ACODE 89
BUSINESS AND NETWORKING MEETING Minutes

Friday 14th July 2023

10.00 am AEST

https://aarnet.zoom.us/j/86877080020?pwd=VTBJZ2hnNnhXSzh5SmxNVlhaQUdLUT09
Password: 393923

TIME ZONES

8.00 am Western Australia
9.30 am Northern Territory
9.00 QLD
9.30 am South Australia
10.00 NSW, VIC, ACT, TAS,
11.00 pm Fiji
12.00 pm New Zealand

* PART A: PRELIMINARY BUSINESS

1.0 Acknowledgement of country and land (AU and NZ)

2.0 Welcome from President and President's Report – Michael Sankey

ACODE 89 went well, we have some great insights in the Padlets, and some great take home snippets from both Thomas King (Microsoft) and Nikki Peever(CAUDIT).

Sincere thanks to Sheila McCarthy and Simone Poulsen for pulling this together.

BM9 is still plugging along, with the working party meeting twice a week. The discussion is very fruitful and we hope that the wording we now have is going to be decisive for all.

I encourage you all to participate in the linked in and Twitter feeds relating to ACODE.

Theta was a great conference and thanks to Karen and Ratna who were the ACODE reps on committees.

The LTLI is shaping up well with a meeting of the Faculty next week. We have surpassed the attendees that we thought we would get and have 45 registrations which a fantastic response.

We have sponsorships from Pebblepad, FeedbackFruits, Echo 360 and Anthology(Blackboard) and still waiting to hear from one more.

Elections for the Exec will take place in November and we will be looking for a new President in 2024 as my 2 terms are up.

Please consider nominating for the Exec, we have a very good reputation in the Sector and the Exec fly the flag for ACODE.

This will also be the final year for Karen who will retire after 12 years with ACODE.

3.0 Attendance and apologies

Attendees:

Karen Halley	ACODE Secretariat
Michael Sankey	ACODE President
Lynnae Venaruzzo	Western Sydney University
Patrick Stoddart	University of Melbourne
Ratna Selvaratnam	Edith Cowan University
Travis Cox	University of Adelaide
Kate Ames	Central Queensland University
Gordon Cunningham	Curtin University
Steve Leichtweis	University of Auckland
Liane Joubert	Australian National University
Shane Nuessler	University of Canberra
Sheila McCarthy	Griffith University
Jenny Edwards	Australian National University
Bill Searle	Charles Darwin University
Nadine Adams	Central Queensland University

APOLOGIES:

Julie Brunner	Curtin University

4.0 Minutes of previous meeting

Moved –Gordon Cunningham………. Seconded – Patrick Stoddart

Identification of unstarred items for discussion – and proposal of Hot Topics

5.0 Adoption of items not starred for discussion

MOTION: That all items on the agenda not starred for discussion be noted and where recommendations have been made, that these be adopted as resolutions of the ACODE Business and Networking Meeting. - Nil

6.0 Matters arising from previous Business & Networking Meeting - Nil

7.0 ACODE Executive Report – Online

8.0 *** PART B: ITEMS FOR DISCUSSION***

9.0 Report from A89 Workshop Notes – Sheila/Lynnae

Executive Summary

"Data is the new oil...don't let it slip!"

The ACODE 89 workshop was held on Thursday 13 July 2023 in partnership with CAUDIT on the topic of empowering educations: cyber acuity with security for 21st Century Classrooms. Just over 40 attendees represented a broad range of roles from across the L&T sector, including teaching academic staff, educational designers and technologists, directors of learning and teaching, and learning support specialist staff.

Key points shared during the workshop

- Cybersecurity is a shared responsibility across organisational levels
- Individuals can take simple steps to protect themselves and the data they have access to. Institutions have a role to play to develop the digital literacy and fluency of staff and students.
- Polite cautiousness or being professionally paranoid about unexpected emails, phone calls and texts are useful techniques to minimise cyber threats and risks.
- Acuity is a core life skill that helps produce smarter graduates and employees.

Keynote

Thomas King, Higher Education Industry Executive, Microsoft ANZ

"We need to get it right every day. Hackers only need to get it right once!"

Cyber security can seem endlessly complex with many moving parts such as devices we use to access resources and connect with each other, and devices that power our campus infrastructure. Many of our teaching and learning technologies are delivered software as a service (SaaS) yet require integration across systems. Further complexity occurs in hybrid infrastructures, identity and access management across many different technologies. Consider these components like moving puzzle pieces with thousands of threats looking for vulnerabilities.

