Empowering schools to nurture cyber safe citizens – transcript

Sharon: She has extensive teaching experience in NSW public schools and as you would all know she has changed the technology paradigm in many a classroom. So, Megan with her cyber powers has brought about a real cultural shift in teaching and learning and continues to empower others around her and she's going to lead our session today on 'Empowering schools to nurture cyber safe citizens'. Welcome, Megan and we'll pass over to you now.

Megan: Thank you. If someone can just enable my share screen video that would be awesome, please. That was quite an introduction! Thank you very much, Sharon. Super excited to be with you all today. I'll just try that share screen. Yes, excellent! Thank you. We should be good now. Just to get the chat up so I can see you all chatting. Feel free to pop into the chat and ask any questions as we go. So, just getting my mini screen setup here. So yeah, first of all I'm coming to you from the land of the Darug people. I also want to acknowledge that this always was, always will be the land of the First Nations people. Hello, it's great that you can join me today. Look forward to chatting to you all about – Empowering schools to nurture cybersafe citizens.

I guess you know, I don't talk to this as a standard experience with what I do at Microsoft. As mentioned, I did run lots of teacher workshops previously and spoke to lots of teachers and schools out there around, you know using Teams and creativity on windows devices. I now work in a slightly different role – working more with the IT pros across education sectors across Australia talking about security and compliance and you know very different things to what I did as a Learning Delivery Specialist. So, now this presentation that I've put together is really just a bit of a storytelling experience I guess from both my time as a teacher myself, as a person who trained teachers but also as a person now who works quite closely with Departments of Education and Dioceses and Independent sectors across Australia to really think about how both the system and the people in that system can take responsibility for nurturing cyber safe citizens in the long run. So yeah, it's not an out-of-the-box presentation that I usually do so hopefully it all makes sense to you at the other end. So, sorry I'm just bringing up, sorry can't see everyone's videos anymore but that's alright. May be gone!

So, at Microsoft we have a mission to empower every person and organization on the planet to achieve more and when we talk to schools or when I talk to schools I talked about empowering every student teacher and school on the planet to achieve more. Now I think that's really important as a company that's our mission. We don't care about your data we don't care about what you're putting into our system we care that you are using it to empower yourselves and your community and your students and we want to make sure that that's the most secure environment as well. So, while normally when I'm talking to the likes of the teaching community and leaders across schools, I always talk to these amazing tools in the middle. But today I'm actually going to make mention some of the other ones on the outside that might not be as familiar to you.

So, I want to highlight just how important the work is that ITD do at the Department of Education level and the other IT directorates around Australia are the same as well. Looking at, you know, how the security tools and the identity tools are so important but the good news is you don't have to worry about those. The security and the identities tools have been set up for your protection and in the background, if we wanted to look at the architecture of that it's a bit of an eye shot and I'm not going to

talk about that at all. I just want you just sort of know that you know when you work in a big Department of Education there is a lot of work that goes on in the background to secure you so that you can focus on the amazing tools available to you to empower your students. So, I thought that was just sort of mentioning that sort of architecture that's in the background when you're accessing the Microsoft cloud. The other piece is around some of the tools available to you – so the ones that I'm going to mention quite a lot today are the Windows devices that you have access to, Microsoft Edge browser which you also now have access to or most schools, I remember, we've got multiple states here. The security embedded into those, quite often I don't talk to this pillar – we have 3 pillars in our education team. Often, I just talk to that one when talking to IT pros but I'm going to talk to some of those technologies today and then Teams will be a bit of a focus as well.

But what I want you to think about over the next 60 or 70 minutes or so is that we, you know, you're here today more than likely, to learn how you can empower, you know, your colleagues, whether you can, as well as how you can empower your students and most probably most importantly or equally as important your community. How can you empower all of these users so that they are using technology in a secure way and protecting the data and the information that you know is so rampantly available in today's education system? And then how can you empower those users through both the technology itself but also education about that technology and so when we look at the changing landscape of security specifically in education – this is actually stats out of the USA, a little bit older but that's OK but they would still be quite relevant if not higher in 2021 but 60% of student data and these are, a promise I only have a couple of scary slides!

