Response

Report: ICT Acceptable Use Policy

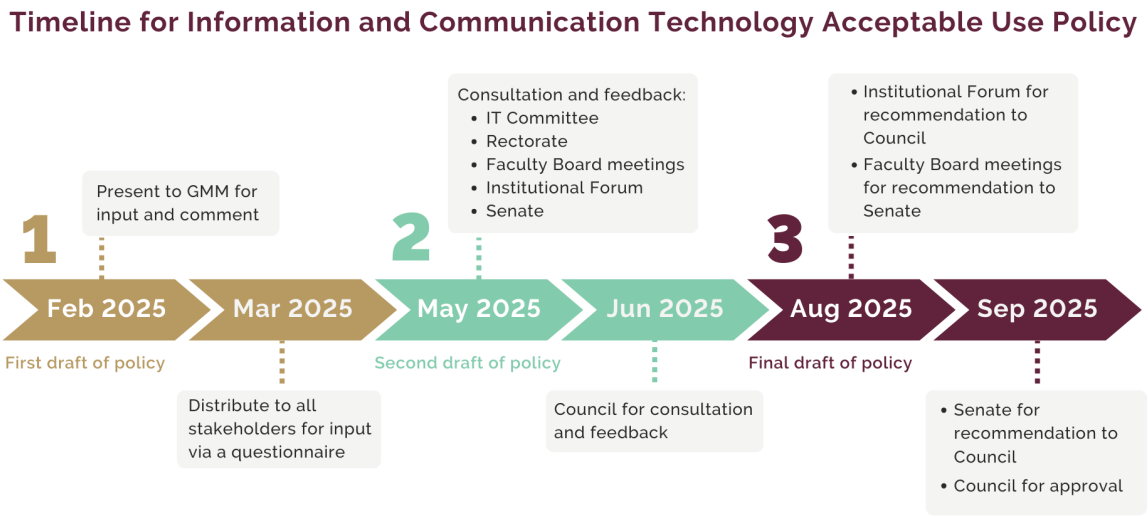
Feedback solicited via Student and Staff Questionnaire from 1-31 March 2025

25 April 2025

Background

The Information Technology Division is in the process of reviewing and updating its **Information and Communication Technology (ICT) Acceptable Use Policy** to guide the acceptable use of SU's information and communication technology resources (ICT resources) to ensure the lawful and secure use in support of the University's activities whilst adhering to SU's values. The Policy addresses the need to protect the University's intellectual property and stakeholder(s)' data while enabling them to do their work aligned with SU's vision.

As part of a transparent and consultative approach, we invite input from stakeholders throughout the revision process. Below is a high-level timeline of the revision process. The IT Blog will be updated regularly with the latest information.



Response rate

First of all, we are very grateful to everyone who took the time to respond. 76 responses were received, of which 30 were from staff members, 28 from undergraduate students and 18 from postgraduate students (see figure 1 below). Two email responses were also received. For these two responses, proposed changes and feedback was indicated on the Word version of the policy.

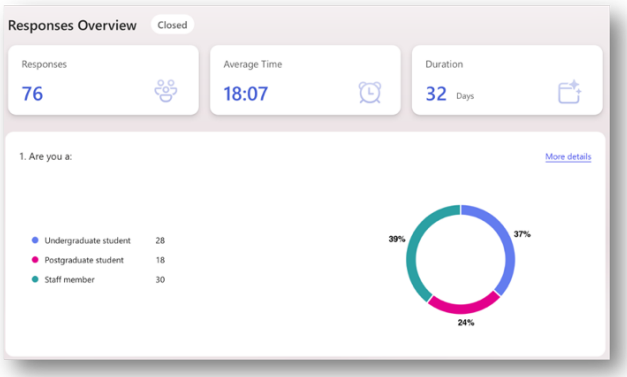


Figure 1: Response overview

Figure 2 below provides the responses disaggregated according to faculty, school and Responsibility Centre (RC). The Faculties of Science (12 responses), Arts and Social Sciences (11 responses) and Engineering (11 responses) provided about half of the responses.