While cyber professions have frameworks and technologies to manage the complexity of secure university, individuals have a significant role to play. Thomas shared four key things we can do to protect and manage our data. These recommendations are:

1. You and your digital identity are valuable. **Multi-factor authentication (MFA) and strong passwords** are protective shields in your cyber protection efforts.

2. Make sure the **devices you use are secure** and keep your software up to date, automatically as much as possible.

3. Ensure you have **least privilege rights**, or in other words only access the data you need to do your job.

4. Think about your contribution to **reduction of software sprawl** at your institution by proof of concepts, pilots of new technologies, and the applications you must use to do your job to ensure competency and security/infrastructure approval status. Become experts in the applications you use as there is a direct correlation between identifying phishing attempts and competency in the applications.

Cybersecurity 101: Defending our Digital Environments and Empowering Educators

Nikki Peever, Director Cybersecurity (CAUDIT)
Jakob Sellmann, Cybersecurity Officer (CAUDIT)

"Criminals collaborate...we need to copy the criminals to improve our defences together"

Understanding the behaviours of cybercriminals is key to defending our digital environments and empowering educators. Common techniques used by cybercriminals include deceptive calls, texts and emails that mimic something or someone you know and coercing you to act urgently. To combat these techniques **be politely cautious,** pause and assess what the action request is and whether it is a legitimate request. Cybercriminals seek to create a situation of fear, curiosity, urgency, and intimidation (social engineering), and it is okay to be professionally paranoid and politely cautious about every email, text and call you receive.

Universities may be seen as a soft-targets due to the complexity of systems in place and the valuable data they collect, store and use. For instance, information on students (past, present, potential), staff (past, present), research participants and research data, financial data, and IP. However, not all threats are externally generated and may be internal through accidental or malicious actions. Defending yourself from cyberthreats is simpler than you think, and four strategies were shared.

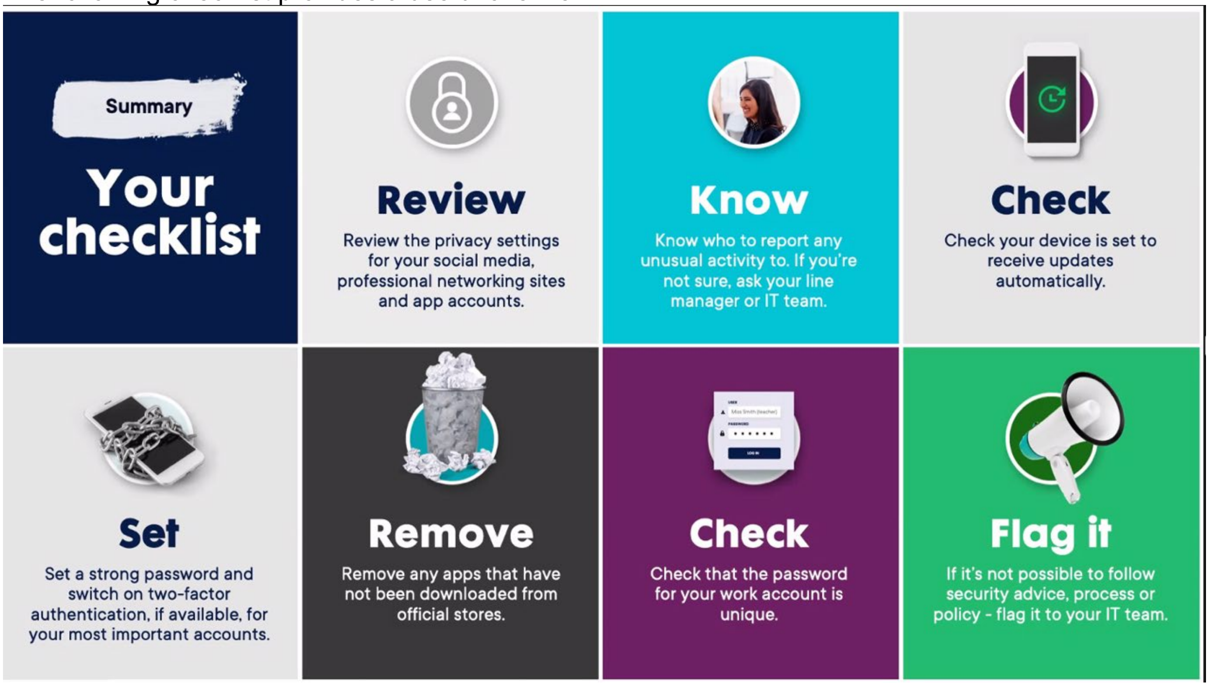
1. Defend yourself against phishing attempts – be politely cautious.