You know student data can often be breached the data breaches are often caused by members of the school community whether that's an individual clicking on an e-mail or logging into an account that is not, logging into a, yeah, a platform or account that's not secure and secured by the schools' IT department and also the number of security events that occur in education are quite significant. So, you know we're aware of security threats happening not just across the world but specifically in Australia as well and the big concern is in education. It's the most threatened industry so when hackers when, what are they called, threat actors, when the states as it's they're known as lowercase S are looking to who they should attack – education as you can see there, you know, these graphics are not hiding the other blue bars. That's literally where business and professional services stop and education extends out. Education is low-hanging fruit for the undesirables of the world.

So, it's important that you know it's great to use technology. I'm definitely not here to scare you off. I'm here to say that you need to ensure that that technology is set up effectively and used properly both at home and at school and I think the most important thing and I just realized that I didn't make this slide pretty. I meant to. That I like to always think of is Mark Greentree who is the IT director, T4L Director for DoE – he wears a few hats I forget what title he currently has or titles! But he has this really simple philosophy around technology that should be simple, reliable and effective and I think that's what we need to have in our minds as school leaders as we think about the technology we use to ensure that it is simple, reliable effective and what I've been thinking is that they perhaps should be a fourth one that says secure. So, I'll message MG at some point and suggest that he adds that to his action when he talks about technology. So, secure is another one along with those other three that I think are really important.

So, let me share over the next however long. I'll be sharing some resources, I'll be sharing some thoughts, you know, some things you should be thinking about and even just some really simple tricks. And so, for this first one, I want to share something that you can do with students and it's a really simple way to educate your students around digital safety. And apologies Mona. I did see your e-mail earlier I didn't send through the hyperlinks but I promise I will send those through at the end. So, this website is a website actually built by our New Zealand colleagues over the ditch. It's not region-specific so you can use it with your students here in Australia and the idea is you know it is one of those you know and I think about MG's simple, reliable effective – it is a really simple and reliable and effective resource that I think schools could make use of and the idea is that it's about educating students on four essential behaviours with technology and getting them to learn how to protect their data and let's face it a lot of adults could probably do with this education as well. Looking at how students should not be putting up with bullying behaviour, how they can wise up to risky situations when using technology and then also be responsible for your actions. And I guess in the context of cyber safety and security protect your data is the one way looking at, but I think all four are really important in the context of an effective learning pathway for students across all age groups in regards to their digital safety.

And so, when we look at the resources they're really simple. You get four PDF documents when you go onto that website – the first one is protecting your data and looking at it's like I said very simple. Teachers could use that, maybe create a roll call sort of program in in the high school context where you've run through some of this stuff from year to year or maybe every year and there's a simple quiz at the end so it just gets students thinking about identity theft and phishing and malware then there's the cyberbullying one, the risky situations and introducing the digital citizenship as well. So, really really simple reliable and effective resource. So, check that one out https://aka.ms/studentdigitalsafety as I think the students sometimes are not so much the easiest ones to educate but you know we can easily integrate the digital safety message into the curriculum. When we're working with parents and teachers, it can be a bit more of a challenge. And so, for this one I do want to talk more to, you know, your staff your broader community, your parent community and even other people in the community who access the school and use your technology as well as your students to a lesser degree and looking at some sort of all-up-messaging that I think should be prevalent in schools when using technology. So, to a certain extent with messaging, it is education!

So, with your Microsoft 365 accounts, every single user in every Department of Education in Australia has a Microsoft 365 account and your e-mail address and password you use to access the Internet or access your e-mail is your username and password for Microsoft 365 and it's really important to know you know the Department of Education across Australia invest in like Microsoft 365 licenses for you which means you get a whole heap of technology available to you as to your students but I do want to highlight the security built into all of those technologies. So, whether you're using Office 365 on a home or personal device, whether you're using Windows at home, whether you're using it at school, yeah you have mobility and security built into those.

So, I do just want to take a moment to talk about home and school. Because one of the biggest challenges in the eight last 18 months is that that experience has merged and it's still merged for those of us in in NSW and Victoria. So, we need to think about, you know, the devices that we have at home so and our students have at home but also thinking about the devices that our teachers have at home and the security of those devices and like I mentioned at the very beginning the departments of education across Australia do a really good job of ensuring the security of your profiles and the like so that you can