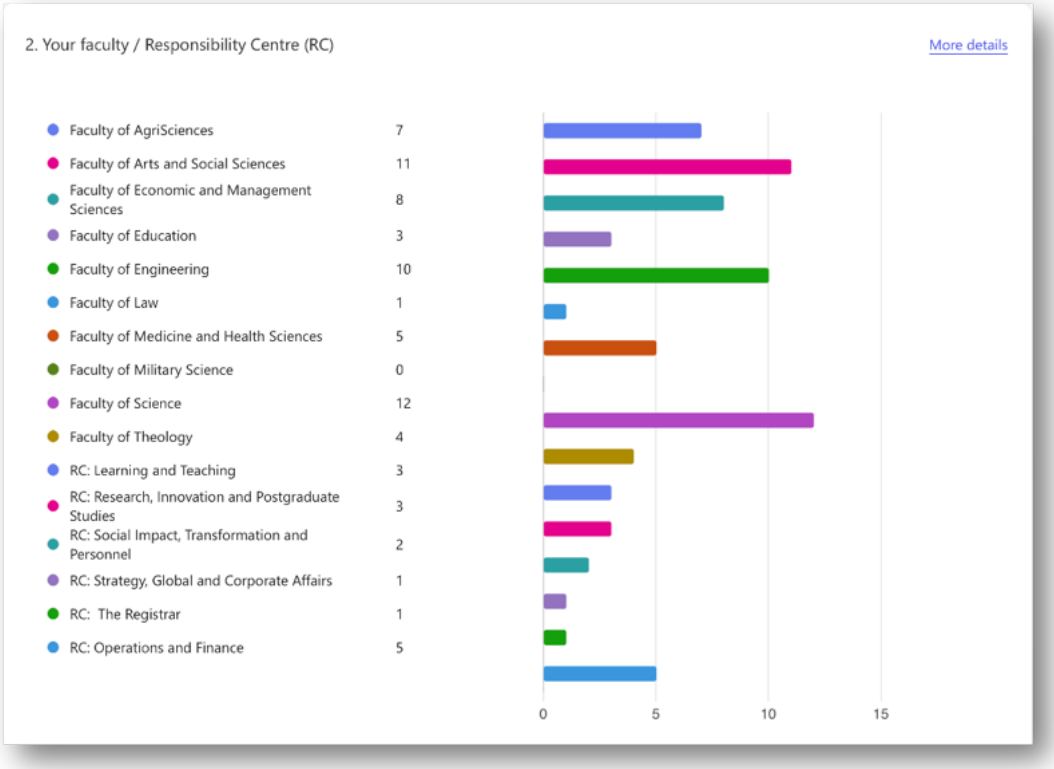


Figure 2: Response overview disaggregated according to faculty, school and RC

The questionnaire was divided into sections consisting of requests for general comments about the full policy as well as requests for feedback on the different sections of the policy. As can be seen in Table 1 below, the most respondents provided general comments on the policy. It should also be noted that some of the comments only indicated "agree", "no", "no comment", "see previous comments". These comments are not included in this response report.

Section	Number of responses
General comments	54
Essence of the policy	31
Application of policy	26
Aims of the policy	29
Policy Principles	22
Policy provision: ICT Infrastructure	31
Policy provision: Software management and usage rights	31
Policy provision: Information and data security	31

Table 1: Responses per question

Main themes emerging from feedback received

When looking at all the feedback received, the following main themes emerge:

1. Clarity regarding **stakeholder groups**, their **accountability**, the **policy's jurisdiction** as well as **roles and responsibilities of various stakeholders.**
2. Clarity regarding the **application of the policy** to **bring-your-own-devices (BYOD) / personal devices** that connect (or not) to the SU network.
3. Further expansion of **definitions and examples** (e.g. **unauthorized device**), move of definitions to the beginning of the document and revision of footnotes.
4. Reference to "**offensive**" content, social media and "**tarnishing**" of University's image (cf 7.1.5, 7.3.2.3, 7.3.3) should be **removed / aligned with the Communication Regulation.**
5. Nuanced view of **software management** in specific research environments / labs to be included.
6. Clarity regarding **"authorised" software**: How it will be vetted / tested by IT? What about research / open source / free software?
7. Distinction between **malicious/intentional** (for which stakeholders should be held accountable) and **unintentional** (for which stakeholders should not be held accountable) activities, e.g. inadvertent spreading of viruses or distribution of phishing emails.
8. **Expansion of clause on AI** to include references to existing documents and what assistance will be provided to stakeholders.
9. More clarity on **Rules, regulations and guidelines** in **Appendix A** (most are still indicated as "in progress").
10. **Editorial** and **style** comments.

These themes will be addressed in the next draft of the policy in consultation with stakeholders. The next section of this report provides all the open feedback received with some initial responses indicated.

Feedback received

The feedback is organized according to the different sections of the policy with preliminary responses indicated. In some instances, detailed discussions are required with stakeholder groups to unpack the responses and the possible reformulation of the relevant clauses of the policy. General comments (editing, positive comments, general comments for clarification and comments that are not related to the policy) are included after the section specific feedback.

Section 1: Essence of the policy

1. Enabling students, staff, alumni, visitors and contingent workers (from here on referred to as stakeholders. Should this not be extended to include researchers and board members?
2. Sections 1, 2 and 4 basically say the same thing.
3. This is important, but privacy is key.

4. Should stakeholders not also include a specific reference to "applicants". Not all applicants become registered students of SU, but applicant's also accesses SU's ICT when they apply to SU.
5. Great initiative. We are protected, that's all that matters in the tech space for us who are less knowledgeable.
6. Very well structured, and honest and fair.
7. The policy should ensure that all measures support both adequate security and process, while not negatively affecting client experience and productivity.
8. The policy should have as a primary aim improving client user experience, based on evidence-based data.
9. Do wholly owned (by SU) but independently operated entities fall into this definition of SU Stakeholder groups?

Response: The Essence (section 1), Introduction (section 2) and Purpose (section 4) do align and could seem repetitive; however, each is important to include. Wholly owned (by SU), but independently operated entities are included in the definition of the SU Stakeholder groups.

Section 3: Application of the policy

1. Please stop using staff cell phones to verify log ins etc. It is my personal device and not a work device.
2. Greater clarity should be made in terms of the differentiation between the devices and systems of persons related to SU and ICT resources, and the policy should be clear on its jurisdiction.