2. Use strong passwords with multi-factor authentication. The longer the password the stronger it becomes, such as three random words with special characters added in. Store passwords securely and use a separate password for work accounts.

3. Secure your devices by applying software updates as soon as they are released and physically protect your device.

4. If in doubt, call it out by reporting any suspicious activity as soon as possible, and don't be afraid to challenge the level of security in place at your work instead of taking workarounds.

The following checklist provides a useful overview:



Summary

Your checklist

Review

Review the privacy settings for your social media, professional networking sites and app accounts.

Know

Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check

Check your device is set to receive updates automatically.

Set

Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove

Remove any apps that have not been downloaded from official stores.

Check

Check that the password for your work account is unique.

Flag it

If it's not possible to follow security advice, process or policy - flag it to your IT team.

Sector Roundtable – What's happening around Cybersecurity at your Organisation

Training: cyber essentials training modules and responsible data use resources to help staff and students create strong passwords and manage their information securely. Training modules are contextually situated to help make the activities relevant to different roles. Mandatory training is common however, voluntary take-up of resources or smaller just-in time, bite-sized, modules tend to be low.

Engagement: Some organisations are using mechanisms such as Communities of Practice, working parties and 'cyber champions' to help 'spread' acuity and identify collaboration opportunities across areas outside of traditional IT departments.

Software and system: Examples shared included emails flagged as [External] with cautionary notes applied, in-context reporting and blocked emails requiring vetoing to view. Some institutions send cyber-security equivalent of a fire drill with emails designed to test system vulnerabilities and user-behaviour with phishing emails. Multi-factor authentication for staff is a common approach broadly applied across university systems; however, MFA was not widely applied for students' access to all university systems or infrastructure. Assessing and managing tech-debt is an emerging approach as institutions manage the software and system sprawl across the enterprise.

Governance: appointments of Chief Information Security Officers, or Chief Security Officers are providing executive level stewardship across university systems and data.

Strategies for promoting cyber acuity in students within the 21st Century Classroom

Cybersecurity is 'everyone's business' and is more than phishing attacks on email. There are associated rules and policies supporting cybersecurity approaches, however promoting acuity leads to smarter graduates and employees.

For students, cybersecurity is a core life skill as students develop their abilities to manage and protect their personal cybersecurity, personal privacy, and identity. Further dimensions are layered on top of these skills in discipline practices such as workplace security and client confidentiality. Strategies shared include the following:

In class:

- Including cybersecurity practices and techniques in activities like case studies, simulations, guest speakers, and interactive workshops.
- Academics leading the way by showing their cybersecurity practices such as not using USBs or leaving open laptops in computer labs.
- Signage in teaching spaces about laws, policy and advice around recordings and broadcasting video during hybrid classes.
- Promoting cybersecurity practices at orientation activities as students start their university journey.

In curriculum:

- Learning materials and activities that promote the handling and maintaining confidentially of data relevant to the discipline and profession.
- Develop students' digital literacy and fluency in discovering, evaluating, and using information effectively and ethically.
- Embed cybersecurity techniques in graduate attributes so it is embedded across their program of study.

Online:

- Training modules, and resources on cybersecurity, privacy, and data handling agreements for the educational technologies they use at the university.

In assessment:

- Embedding digital citizenship skills in assessment tasks to enable them to participate in online communities safely, ethically, and respectfully.

Supporting our Teaching Teams: Where cybersecurity meets curriculum and how we support it

For teaching teams, institution-wide strategies are required to support them in developing their own digital fluency and literacy skills and enable them to embed cybersecurity practices and techniques into the curriculum. Mandatory training is common but underutilised and resisted. Usability and security of technology are seen as opposing forces and finding the 'sweet spot' is a challenge and strategies to address this challenge shared included 'coffee vouchers' for engaging in non-common features of enterprise software and providing easy ways to access supported and approved tools.