log on to personal devices but there's still you know some responsibility on the individual with those devices which I'll talk about soon. You've also got your school-provided devices and like I said there's been a bit of a shift in regards to the last 12 months where the, just double checking that my screen can be shared? So yeah, bit of a shift in the last 12 months that we have devices moving across the school and the home environment constantly. Whether that's teachers who are issued a school device and take it home, whether it's students who have borrowed devices to take them home during remote learning, teachers and students as well in the high school bringing their phones to school and students and teachers accessing files on and across all of those devices. And there's some, I guess sort of rules and regulations and things we need to think about, you know, there all policies written by every state department around the use of those devices and I'm sure all the things I'm about to show are in somewhere in the policies. I guess it's just sort of making it very obvious in this conversation. The other thing I need to talk to is your different accounts that you use both as a personal, you know as a teacher or as a student or as yeah both in the school environment in the home environment. So, like I said when you start work in your relevant department of education, you get an e-mail address. So, it's usually around – so the DET peeps would be very familiar with writing @det.nsw.edu.au as your e-mail domain. Then your students will use @education.nsw.gov.au and I've run out of room, so we won't go around the other state departments but you get the idea, right? That's your Microsoft365 account for work or for school if you're a student.

You probably have other accounts that you've set up over the years from a personal perspective, so you know, I've got a Hotmail e-mail address, I've got, I've got an Outlook one, you know, switch pens, always good to have a backup. Oh, that's so much more delicious! What else do we have out there? You've got, you know, things like Optus.net and Telstra and all that sort of stuff and some fancy people even set up their own domains and have their own email addresses. But the idea is that you know especially for, you sorry, good old Gmail as well.

The two I want to point out are Outlook and Hotmail. If you have a Hotmail or an outlook account, you actually have one of our free Microsoft accounts. So, there is a difference between Office365 home and Office365 for education and it's aligned to who pays. So, the department pays for your school Microsoft365 access and you either have a free account or you pay for your Office 365 home using quite frankly any of these e-mail accounts. But these are the two that are owned by Microsoft. So, it's just important to note in regards to what I'm about to talk about – the personal accounts versus the work or school accounts, alright? So, the difference is ownership and who pay or the free ones.

So yeah, let's move on from that and handwriting. I guess one of the important elements in ensuring that your students and you as a teacher and you as a school leader have the most secure technology environment is updating your software. And this, you know, as far as I'm concerned it doesn't matter what platform you're using, what device you're using, it's important to keep your software up to date – both your operating system software and your apps and software updates. So, whether you've got that iPhone right, don't click later! Install it as soon as you can. No more later! Always install now. You're on a Mac. Do it as soon as you can - in an hour, not tomorrow. Android phone same thing – do it as soon as you can. And if you've got Windows devices, you can update those as well or you can pick your time or snooze. But let's make a promise to one another right now – to update your personal devices when prompted, as soon as possible because with software updates and app updates and operating system updates, comes better security, all right? Almost, if you go in and look at the notes of any update to an app or an operating system, there are always security updates. It's really, really important that you have

the most up-to-date software on your devices, both personal and school ones and we'll talk a little bit about your school-based devices. But, and I've been very red in this slide on purpose right. I cannot reiterate enough how important it is to update your operating systems when it pops up on your screen – make it happen and encourage your students to do that.

I realised that not all students bring to school the most current, you know, the operating system, for example, regard to Windows and that's OK. They can still update and have the most up-to-date settings according to that operating system. So, it is about responsibility and having your personal responsibility, you know, to update your personal devices and then in your schools, you know, in NSW department schools they're called Computer Coordinators. They're called different things around the country. That often falls on, unfortunately sometimes, one person so whatever you can do to support your Computer Coordinator to update your devices to have the latest operating system and software and app updates, please do that. Supporting them and having a process whenever new updates are pushed out is really important in securing your technology.

In the Department of Education T4L team driven by the amazing Stu Hasic put out, from a communications standpoint, put out news and information all the time if you haven't yet checked out the Technology for Learning web page I just go to Bing or Google and type T4L news and it always pops up as the first search. Please check that out. You can follow, you can get updates and get e-mail notifications and the like. These are just screenshots from the last two updates in regard to Windows – the latest image on windows devices, the fact that Internet Explorer is going to be retired. I'm looking at the new e-mail interface that's available or e-mail modernization sort of project that's now happening, so you'll get the latest version of Outlook, which means you can also get the latest version of Outlook desktop as well as Outlook online. They're just four simple updates, not simple updates! They're just four big updates really that are coming. And it's important that you support your Computer Coordinator to ensure that they can update the devices in your school and communicate to your teachers as well. So, whatever you can do I make this, I made this less aggressive, so I made it blue! Whatever you can do to support your Computer Coordinator. Apologies for those who are not in the New South Wales DoE here. F12 is a bit of a verb and Computer Coordinators would know it well when they have to update their devices to the latest T4L Windows image. But you know there would be a similar process in other states. Yeah, please support that Computer Coordinator. It's really important in regard to securing devices. And also, have that plan. A lot of schools will take the time in the holidays to update devices, but I've worked with a lot of schools where the Computer Coordinator isn't supported, and they struggle to get those devices updated. So yeah, please do support them as much as you can to ensure that there's a nice solid plan to update devices as soon as possible so they can be secure.