   For example, the policy is unclear as to whether SU will be monitoring, and thus would sanction, actions made on devices used in terms of BYOD when not connected to University systems (such as Eduroam), which would be outside the jurisdiction of the University, and would violate the privacy rights of users. To illustrate this example, would the policy implement tools which would monitor the use of BYOD devices outside of University systems, such that the mere storage of content which is sanctionable under the University's policy on a personal and private device lead to a violation of this policy.
3. 3.2 The BYOD clause/definition should either include IoT devices like Cameras, power monitors etc or IoT devices should be included as separate items as they can be susceptible to security risks and/or carry identities.
4. Understandable that this policy applies to US assets, but certain aspects shouldn't extend to private devices such as cell phones and laptops that are connected over wifi eg additional software other than a multifactor authenticator. Personal devices should be under owner autonomy.
5. I think it does not make clear which/how provisions apply to BYOD settings/personal devices.
6. BYOD must be monitored to avoid infiltration.
7. Not clear how 3.1 differs from 3.2?

8. 3.3 processes is defined too broadly as it encompases pretty much everything that may have nothing to do with ICT (such as the verbal processes I might use to give class).
9. Agreed, although I assume there will be a procedure that helps explain the processes in more detail.
10. At para 3.3: is there a minor typo that must be corrected so that it read "Processes, that include, but are not limited to..."? Also consider adding the word "lawful" processing of personal information in this paragraph (as it would align with the POPIA Act).
11. Does not adequately address user experience and disruption of productivity.
12. All stakeholders who connect to the university network

Response: Section 3.1 refers to the stakeholders and Section 3.2 to the ICT resources these stakeholders access and use.

Efforts will be made to provide further clarification regarding BYOD, SU assets and private devices in the next version of the policy.

The definition of "processes" will be reconsidered.

Section 5: Aims of the policy

1. 5.2 (& 11.5) eduroam should never capitalised:
   https://eduroam.ac.za/faq/capitalisation/
   Perhaps also mention SAFIRE https://safire.ac.za/ which facilitates access to services & resources of other institutions using SU credentials.
2. At para 5.1: should the reference to "the laws associated with the geographical location ..." not rather refer to the "the laws associated with the relevant jurisdiction in which these services are hosted"?
3. At para 5.3: should the reference to "Industry-specific regulations" not refer to "Industry-specific legislation and regulations"? Also, where any specific Act is referenced throughout the policy, the full reference of the Act should be referred to (whether in the text or as a footnote).
4. With reference to clause 5.3, The latest NDoH guidelines were published in 2024. Please refer to the website for more information:
   https://www.health.gov.za/nhrec-home/
5. It should be the 2024 guidelines from the department of health.
6. 5.4 I cannot find a place where the General Code of conduct for the use of Lab facilities fits in. Would that be a regulation or guideline and do we need to rename the Code of conduct in that context. I am including the previous code of conduct that was submitted for approval.
   CODE OF CONDUCT FOR COMPUTER USER AREAS (CUA'S)
   • Cellphones must be on silent at all times
   • No food or beverages including alcohol and chewing gum, is allowed. (Only closed water bottles.)
   • Smoking is prohibited
   • Behaviour should be quiet and orderly at all times. Other users may not be disturbed.
   • Workstations (including computer tables) must be left neat and tidy. No paper or other litter may be left behind. Chairs should be replaced neatly.

• No notices may be placed without prior approval by the CUA manager.
• With the exception of wheelchairs, CUA's are wheel-free zones. No bicycles, roller-skates/blades, scooters will be allowed.
• No pets, with the exception of guide dogs, are allowed.
• Equipment and furniture, including chairs, tables, air-conditioning, etc. may not be damaged or tampered in any way.
• Reasonable requests by the CUA manager and/or his/her representative(s) may not be denied
• No equipment may be set up in, connected to or removed without prior consent from the CUA manager.
• Access may only be gained by the user's OWN student card. The user's student card must be available at all times.

7. Clear aims and elaborated objectives well.

Response: The edits on 5.1-5.3 will be done.

The General Code of Conduct for the use of CUAS will be included in the list of References.

Section 6: Policy principles

1. Information and data, and the technologies used to process information and data, have value. What value - commercial value?
2. Great if these are applied to IT staff members too. Shocking case of abuse of confidential information last year.
3. What exactly the principles are, could be explained more thoroughly.
4. If it furthers the vision of the university, it is good.

Response: Data and information have value in terms of enhancing decision-making, improving student outcomes, optimizing operations, and enabling research.

Section 7.1: ICT Infrastructure

1. Totally agree. This asset of SU should be top of the range but still cost effective and super safe.
2. Should SU not guarantee the stability of the signal/connectivity for the Eduroam network within reason? There are many places across campus, such as Lecture Hall 230 in the A&SS building, where it is often unable to connect.
3. Again - this is a list of things users may not do (all reasonable) but no emphasis at all on support by IT of user experience.
4. What about the physical hardware - Stakeholders should not deliberately harm physical hardware or unplug LAN cables from devices that needs to stay on the LAN.

Section 7.1.1: Connecting any unauthorised device that poses a threat to ICT services, disrupts the business function of SU, reconfigures network equipment that was not approved or deliberately circumvents ICT security measures.