Attendees shared some of the barriers facing teaching teams such as a lack of authentic connection between IT departments and teaching teams which result in resistance to applying cybersecurity techniques in their practice or completing training modules.

Strategies for supporting academic staff:

- Identifying who takes responsibility for cybersecurity acuity across centralised departments and how they will partner
- Providing explicit listings of approved and supported virtual learning environment (VLE) components (educational technologies). In parallel, listings of technologies that have not been approved in line with the rationales/considerations for non-implementation.
- Ensuring professional development for academics in the use of educational technologies has embedded components of cybersecurity enhancing the acuity and active engagement with linkages between tech and activity/assessment design.
- Working collaboratively with other areas to determine linkages for support and provide risk mitigation across educational use-cases.
- Implementing awareness and/or incentive programs. Coffee vouchers are very attractive.
- Making explicit linkages between ‘enterprise’ modules for staff/students and strategies for embedding continued awareness and practice in courses.

Barriers & considerations:

- VLE Management at Enterprise level – finding the ‘sweet spot’ between usability vs security
- Decentralisation of system management, collaborative mechanisms should be put in place
- Academic/staff time and limited ability to incorporate more content in the curriculum.
- Getting buy in across specific departments – targeted awareness based on use-cases should be garnered to support engagement
- Size, complexity & turnover across Institutions – acuity must be embedded in practice

Other affordances & enablers:

- Implementing industry access to supporting tools (eg. VPN Labs, Cyber ranges)
- Leveraging In-context support mechanisms embedded within systems for example Pop up messages on ‘creation of online assignment’, reminders etc.

Generative AI in Australian Higher Education (July update)

Michael Sankey, ACODE President

A whitepaper from ACODE will be forthcoming about Generative AI in Australian Higher Education. Thirty-eight responses were received to a recent Generative AI survey representing 34 institutions.

Survey highlights include:

- Changes to assessment practices are starting to emerge with examples shared in the survey responses.
- Updates to policies and procedures are occurring across the sector, accompanying the provision of centralised workshops and resources to support staff and students in ethically and effectively use Generative AI.
- There is a progressive shift being seen across the sector in encouraging students to use Generative AI in their work but analyze, improve, and reflect on their work.
- There is a trend observed in how exams are managed across the sector.

Further insights into Generative AI in the sector can be found in the whitepaper when it is available. No spoilers here!

10.0 LTLI update – Michael Sankey

As stated in my opening remarks we have 45 registrations which exceeds our expectations. We have sponsorship from Pebblepad, FeedbackFruits, Echo 360 and Anthology(Blackboard).

The program has been completed but will need some tweaking of presentation titles but that is all.

Catering and events have organized and all the merchandise has been kindly stored at Sunshine Coast University awaiting collection by Karen.

All in all the LTLI is coming together nicely

11.0 Benchmark 9 Learning Spaces update – Michael Sankey

As previously reported the working group is meeting twice a week and working through the benchmark

Once completed ANU will host ACODE 90 in November as a demonstration of the benchmark and Learning Spaces.

The review of the other 8 Benchmarks will start once BM9 is complete.

12.0 THETA update – Michael Sankey/Karen Halley

A very successful THETA in Brisbane, Over 70% of participants were first timers so that indicates that the future of HE is in good hands. We are still waiting for the final report from CAUDIT

13.0 Learning Space Portal

A reminder that the Learning Space Portal. See link below is always looking for new material. If you have a space that you would like to showcase send pictures and a small story to add to the website. https://www.acode.edu.au/course/view.php?id=62

14.0 Liaison with other Organisations

ASCILITE- Karen is liasing with ASCILITE re holding the 2024 meeting in Canberra

CAUDIT – Awaiting final numbers from THETA

TEQSA - Nil

ICDE- News forum for updates

15.0 HOT TOPICS:

Data and artificial intelligence ethics, and what universities/HE are doing in this space- both within teaching and learning and at the overall enterprise level. – Ratna Selvartnam

Ratna introduced the Topic. The context being always, It's that from our institution we know that generative. AI. and everything is such a hot topic now. But it's gone beyond the whole technology piece. It's become almost like a lifestyle discussion. But the main concern we are having around the university, in parallel with how teaching and learning is impacted is data and ethics data, ethics and artificial intelligence ethics policy. So we have a first draft going out to senior leadership to be socialized and to get feedback on.