When it comes to software, Microsoft software and keeping that secure, this applies to everybody. Because you and this applies to everyone working in or attending any department school in Australia. When you go to office.com via a web browser, for some reason, a lot of people click this button. I don't know why. I think it's just cause it's big and blue! I don't know. Don't click that one that's a bad button to press. Lots of people do. What you want to do is simply just sign in and you will be taken to your, you know, whichever department you work in – you'll sign in with your usual school e-mail address and password and then be taken to the Office365 dashboard. Install office for free up the top right-hand corner on your personal devices. This is a really good thing to share with your community. That way they can have access to the latest and most secure version of Office. So, they can install that on up to five personal devices. On your school devices – you don't have to worry about that. That's managed by your,

you know, Computer Coordinator who pushes out the software and it regularly updates automatically with the updates pushed out by the department.

But on your personal devices and this is great for your BYOD programs but just also good for both teachers and students to know about on their PCs at home, on their Macs at home, it works on Mac you know that you can install office on a Mac also. You can install that Office software for free. If you ever leave the Department of Education or the students finish up in year 12 then it will simply, it does survive for a little bit but then it pops up saying you need an Office365 licence. You can either, you know, put in your new school's e-mail address if you've changed sectors or you can put in your personal Microsoft365 account as well. Or if the year 12 student goes on to university you can pop that in. So, yeah office.com, you have that access.

Silesh, just let us know where you're from and we can potentially help you out in the chat there in regard to access. So yeah, just be aware of that free Office because it really does, one it's great from an accessibility sorry inclusive perspective. Every single student can get Office on their devices no matter how old they are. So yeah, check that one out. So, everyone in the NSW Department of Education can get Office for free, you have that access. So yeah, not a problem on your personal devices.

All right! What I want to talk to you now is that that home experience and to a certain extent educating your community, you know, your parent community and your students as well about how they can be more secure and teachers actually, as well. Let's just go with everyone! Around securing their devices because of the files that live on those devices. A lot of teachers especially or obviously saving work that has personally identifying information in regards to students sometimes it's very sensitive information and it's saved that can save to different places, quite frankly. But then students also need to be aware of you know securing their devices if they're out a cafe or something like that. Teachers need to be aware of you know signing into devices as well if you share your home device with your own children or a spouse you need to secure your identity on that device. So, just going to share a few tips and tricks from a personal device perspective. So, signing in with Windows Hello that's not enabled on a lot of department devices, but your face is very secure. So, if you do have a personal device and it prompts you to set up Windows Hello, great idea. Really good for younger students at home as well.

Microsoft Edge, the new edge browser which I don't think is standard on the department's image at the moment, but it can be pushed out by your Computer Coordinator, has some really powerful tools for password protection. OneDrive, I won't talk about it so much in the sense of personal use, but I do like to use my personal One Drive – my OneDrive that's associated with my Outlook.com account. I use that for my own like my own personal family stuff. I try and keep my work and, well I know, I do I keep my work and my personal files very separate. So, you know if you have your personal stuff saved in your school account it is not a bad either to either use your 365 home One Drive or if you don't have one of those just go to Office, sorry go to Outlook.com and you can set it up for free. And you can save your files there. So yeah, that's all I'll mention in regards to personal OneDrive.

And then another great tool that I don't think a lot of people are aware of and it's a really good one to communicate out to families is Microsoft Family. Fabulous name for a piece of technology. So, we're going to look at those four things right now.

So, first, let's look at the setup of a device at home. So, this is definitely something that's nice to communicate out to your community around setting up their technology at home and also applicable for

staff who are on devices at home where they're shared with their household. So, this is Windows 11, but it would be similar in Windows 10 as well. But when we look at setting up, actually sorry let me just talk to security first. If you go to security, so if you go into your settings in Windows and just type security. The built-in security in windows is amazing you don't have to have any extra software installed the, you know, the threat virus protection built into Windows now from Windows 10 and Windows 11, there are firewalls set up and it's all absolute industry standard. And you, I just regularly come in here you get the notifications and pop-ups if there are any issues. But green ticks are what you're after. The same thing exists in Windows 10.