1. It will be useful to define 'unauthorised' device (also 'authorised device'). Also, the process to authorise a device. The use cases we have in mind are hardware gifted to research groups (e.g., servers gifted to CERI) and also research equipment such as the Tecan Fluent used by the BioFoundry (https://www.sun.ac.za/english/faculty/science/biofoundry). Our concern is that 'unauthorised device' might be used as a hard stop that could hamper innovation, if there is not also a clear process for bringing devices into the SU fold.
2. Unauthorised device must be defined. It should also be made clear how devices are to be authorised.
3. 7.1.1 No unauthorised device should be connected (irrespective if it poses a threat etc). How will this be enforced? Not all stakeholders have the necessary knowledge about how to safeguard the ICT infrastructure.
4. 7.1.1 Connecting any unauthorised device that poses a threat to ICT services, disrupts the business function of SU, reconfigures network equipment that was not approved or deliberately circumvents ICT security measures.
   It will be useful to define 'unauthorised' device (also 'authorised device'). Also, the process to authorise a device. The use cases we have in mind are hardware gifted to research groups (e.g., servers gifted to CERI) and also research equipment such as the Tecan Fluent used by the BioFoundry (https://www.sun.ac.za/english/faculty/science/biofoundry). Our concern is that 'unauthorised device' might be used as a hard stop that could hamper innovation, if there is not also a clear process for bringing devices into the SU fold.

Section 7.1.3:

1. Distinction should be made between malicious and inadvertent spreading of viruses.

Section 7.1.4: Interfering with or disrupting the normal operation of technology resources, including intentional or unintentional actions that impact system performance or availability.

1. According to 7.1.4, this policy holds the stakeholder to account, even if they mistakenly interrupt the performance of the system - is this fair given that the individual might not understand how the technology they are utilising works?

Response:

Physical hardware will be considered to be included.

"or unintentional" will be deleted to make the distinction between malicious and inadvertent spreading of viruses.

Examples and a definition of "unauthorised devices" will be included and an indication will also be given as to how it will be enforced.

Sections 7.1.5: Accessing, storing, or distributing content that is offensive, discriminatory, or violates institutional standards.

Section 7.3.2.3: Creating, downloading, storing or transmitting unlawful material, or material that is indecent, offensive, threatening, or discriminatory.

Section 7.3.3: Engage responsibly in social media without tarnishing the institution's reputation. Any offensive material will be removed from institutional systems. The communication regulation lays the foundation for the range of SU communication-related documents.

1. Furthermore, and I write this without having again read the guidelines attached to this policy, but it must be noted that including within a policy a provision sanctioning "content that is offensive" without making clear and concise definitions thereof is likely to lead to outcomes which violate the rights of students, and also seems to be a slippery of over-regulation.
2. In response to point 7.1.5: *Accessing, storing, or distributing content that is offensive, discriminatory, or violates institutional standards.*

   How will 'offensive content' be identified or policed? What are the definitions in place to do so? What if a researcher is working with material that might be deemed 'offensive' by someone else, and it actually forms part of their research project? This term is used too loosely and comes across as draconian. It also assumes a degree of moral generalism that does not sit well in an institution that supposedly supports academic freedom. Also see point 7.3.2.3 on creating, downloading, storing or transmitting material that is "indecent" or "offensive".
3. Offensive and discriminatory needs to be defined. What does institutional standards refer to? What are the standards?
4. The use of the term "offensive" is not wise. Something that is offensive for one person might not be offensive for another and to prescribing what is or is not offensive is not a good idea in a diverse environment. Some people might find the word "shit" offensive, while I do not, but on the other hand I find the casual use of the word "God" offensive. The same applies to political and gender views. Naturally there are things that are unlawful (like racism, hate speech and child pornography etc.) that should be prohibited.
5. We should be allowed to say what we like about a public institution that we are, as staff, in measure entrusted with critiquing. There is a fine line between "tarnishing" the university's reputation and doing our job of holding it accountable.
6. In response to point 7.3.3: What if a researcher is engaging critically with university actions or protocol where these are unethical or where such engagement is called for? Is the university banning all critical engagement with its social media content or prohibiting all lecturers and staff from offering critical opinions on such platforms? This feels like outright censorship. nIt also limits my freedom of speech by requiring that I not use social media to tarnish the institution's reputation - even if such a post were true.nThe policy infringes on certain key rights of lecturers and students (on the points mentioned before) and needs a more nuanced description around its blanket use of 'offensive'.
7. With regard to 7.1.5, greater clarity should be provided, and a broad, reasonable approach should be taken with such provisions.
8. Regarding 7.1.5: being offensive is subjective - if it is to be included this should be more carefully described.

9. Regarding 7.1.5: almost any data is discriminatory in some sense - even maintaining data to adhere to employment equity requirements can be viewed as discriminatory. I would remove.
10. Does 7.1.5 prohibit dealing with such content even for research purposes? There are legitimate reasons for having to store and otherwise deal with legal but offensive etc. content from, e.g., extremist movements, for the purposes of research, particularly in the Arts and Social Sciences faculty. Further, what is considered "offensive" content is not an objective measure: different parts of society would consider different things offensive, and some things are offensive not in themselves but only because of their method of distribution and audience (for example, pornography shown in a lecture hall with unexpecting students is offensive, but the same thing watched on a personal device in private in a university residence using the university internet connection is presumably allowed).

Response: Consideration will be given to completely removing 7.1.5, 7.3.2.3 and 7.3.3 because they are already covered in the Communication regulation.

An alternative is to revise them to include the principles of the Communication regulation: *All statements related to SU and the University community, in any capacity and on any platform, must be aligned with Code 2040: SU's Integrated Ethics Code and the institutional values of excellence, respect, equity, compassion and accountability.* See principles of the Communication regulation (section 3).