But it's when we did a bit of a benchmark in the landscape. It seems very limited. Not many universities have this, and we don't even know whether, when we've already declared that ours is going to be a living document because it's such a fast moving area. I just need to get a sense of what everyone is feeling and doing within this space, and whether there is interest in actually opening this up wider to our members to get some feedback, whether it's a report or a white paper, whether a few of us wanted to do this together. But really we need a bit more Intel to help navigate the space.

CQU University have a position paper and are pretty happy with where it’s at. It was passed by Academic board, and we're now just working out the scope of implementation. It's really a policy review and I don't know why I haven't thought to have the question with our digital services about what they're doing from the digital side to protect the students and their data. I know they are doing things but actually haven’t had that conversation, because we're quite separate divide but do work together. We do have data governance structures. ITM would revise that without even talking to me or our area, that need to have more discussion at CQU.

Griffith University is in a similar type of situation, where there's certainly a lot of work going on in the IT area and digital solutions kind of realm. We're not exactly aware of what that is. But from our PVC and executive level we're forming working groups and things around the establishment of the policies and procedures. Mainly for us, it's professional development. We are really concentrating now on, what development can we help academics with in terms of learning, design patterns and assist on the ground in assessment as a priority of course.

At Auckland I'm just pushing links to the publicly accessible stuff that we have some of it's old, I think the oldest policy in there is from 2018, and I know that the university is tackling the additions of data, sovereignty issues and generative AI in the update of these policies that are coming, particularly data governance ones. But that's where we are right now. I, I think the big focus has been on academic integrity and generative AI first.

Sovereignty is a huge issue, particularly when you start thinking about indigenous data and their identification or concern that as what they would consider Tom, now, which is which is kind of trademarked cultural knowledge. There's real concern around these types of tools. And how we protect that treasure and that cultural.

That's a good point, Steve. I mean, we have similar things hereat CDU. We haven't really considered them as such. I mean, we do consider we have. We need to see permission from elders and people like that. But I think that's not well understood by most of our staff, the responsibility they have to actually seek permissions and things like that at least by some of them.

The use of AI in that space because a lot of the AI or the course, which is a combination of all the stuff that over the over the years, which is, can be quite discriminatory.

At Western. And it's interesting because we've been talking about it in a generative AI in the context of academic integrity. It's a lot of work happening in there. But we've now got a project to look at a pilot of generative AI across the institution and around that. So we've got that as a test case, if you like. There is a steering committee. What's interesting on that steering committee is you've got the C idea, not the size of.

You've got members from your teaching and learning. You've got research, and you also have the university secretary on there.

So that that from that perspective, and also since the second tier, then the third tier of that work is in generative. AI policy and framework, so looking at contractual issues, privacy concerns, IP, etc., etc.

ECU are trying to get a bit of a front foot, which I don't think it will ever happen before Microsoft rolls out their co-pilot and user end features. Then, you know, as 0 is going down the co-pilot route. And then they're talking about cognitive AI.

Michael Sankey -The thing is we're looking at this from individual institutional perspectives which is great, we need to. But part of the problem is, we're not getting any direction from places like TEQSA and the Government that's a real concern that we'll all end up with our own kind of nuances on this, without a clear way forward.

16.0 Any other Business: Possible name change- We are considering changing the name for ACODE the acronym stays, but should we become the Australasian Council on Open Digital Education? Thoughts on this to the Secretariat and we will bring this to the AGM

- Suggestions sought for future Vodcast series topics

- Suggestions sought for future White Paper topics

PART C: ITEMS FOR NOTING

17.0 Future workshops and meetings:

ACODE 90 November 2023 – ANU

We are urgently seeking Workshop Hosts for the remainder of 2023. Please contact secretariat@acode.edu.au

Meeting Closed 11.33am

Michael Sankey
President, ACODE

EXPLANATION

Note that the Agenda for this Business and Networking Meeting follows that proposed by the Executive in June 2003. Unstarred items on the Agenda will not be discussed, but any recommendations they contain will be covered by a single motion covering all unstarred items.
Any unstarred item may be identified for discussion by request to the President at any time up to item 4 on this agenda.
Please Note: Each member institution has *one* vote only. Members with affiliate status do not have voting rights, however are able to participate in discussion at the discretion of the President.