When we look at setting up your account on a device that's I'm sorry, that's Windows Hello, sorry. I just search Windows 10 and sorry, click on the start button on Windows and type hello and that allows you to set up a sign in and you can set up what's called facial recognition or Windows Hello. So, I just thought I'd point out that Windows Hello one as well. All right, so that's some of the Windows settings. The really important one, sorry, is setting up multiple users, right? So, if I set up multiple users what I'm able to do is again go into my windows settings, select family and other users and add someone else to this PC. Rather than everyone logging on with the same username and password. If you're doing that you're exposing, you know, if you're signed into your school account, you're potentially exposing that information to other people in your household which again I'm pretty sure, if you check your policies your department policies, you're probably not supposed to be doing that. So, by adding multiple users it's a really safe way to operate. So, this is literally a photo I went and took of our home PC so that's my login, but you can see two of my kids have also got their own login as well. It also keeps things separate. So, I like logging into my computer and not seeing all the rubbish that my kids have installed on their profiles, and I can just log in with mine. No different to having multiple profile logins on your home, sorry on your school computers, but you can set it up at home. There's a really good reason why you want to do that which I'll share with that Microsoft Family in a moment. And then once you're into your profile it's really easy. You just click start, right-click on your name and you can switch to other users or sign out.

Another really important one is that lock. So, this is probably my favorite, my most used keyboard shortcut. This is really important if you've got your computer sitting there on your desk in your classroom especially, and I don't know why I'm just, I'm so used to doing it now, I don't think about it even when I'm at home. Windows L – don't do it on your computer right now if you're in a Window device because you'll lock your computer. When you click windows L it just automatically locks your device. So, I just click windows L every time I step away from my computer. It's just second nature to me now and it's something you should do yourself, it's something you should encourage with your staff, it's something you should catch stuff out on. So, if you see a staff member walk away from their computer and their computer screen is still logged in, all them out on it and say, “Hey, just quickly click windows L.” I am sure there's a keyboard shortcut for Windows as well. It's really important that you encourage that practice. Even with students, encourage students to not remain logged in to their computer if they're stepping from it. From a cyber security perspective that is essential.

If we also look at the Edge browser. So, the Edge browser I mentioned before, the new one so it's not the bright blue E look down the bottom this is a screenshot of my computer. I've got four different profiles set up using Microsoft Edge. And you can go in, I'll share a link to our support page later where you can learn how to do this. But basically, this is my Department of Education account that I have signed in so that's that one there. I also have a demo Microsoft account, my personal e-mail and then

further down that page you'll actually see my Microsoft account. So, I have four different sort of browser profiles set up, so that's my Microsoft one, that's my personal one, that's the department and that's my demo account. What it means is that I can actually work in different ways. So, if I'm online shopping, let's face it I'm usually in my personal account. I go and check my personal e-mail address there I you know if I'm not working and I'm just browsing my computer and doing personal stuff you know creating invitations or whatever I'm in that profile. It's just it just keeps again my work, and my home sort of technology experiences separate and then I set up a different profile for work. So, most people would only have two – work and home. Because of the nature of my work, I have quite a few of those setup. I just find that really handy.

The other thing I really liked about Edge is the password manager. Now this is very secure yet again, you know, when it pops up in my browser – do you want to save your password? I say yes and I use the password manager all the time. I've got to go in and fix up a few things, you know. I love it! I don't know about you, but I have a lot of accounts, a lot of accounts! And once upon a time I used to use the same password all the time. But that is really, really, really bad! It's really bad practice. But I know it's really really hard to remember passwords. I'm responsible in my house, I swear, for remembering all the passwords for all the streaming services cause nobody can remember them in my household at all and that's fine. But yeah, I do acknowledge that remembering passwords is hard so using tools like the password manager in Edge you just click the ellipses off the top and select settings and that will bring you into this settings area specifically for Edge. And so, what you're able to do is click, you know, within profiles so I'm now this is my Microsoft profile, I select passwords, and this is sort of the password manager. So, whenever I click yes remember word, this is where it comes and I then have the power to manage it.