Section 7.1.6: Sending or responding to unsolicited emails, spam, or phishing attempts

1. In response to point 7.1.6: What if someone unknowingly responds to an email that is spam or a phishing attempt? Some of these are so well written that detection is difficult. Why should a member of staff, or anyone, for that matter, be penalised if this is the case?
2. As with 7.1.3 distinction must be made between malicious and inadvertent actions. Suggest adding responsibilities for users that refers to due diligence of preventing inadvertent spreading of viruses or distribution of phishing emails.
3. Regarding 7.1.6: there are 18 documents listed in Appendix A, which most end-users are likely to find highly technical. I don't think it is reasonable or realistic to expect stakeholders to be familiar with these. It is also problematic for us to accept this policy without knowing the proposed content of these documents - only 5 of them seem to have been completed - or the approval and consultation process that will be involved when formulating them. 7.1.6 seems to prohibit responding to any emails that were not explicitly solicited (for example, I do not "solicit" emails about workshops or seminars around campus, but presumably it would be acceptable for me to reply to them). "Unsolicited" needs to be defined or replaced with a clearer word (perhaps say: "malicious emails, including phishing"). Spam is also not a clear word choice and can be used for any email that is unwanted. I also don't think that replying to junk mail should be itself against policy, since it can often be benign (a student spamming their class with advertisements for second hand textbooks counts as spam, but surely it should not be against policy to reply to them?). It should be made explicit that it is only *malicious* emails that should not be replied to. But then again, it seems that this is here to punish users who fall for phishing or scams. If a user makes a mistake as to whether an email is malicious, should they be in contravention of policy? Some phishing emails, especially spear-phishing / targeted attacks, can be very

sophisticated, to the point where even the most wary user might fall for it — is it fair to say that such a reasonable user is contravening policy? Similarly, in 7.1.3, I think it would be better to specify that "deliberately or knowingly introducing". If your goal is prevention or minimisation of cyber-threats and maintaining proper service, then it should be made clear that there is a difference between a malicious threat-actor and an unwitting user, and they should be treated differently. (If you kick out everyone who might let in a threat, you will end up with a network of zero users.)

Response: This section will be revised to make a distinction between malicious and inadvertent actions.

Consideration will also be given to a reasonable list of guidelines and one-pager infographics will be considered to summarise the pertinent aspects of the guidelines / rules / regulations.

Section 7.2: Software management and usage rights

1. It is not always a good idea to update to the newest version since these are not always stable. In my Lab I have 2 linux servers that are linked to instruments, but the software used to drive the instruments run on the last stable Linux distribution. Updating Linux or even installing patches before it has been tested by the instrument manufacturer might cause issues in using the system. (7.2.2)
2. We have several Windows machines that do data collection. There machines are not on the university network since we cannot run antivirus software in these machines. If a virus scan starts while data is collected, not all data will be collected. The policy should make allowance for issues like this. (7.2.4)
3. Software management involves the acquisition, installation and maintenance of standard software applications installed on SU assets, institutional software systems, as well as software used within the faculties for academic programs. Is specialised research software included in this scope?
4. Introductory paragraph seems to exclude software used by PASS environments that aren't deemed institutional software.
   Software and institutional software must be defined.
   Responsibilities of users and ICT must be included as it relates to software purchasing, installation, and maintenance. For example, some software is updated by IT, while others (such as those used only by a specific division) may be updated by the division themselves
5. Greater clarity should be made in terms of the differentiation between the devices and systems of persons related to SU and ICT resources, and the policy should be clear on its jurisdiction.
   For example, the policy is unclear as to whether SU will be monitoring, and thus would sanction, actions made on devices used in terms of BYOD when not connected to University systems (such as Eduroam), which would be outside the jurisdiction of the University, and would violate the privacy rights of users. To illustrate this example, would the policy implement tools which would monitor the use of BYOD devices outside of University systems, such that the mere storage of content which is sanctionable under the University's policy on a personal and private device lead to a violation of this policy.aIt is not clear how this section is expected to interact with the management of personal devices used with BYOD, where IT presumably does not have control over what software

is installed or the status of virus protection and updates.dWould staff have the option to choose software that suits their purposes? I.e. using Zoom for online classes instead of MS Teams?

6. Presumably, this section is only applicable to devices owned or operated by SU. However, "software used within the faculties for academic programs" seems to include software on *any* devices, including personal devices.
7. Is specialised research software included in this scope?

Section 7.2.1

7.2.1: "fraudulent actions" is extremely ambiguous, to the point of not meaning anything at all.

Section 7.2.2: IT terminology

1. With reference to 7.2.2, consider how a stakeholder who has no IT background would know what hotfixes, patches and other IT terminology is. Whilst you have defined it in this policy, how would they understand all of it in reality?
2. 7.2.2 The responsible party for patch management must be indicated.

Section 7.2.3: Use only software that the institution has licensed, either through a campus agreement, subscription, perpetual licenses, or a license model according to the software usage rights of the software/application. Installing unauthorised software is prohibited.

