '*identifiers and linked identifiers, which could be used to identify me. This could include MUID identifiers…'*. Based on this description, it is understood that the Category 1 information sought by the applicant on external review comprises MUID information, and the review has proceeded on this basis.[63]

35. As outlined above, the threshold question to be answered is whether the MUID information is '*about'* the applicant.[64] A MUID is a type of 'third-party cookie'[65] set by a Microsoft product called Microsoft Clarity.[66] The purpose of a MUID is to identify '*unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes'*.[67]

---

[62] See footnote 50.
[63] See for example, the applicant's submissions dated 3 July 2025. With respect to '*linked identifiers',* the only further information provided by the applicant in relation to this was that '*this could include MUIDs that are further linked such as non-logged in traffic, or other accounts*' (applicant's submissions dated 3 July 2025). As such, I am satisfied the Category 1 information sought by the applicant on external review is MUID information. However, if I am wrong about this (and or to the extent that the MUID information 'value passed' is 'GUID' – see Clarity Cookies | Microsoft Learn), I observe that that there are other identifiers such as globally unique identifiers (**GUIDs**), which I understand can be '*non-logged in traffic*'. According to Microsoft, GUIDs and universally unique identifiers are '*intended to serve as a unique identifier for an object'* ([MS-DTYP]: GUID and UUID | Microsoft Learn) and '*can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and RPC objects*'. See [MS-DRSR]: Glossary | Microsoft Learn. Please see footnote 75 below.
[64] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4. In this case the Full Federal Court considered the considered the equivalent definition of 'personal information' in the *Privacy Act 1988* (Cth). Like the definition in the IP Act, this definition requires the information to be about the individual who has requested access, and whose identity is apparent, or can reasonably be ascertained, from the information or opinion (see the definition in Part II - interpretation).
[65] Microsoft defines '[t]*hird-party cookies* [as] *small pieces of data stored on a user's browser by a website other than the one they are currently visiting. These cookies are typically used by external services, such as advertisers, analytics platforms, or social media networks to track user behavior across different websites'*.
[66] Microsoft Clarity's website (https://clarity.microsoft.com/) defines this product as being '*a free user behavior analytics tool that helps you understand how users are interacting with your website through session replays and heatmaps*'.
[67] See https://learn.microsoft.com/en-us/clarity/setup-and-installation/clarity-cookies.

36. With respect to MUIDs on a University provided account and device, the University submitted that:[68]

    - MUIDs can be described as a '*log of interactions of that* [University]-*provided account with Microsoft sites and web services'*
    - the '*personal opinions of the applicant are not contained within the logs of capture of their use of a* [the University] *provided account to interact with Microsoft services'*
    - the information a MUID captures is only the '*domain, not the specific interactions underneath it. E.g. it will indicate they used their* [University] *account to access Bing to conduct a search, but will not reveal the particular search string used'*
    - a MUID is used to '*anonymously record'/'track user behaviour on all Microsoft domains'*
    - a MUID does '*not contain personally identifiable information about any user (account name, email address, personal name) and cannot be used to identify a particular individual who interacts with a Microsoft service'*
    - as a MUID does *'not contain personally identifiable information about the user…different MUIDs created on each* [and any] *devices used by the same user cannot be associated with the same individual';* and
    - a MUID is *'stored locally* [on] *the user's browser cookies'* and *'information related to MUIDs is collected and held by Microsoft'* on its browsers, however this can be deleted by users.

37. According to the University, while a MUID records how users interact with Microsoft web browsers, it does so anonymously.

38. The University also noted that internet users typically have '*multiple MUID's on each device they use'* as there is a '*different MUID* [for] *each different browser* [a user] *uses on* [any specific] *device].* These also cannot be associated with each other as '*multiple MUIDs located on a user's device for each browser'* do not '*contain the account details* [or personally identifying information] *of the user'.* The University provided the following example:[69]

    > *For example, if an individual uses both Chrome and Edge to access the same Microsoft web service from the same device with the same account, they will have different MUIDs in the browser cookies of their Chrome and Edge browsers, with neither MUID being associated with each other or the individual.*

39. While the applicant would have been assigned a MUID by Microsoft when interacting with a Microsoft web service, I do not consider that that MUID is information *about* the applicant. Having carefully considered all material before me, I consider that there is an insufficient connection or link between the MUID and the applicant, such that the applicant's identity would be apparent. In this instance, the connection between the applicant and any MUID is that the MUID is stored locally on the applicant's browser/s – while using his University provided account on a University provided device. The MUID tracks the browsing behaviour of a specific browser/device used by the applicant (through his University provided account).

40. Further, I am not satisfied that the applicant's identity would be *reasonably ascertainable* from any MUIDs. I acknowledge that the applicant '*kept* [his] *use of the Microsoft account at a minimum and only as directed by the University as* [he] *was particularly concerned that*

[68] Architecture Brief page 11 and the University's submissions dated 8 October 2025.
[69] University submissions dated 8 October 2025, page 1.