1. In 7.2.3 the policy says we are not allowed to install any software whatsoever on SU supplied devices that IT has not specifically tested and vetted. This is incredibly restrictive. IT cannot test every single program that someone might want to install on their computer. Staff need to be able to make their own judgements about what software they need to their jobs.
2. I think the policy overreaches. It includes that I may not install "unapproved" software on any devices linked to the SU network. This now includes my cell phone. so now I must get permission to install "angry birds" on my phone.
3. The document needs to make clear provision for the use of open-source software and software provided without licences.
4. In science a lot of software used for data analysis are open source tools. These tools come and go with alarming speed and there are an enormous number of tools. Very often a tool is tried for a specific analysis and then discarded because it does not work, or because it was only used for one analysis and is not needed again. How will these tools be tested.
5. Is this saying all software that is not institutionally licensed will be considered unauthorised? Does 'institutionally licensed' mean SU IT holds the license? If 'yes', this will most likely exclude specialised research software and hamper SU's research vision. What process must be followed to get authorisation to use software that is not institutionally licensed? What if a research collaborator holds the license?
6. 7.2.3 A description must be added to explain how software is to be authorised. Is there a process for this? Not all software is purchased or licensed by IT. "Copying or sharing of authorised software is prohibited" should be moved to 7.2.1.
7. Under the definitions, unauthorized software is referred to software that hasn't been tested and vetted by IT - so therefore any apps or software used by

departments and faculties that isn't standard software, is considered unauthorized? How does IT intend to test and vet all software? oIn 7.2.3 the policy says we are not allowed to install any software whatsoever on SU supplied devices that IT has not specifically tested and vetted. This is incredibly restrictive. IT cannot test every single program that someone might want to install on their computer. Staff need to be able to make their own judgements about what software they need to their jobs.

8. Regarding 7.2.3 and 7.2.4: Please clarify the status of free/open-source operating systems and software in these clauses.
9. I find the point 7.2.3 rather limiting. There are some ad-hoc software which one might need urgently while working (it could even be that you want to test the software that you are building). I do not know what is a better way to reformulate this, but "Installing unauthorised software is prohibited." is, I think, unreasonable.
10. 7.2.3 is too broad. there are many examples of software that researchers would need which are not yet licensed by the university. Should you enact this point, you will be inundated with requests for 'permission'.
11. 7.2.3 Use only software that the institution has licensed, either through a campus agreement, subscription, perpetual licenses, or a license model according to the software usage rights of the software/application. Installing unauthorised software is prohibited.
    Is this saying all software that is not institutionally licensed will be considered unauthorised? Does 'institutionally licensed' mean SU IT holds the license? If 'yes', this will most likely exclude specialised research software and hamper SU's research vision. What process must be followed to get authorisation to use software that is not institutionally licensed? What if a research collaborator holds the license?
12. 7.2.3 - What about freeware, open source software that is needed to do your work? Would all such software have to be authorized? and how?

    Operations often require specialised software beyond SU's standard list. The policy restricts unauthorised software installation but does not specify an approval process for affiliated entities requiring non-standard software for operational needs. Can we propose a formal request mechanism for affiliated entities to install and manage software beyond SU's standard list, particularly where necessary for business functions such as marketing, design, and external engagement.

Section 7.2.4

1. 7.2.4 Who is responsible for installing antivirus software? This paragraph also doesn't make provision for antivirus software on personal devices. What is the requirement in terms of antivirus software for personal devices?

Section 7.2.5

1. 7.2.5 the content of the 'E-mail and communication regulation' will be important
2. Regarding 7.2.5: The email and communication regulation in Appendix A is not yet available, so it is hard to comment on this.
3. 7.2.5 feels out of place. While email is managed through software, including email communication here isn't sensible.

Response: These sections will be revised to present a more nuanced, context specific approach to "authorised software", the process of vetting software as well as research-specific / open-source software and freeware.

Section 7.3: Information and Data Security

1. Very important. Also the security/password access to Apple devices.
2. This section also requires roles and responsibilities. The introductory paragraphs are too vague.
3. Does this imply that we can extract student information from SUNStudent and use it to do our work? Without questions asked.

Section 7.3.1

1. Stakeholders are not allowed to share their CREDENTIALS (e.g. passwords, digital security keys, access cards etc)
   Note that passwords are not the only credentials and could be replaced in its entirety in future.
2. 7.3.1 Safeguard SU credentials should prohibit the sharing of credentials (usernames and passwords) and specifically state that access by another party can only be obtained in special cases like for business continuity and/or legal action and that such approval must be given by the legal department and The Chief Director IT. This is a very important and current issue as students share their identities and the third-party involved claims its legal use as he/she received the identity from the owner in good faith.

Section 7.3.2

1. 7.3.2.2: Where is the line between information belonging to individuals and information that individuals have placed in the public domain?
2. 7.3.2.3 Definitions needed for unlawful material, indecent material, offensive material, threatening material, discriminatory material.

Response: See comments above regarding "indecent", "offensive" and "discriminatory". This terminology will be deleted / the complete clauses will be deleted.

Section 7.3.3

1. 7.3.3 It is unclear to me why social media is included here. Reputation management is not an ICT function, as it relates to social media. It is also not possible, on social media, to remove offensive material from institutional systems.

Response: As mentioned above, it will be considered to exclude the social media clause.

Section 7.3.4

1. What is meant with "responsibly and ethically"? I think you need to explain this more.
2. 7.3.4 This is a very broad and vague statement.

3. With reference to 7.3.4, will SU provide guidelines and workshops to outline and demonstrate how to use AI responsibly? This would be helpful and also ethical since the policy holds stakeholders accountable.
4. Regarding the use of AI - it would be beneficial to all students and faculty if an official inter-departmental awareness and use policy for AI existed, as some departments are better-equipped than others to prevent the unethical use of AI and to ensure the accuracy of assessments when it is suspected that a student may be using AI unethically (i.e. an excess of faith in the accuracy of Turnitin and other so-called "detection" algorithms. I would be interested in having a table discussion of the subject if that were possible. Thank you.
5. 7.3.4 Use of AI responsible and ethically should include an understanding of the terms and conditions related to using those tools. It is not enough to say responsible and ethically without indicating what is responsible or ethical use. I think it covers most of what is expected. Surprisingly little about AI, though. There is one sentence reference, I think. Difficult to see AI use as either licenses or software as it is so ubiquitous. Maybe a bit more needed.
6. Refer to the AI Position Statement. When we wrote the RDM Regulation our academic stakeholders asked us to link to related documents wherever relevant to facilitate easy access to those documents.
7. With reference to clause 7.3.4 - perhaps include a link/footnote to the SU position statement on ethical use of AI in research and T&L
8. 7.3.4. Perhaps refer the reader to the position statement in Appendix B (in alignment with earlier instances in the document)
9. 7.3.4 'responsible' should read 'responsibly'. Further, there is no clear guidance as to what 'responsibly and ethically' means or how to ensure this, other than as contained in the institutional position statement on 'ethical use of AI...'.
10. 7.3.4: *responsibly. This is also very vague, and what it means to use AI responsibly and ethically is under contention worldwide at the moment. But the other rules in this document should already suffice to ensure AI is used responsibly, for example, it is already said elsewhere that piracy etc. is against the policy. I assume that a separate AI policy is in the pipeline. Other AI ethics concerns (such as plagiarism) are outside the scope of the document. Therefore, what does 7.3.4 add that is not already said? If it does add something that is not already said, then that should be made explicit.
11. Consider writing out AI in full, i.e. artificial intelligence because AI is also a short term for artificial insemination.
12. In this day of AI, it is important to protect people's privacy, and it seems as though this is a key facet of this reading

Response: Responsible will be changed to responsibly and AI will be written out in full.

Reference will be made to existing guidelines, e.g. the Position Statement on the Responsible use of AI in Research and Teaching-Learning-Assessment.

Consideration will also be given to further expanding this section.

Section 8.1: Roles

1. The policy needs a section on roles and responsibilities that specifically speaks to the various policy provisions.

Section 8.3: Implementation

1. The Information and Communication Technology Acceptable Use Policy regulates the use of ICT resources at SU. Within this context, the IT division develops and continually updates its guidelines, rules and *regulation*. Regulation*s*?

Response: This section will be updated.

Section 8.4: Monitoring and reporting

1. The policy also includes provision for the university to spy on my activities in a completely opaque manner (whether on my phone or on my work laptop).

Response: The policy states under which conditions SU can monitor devices.

Section 9: Non-compliance and Infringement

1. Finally, how will parents, donors, and other external SU stakeholders be held accountable to this policy?

Section 11: Definitions

1. Define "community" in the context of this policy, or your definition is so vague that it serves no purpose.
2. 11.14: “Unauthorised software”: Is there a list that is kept updated that we can access to see which software has been tested and vetted by IT?
3. As its not included in this questionnaire in 11.2 The BYOD definition should either include IoT devices like Cameras, power monitors etc or IoT devices should be included as separate items as they can be susceptible to security risks and/or carry identities.
4. It will be useful to move Definitions to the start of the document so that people can familiarise themselves with the terms before they read the stipulations of the regulation.
5. The use of footnotes to define certain terms seems unnecessary given the definitions in section 11.
6. Stakeholders must be included in definitions, as defined in policy essence. The definition of SU stakeholder groups is different to how it is defined under policy essence.

Response: Definitions (community, unauthorised software, BYOD) will be reconsidered and moved to start of the document. Footnotes will be reconsidered once definitions are moved.

Section 12: Appendix A: Supporting documents

1. There is reference to Annexure A throughout the document, but it does not align with the content in Annexure A.
2. Links to (at least the accepted) policies/regulations in the appendices would be useful.
3. It is difficult to make judgments on various things without details on the many regulation documents that are "in process" in Appendix A.

Response: It is unclear what the reference to "Annexure A" is. Links will be provided where possible, but we acknowledge that there are many regulation documents "in process". However, the policy provides the overarching framework for these rules, regulations and guidelines.

Section 13: Appendix B: Related documents

1. Under related documents, there is reference to the Electronic Communication Policy. This policy was approved in 2003!!!
2. The NHREC Guidelines need to be updated to refer to the 2024 guidelines, not 2015.

Response: The NHREC Guidelines will be updated. It is confirmed that the ECP dates from 2003.

General comments / further clarification required

1. There is nothing in there addressing client experience or low friction user experience or striking a reasonable balance between security and productivity. The current level of multiple sign-ins across devices with short timeouts and no ability to stay signed in has a profound impact on daily productivity of all staff and is not the norm in large institutions. Further to this, eduroam at other locations just works, but is generally flaky and unreliable across the actual SU campus.
2. TLDR version - the strategy is entirely IT technical and says nothing about user experience and impact.
3. Will this policy be like an NDA for staff to be able to use student data to do their work?
4. We appreciate the importance of maintaining a secure and compliant ICT environment and fully support SU's efforts in this regard. However, we believe that the policy should explicitly account for affiliated and wholly owned entities, which operate independently while using SU resources. We kindly request that the policy supports both SU's security objectives and the affiliated and wholly owned entities' operational needs.
5. Support optimal client/user experience and productivity by minimising the impact of the above on daily work experience. This may include reducing sign-ins, supporting password autofills from approved apps, ensuring connectivity to eduroam is improved,
6. The strategy in its current form completely ignores the actual clients.