Microsoft was collecting data about [him] *outside of its agreement with the University'.*[70] I also acknowledge that the applicant considers that MUIDs contain his personal information as it is a cookie that identifies '*unique web browsers visiting Microsoft sites'.*[71] However, the applicant's identity is not reasonably ascertainable from the information in question.[72] I accept the view put forward by the University that while a MUID on a University provided account, on a University provided device, is an interaction '*of that* [University]*-provided account with Microsoft sites and web services',*[73] a MUID itself '*does not contain personally identifiable information about any user (*[such as] *account name, email address, personal name)*'.[74] As such, even if the University was able to obtain/extract a MUID, it cannot be used to identify a particular individual who has interacted with a Microsoft web service. This is further supported as there can also be several MUIDs associated with the applicant's University provided account if he used different Microsoft browsers and different devices.

41. I am not satisfied on the information before me that the applicant's identity is apparent or can be *reasonably ascertained* from a MUID.

42. Accordingly, I am not satisfied that MUID information can properly be characterised as being *about* the applicant.[75] I therefore find that it does not comprise the applicant's personal information under section 12 of the IP Act and, accordingly, there is no right of access to it under section 40(1)(a) of the IP Act.

43. Furthermore, if I am incorrect in finding that the information did comprise the applicant's personal information, I am not satisfied that these Microsoft identifiers are information contained in '*a document of an agency'* which can be requested under the IP Act. As outlined above, the term '*possession*' as used in section 12 of the IP Act includes physical possession or a '*present legal entitlement*' to physical possession.

44. The applicant submits that he is entitled to the tracking identifiers such as a MUID as it is information *'about* [him] *held by Microsoft, as a contractor to* [the] *University, of which* [he has] *no personal relationship with'.*[76]

45. I do not have evidence before me that suggests the University, or any officer thereof,[77] has physical possession[78] to the information Microsoft collects within its products regarding how users interact with their products, as sought at Category 1. I also do not have evidence before me that suggests the University has a legal entitlement to such information. Further, I have no evidence before me that the University can access MUIDs that are stored locally on an applicant's browser, whether the applicant is using a University issued device or not.

46. The University confirmed that tracking information such as MUIDs are '*created by Microsoft whenever any web user interacts with any Microsoft site or Microsoft web service'* and this information is '*collected and held by Microsoft'.* A MUID is *'stored on the browser of the user that interacts with a Microsoft site or service'.* The University has also confirmed it *'does not control or have any influence over what data Microsoft collects via the MUID'.*

---

[70] Applicant's submissions dated 15 April 2025.
[71] Applicant's submissions dated 6 November 2025.
[72] *Re Seven Network (Operations) Limited and Public Transport Authority* [2017] WAICmr 12 at [50]. Also see *Mahoney* at [21] as applied in *Tomkins* at [16] and *Alsop* at [21].
[73] Architecture Brief, page 11.
[74] University submissions dated 8 October 2025.
[75] As noted at footnote 63 above, I consider the Category 1 information sought by the applicant on external review is limited to MUID information. However, if I am wrong about this, to the extent that the applicant was also seeking identifiers such as GUIDs (and or to the extent MUIDs include GUID information), I am also not satisfied that GUID information alone can be properly characterised as being about the applicant, for similar reasoning as set out in [39]-[41]. This is because GUIDs comprise a unique set of numbers of which the applicant's identity cannot be reasonably ascertained.
[76] Applicant's submissions dated 3 July 2025.
[77] In their official capacity (as required by section 12(b) of the RTI Act and noted in *Tol and The University of Queensland* [2015] QICmr 4 (18 February 2015)) or indeed otherwise.
[78] See *L36 and Lockyer Valley Regional Council* [2023] QICmr 59 (8 November 2023).

While the University is a '*subscriber of multiple services of Microsoft',* it only purchases the '*right to use Microsoft services for the duration of the subscription agreement'.*[79]

47. Based on the information provided by the University, I consider that Microsoft identifier information such as MUID is not in the physical possession of the University and there is nothing before me that evidences a legal entitlement of the University to control the use or physical possession of it.[80] Accordingly, I am satisfied that the information sought is not information contained in *'documents of an agency'* within the meaning of section 12 of the RTI Act, and find that there is no right of access to this information under section 40(1)(a) of the IP Act.

Category 5

48. Again, the issue for determination in relation to the Category 5 information is whether the information the applicant is seeking is information which can be requested under the IP Act, and the relevant consideration is whether the information is contained in *'documents of an agency'* – that is, documents of the University.

49. As outlined above, under the IP Act applicants have a right to seek access to their personal information that is held by an agency. '*Documents of an agency'* is not only information which an agency has physical possession but can include information under the control of an agency of which an agency is legally able to produce.

50. Based on the information available on review, Snowflake (a data host) and SCUBA (analysis software tool) are service providers used by Microsoft and or integrated with Microsoft products. The University submits that the information requested by the applicant at Category 5 *'appears to seek information that may or may not exist within infrastructure managed by* [the University]. *Furthermore, the external data host (Snowflake) would not be able to satisfy the request without a specific service or context'.*[81]

51. The University confirmed that:[82]

> [In relation to Snowflake] *[the] University does not and cannot search or monitor all data hosted by Snowflake. Snowflake is a data hosting platform, not a data recipient. The data host only knows what clients use their data centres to host their data. It is the responsibility of the web service or application developer that uses a particular data host to collect and manage personal and private data appropriately.*
>
> [The University] *does not track how a person uses their university-provided email address with external services. If the Applicant has interacted with a third-party service that uses Snowflake, [the University] has no visibility into that interaction or the data involved. It is not possible for [the] University to search or scan a data host external to [the University] for any personal information that may have been sent to the that* [sic] *host by the Applicant through a web service or application.*
>
> *…*
>
> [In relation to SCUBA] *SCUBA is a software tool used to manage data. It is not a discrete entity, service or destination that data is 'captured by/passed on' to…The applicant's original request referred broadly to information that may have been collected or processed by external*

[79] University's submissions dated 8 October 2025, page 3.
[80] The applicant sought access to '*tracking identifiers and relevant logs linked'* to him as held by the University, not in relation to a specific program or document. In terms of metadata, under section 48(1) of the IP Act, an access application for a document is taken *not* to include an application for metadata about a document *unless* the applicant expressly states that it does. Given the applicant has not specifically requested metadata in relation to Category 1 information, I am satisfied that the applicant's request is not for 'metadata about a document'. However, if I am wrong in this regard, to the extent that the applicant may have sought access to metadata under section 48 of the IP Act in relation to Category 1, I consider access to this would also not be reasonably practicable as it would be in the possession of Microsoft.
[81] University's submission dated 8 October 2025, page 3.
[82] University's submission dated 8 October 2025, page 2 and 3.

> *data host, Snowflake, or interrogated by analytics tool, SCUBA. No relevant context was provided by the applicant to enable [the University] to identify a particular interaction, service, or dataset under its control that would relate to the request.*

52. The University also submits that:[83]

> *…the appropriate entity to contact regarding Microsoft data is Microsoft.…Snowflake is a data host, SCUBA is* [an] *analytics tool - it is not practical for any entity to provide all identifiers sent to a cloud host, or, all data used by an analytics tool without more specific context such as a particular service or application that used these services.*

53. The applicant has submitted that the University's interpretation that it '*does not have any control or influence by its service provider may be a breach in this instance… the University users terms like "cloud-hosted services" that are irrelevant as they do not recuse the University of its service providers of its responsibilities under the* [IP] *Act'.*[84] While consideration of that particular concern falls outside what may be reviewed in this matter, I can conclude that the University has '*purchase*[d] *the right* [to] *use Microsoft services for the duration of the subscription agreement'*[85] and does appear to have access to some information in relation to how the applicant uses Microsoft products.[86] However, having carefully considered all the material before me, I accept the University's submission that being a subscriber of Microsoft does not mean it has '*any ownership, control, or influence over how Microsoft collects data'* within its products or by its service providers.[87]

54. On this basis, I am satisfied that the University, as a subscriber of Microsoft does not have a present legal entitlement under the IP Act to access, produce or control the use or physical possession of '*records transferred to Snowflake Inc and/or SCUBA'.*

55. In these circumstances, I am satisfied that the Category 5 information is not information contained in *'documents of an agency'* within the meaning of section 12 of the RTI Act, and find that there is no right of access to this information under section 40(1)(a) of the IP Act.

DECISION

56. For the reasons set out above, I set aside the reviewable decision[88] and find that:

- there is no right of access to the Category 1 information under section 40(1)(a) of the IP Act because it does not comprise the applicant's personal information and/or because it is not information contained in 'a *document of an agency'*; and

- there is no right of access to the Category 5 information under section 40(1)(a) of the IP Act because it is not information contained in 'a *document of an agency'*.

[83] Architecture Brief, page 12.
[84] Applicant's submissions dated 6 November 2025.
[85] University's submission dated 8 October 2025, page 3.
[86] For example, in its initial decision the University released information to the applicant in relation to two categories of information as it sought access to '*history of non-Microsoft links that I have clicked/accessed in Microsoft Team & Microsoft Outlook'* and '*logs and timestamp of* [his] *online activity in Microsoft teams.*
[87] See for example, the reasoning in *Nine Entertainment Co Pty Ltd and Department of the Premier and Cabinet* [2023] QICmr 8 (28 February 2023) at [22]-[30].
[88] Under section 123(1)(c) of the IP Act.

57. I have made this decision under section 123 of the IP Act as a delegate of the Information Commissioner, under section 139 of the IP Act.

K Zaidiza
Manager, Right to Information

Date: 23 February 2026