7. Ditto - a list of rules that may not be done, nothing encouraging improved systems or experience by client which will actually support the above.

Response: It should be noted that this is a policy and not a strategy. IT however remains committed to optimal client/user support. Further discussions to clarify SLAs and the cost of services to wholly owned entities are underway.

Terminology, Style, editing

1. Draft is inconsistent wrt the SU style guide (punctuation, grammar, capitalisation, etc). Inconsistent use of the institution vs the University; Oxford comma (not applicable in SU language style and used only if last element in series includes [and])>.
    a. Style note: lower case lettering for common noun occurrences of word, policy / See discrepancy in header (which is correctly written in Sentence case style, Essence of the policy vs text para 1 line 01 where it's written as This Policy. Suggest edit latter to: policy across paper.oSection 3: University <EDIT initial cap / see SU style guide p58> [BYOD]) <line 05: suggest use square brackets as already within round parentheses>oSection 5: Style corrections:
    standards and best practices, and <line 01, 02>
    Third-party <line 06: 5.2 - format T to bold>
    SU Policies and regulation <last line - says available but text not linked?>
    b. Section 6: Style guide edits:
    Policy principles <header: all other sections are Sentence case style, as per SU guide. Suggest this is too><AND suggest delete the colon - no other headers include colon and not relevant here>
    c. Section 7.1 Style guide edits:
    ICT infrastructure <header: all other sections are Sentence case style, as per SU guide. Suggest this is too>
    sustainable and reliable <line 02: delete Oxford comma>
    account or data <7.1.2 delete Oxford comma>
    viruses or any <7.1.3 delete Oxford comma>
    storing or distributing <7.1.5 delete Oxford comma>
    discriminatory or violates <7.1.5 delete Oxford comma>
    spam or phishing <7.1.6 delete Oxford comma>
    d. Section 7.2: SU style guide edits:
    material and fraudulent <7.2.1 line 2: delete Oxford comma>
    systems and applications <7.2.2 line 03: delete Oxford comma>
    tested and applied <7.2.2 last line: delete Oxford comma>
    viruses and other security <7.2.4 line 2: delete Oxford comma>
    scans and taking <7.2.4 second last line: delete Oxford comma>
    e. SU style guide edits:
    the University's <line 01: suggest replace institution with university>
    Information and data security <header: lower case d, s for Sentence case style for titles/headers>
    damage or loss <line 01: delete Oxford comma>
    accurate and <line 06: delete Oxford comma>
    studies or various <line 09: delete Oxford comma>
    SU <para 4 line 04: replace Stellenbosch University with acronym /

consistency across policy text reference>
modify or disclose <7.3.2.2: delete Oxford comma>
threatening or discriminatory <7.3.2.3 line 02: delete Oxford comma. Note: there is no Oxford comma in line 01 [after word: storing] which is correct according to style guide>
<7.3.2.1; 7.3.2.2 suggest replace comma with semi-colon at end of point text>sThe word "should" is used throughout to refer to the actions of the stakeholders. Should it not be "must"? Otherwise it is not enforceable

f. There is inconsistent use of SU, University and university (where the latter two terms are not defined currently). Consistent use of SU seems preferable.

2. Numbering edit needed, from Item 11:13 (repeated twice, and the following numbers to be adjusted also)
3. […] the policy aims to give effect to: 5.1 Foreign and domestic law (including the services) that are hosted or supplied by international partnerships." Should this read "the policy aims to give effect to: 5.1 Foreign and domestic law (including the services that are hosted or supplied by international partnerships) (p.3)"? If we ignore the bracketed phrase it currently reads "the policy aims to give effect to: 5.1 Foreign and domestic law … that are hosted or supplied by international partnerships (p.3)"

   5.1 "(including the services)" should not be in parentheses.
4. 7.3.2 'procession' should read 'processing'.
5. At Footnote 4 (relating to "patches" at para 7.2.2) on pg 4: "operating System" should be capitalised as "Operating System".

Response: The final draft of the policy will be professionally edited and translated but this feedback is very valuable for the current draft.

Positive comments

1. No, the policy is comprehensive without being restrictive. Well written.
2. I think it is well written and clear.
3. None. It seems like a thoroughly thought-through document.
4. No comment in the questionnaire means I agree that the section meets requirements from my perspective. With the exception of a few minor questions/opinions on specific items it covers the scope of Acceptable Use comprehensively.
5. The policy is clear.
6. Policy is relevant and concise.

Unrelated to the policy or unclear

Wifi

1. I am unable to use Wi Fi as I have to do readings

2. I need to get access to school Wi Fi so that I can be able to do my school work, readings and to get my student emails as I fail to do since I cannot connect my Wi Fi does not connect
3. EDUROAM

SUNLearn

1. Please put something on stemlearn where I can see all assignments that are due across courses in order by date

Unclear

1. Cannot find it on the system
2. This question is very unclear, especially that I cannot see what questions come after this.

Network

1. The network is slow for me

Conclusion

Again, a big word of thanks to everyone who provided feedback. This feedback helps us to improve the draft policy. The next steps include consultation with the faculty boards, the General Managers Meeting (GMM), the Institutional Forum (IF) and Senate. This response report will be amended with additional feedback during the consultation process. The final draft of the policy will again serve at the IT Committee, the GMM, the IF, the Faculty boards and finally Senate for recommendation for approval by Council.