What's really powerful is that in the, you know, there's basically AI happening as part of this password manager and it will actually - knows all my passwords, and it will determine whether the passwords I have used have been found in an online leak. Microsoft – a massive company, we have access to lots of information and they release all the time. Companies release all the time, the leaks that have occurred from a cyber security perspective. And so, as you can see 19 of my passwords were used in a leak, were used in various leaks. So, I can go in and update those. And so, what happens when I scroll further down it I will say the website that I'm signed, I've got an account with, the username I used, and I can click my little ellipses here to reveal the password and then I see the health of the password and you can see there are different statuses there. They're explained over there on the right-hand side. So, at the moment I'm looking at this I should definitely be going in and updating those two. Knowing me I probably looked at the account and I don't use it anymore, don't care. But I think again, that's just a really nice tool for you to be aware of in regards to your password management because when it comes to cyber safety both, you know, you as users but also your students need to have effective password management so using tools like the Edge password manager are really powerful. If you've got a mobile device, sure we all do, most of your mobile devices have a similar password manager built-in. I'm always a bit sceptical of the password managers you download and have accounts for because I think, what are they doing with that information? You know, if it's not a trusted company who's managing your passwords you probably shouldn't be using that as a password manager. So yeah, that's the Edge browser and some of the Window's capabilities that can ensure that you and your students remain safer.

When we look at something you can tell your parent community a resource you can share, I think this one is really cool, and I've been using it myself as my own kids for quite some time so they are getting a bit older I probably should turn it off! But with Microsoft Family, this is a consumer tool. So, it's not something that's attached to your education accounts, this is something that I simply just suggest to schools that they share with their parent community. Parents quite often ask, you know, how can I keep an eye on my child and what they're doing on their computer and so Microsoft family has both a free and a paid option. I might actually just jump onto the Microsoft Family webpage right now, sorry just on another page. All right so, let's go live. So yeah, with Microsoft Family, this is not aligned to a device per se but to the user profiles. So, I've had an Outlook account for each one of my kids since they were in primary school and whenever I add the kids to the Windows device, I add them as their, you know, townsey03@outlook.com e-mail address or whatever it is and that's you know how they've had those e-mail accounts for quite some time. And so, when you create a family group you add those Microsoft accounts in for all of your kids and what you're able to do is whenever they are signed into any computer, right so both our family PC but also their personal devices, you can control screen time limits, you can filter content, so for younger students or for younger children, parents can determine what they can and can't look at. And even at certain times so, if they wanted to block YouTube for certain time periods or days across the week, they can do that and then weekly you get an activity report. Actually, I must only have it turned off for one kid as I just received my activity report e-mail. So, each week in my e-mail I get an activity report of how long the child has spent on certain software and the web browsing that they have done so really nice way for a family to manage their, I guess screen time but also just to manage their technology use. And then there's some paid services like if you want to use – find your family and know where your kids are at all times there's that and then there's just some other capabilities I think if you use Office, not sure about the paid experience but I'm sure I think if you have an Office365 home subscription, maybe it's already a part of that, can't remember but definitely check out Microsoft Family. And you know use it yourself if you have your own students but also share it with your parent community because I think it's another great one for saying staying cyber smart with parents and families.

Where are we at? Plenty of time! Alright so, the next one I want to look at is really sort of coming back to school, you know. The last few things I've talked to have been about, you know, home and personal use. I want us to sort of set the mindset now around teachers and school operations and how a school can set them up to be secure in the way that they work on their files, all right. So, staff very much use technology. So yeah, more and more, as you know, particularly the pandemic, we saw literally two years of transformation in two months in March and April of last year and we continue to see rapid digital transformation as we shifted back to remote learning obviously in education it sort of happened again. But what we know, because obviously, Microsoft works across multiple industries not just education, but what we know is that the world has shifted and we know you know most businesses at all industry levels, we are talking to businesses, organisations, universities, schools digitizing every part of their experience, so that if and when remote anything needs to happen again that will be easier. But also, because that is where the world is going. The world is moving to the cloud, on-site servers and the like which I will talk to you soon as well, are a thing of the past. Companies and organisations and departments of education are investing in cloud technology so that the secure cloud that you have access to is where you can digitize your world.

And so, with Microsoft365 and all of the amazing tools you have access to when it comes to thinking about securing your files, you can do that at both a personal and a school level, all right? So, when you're working by yourself – you're able to save your files into One Drive and you can give access to others if you choose to, not a problem. You can sync them down to your computer for offline access, not something you would recommend doing on a shared device in schools. If you're at home, maybe it depends on the size of your hard drive but also making sure that if you are syncing your files down to your device that you have those separate profiles set up on personal computers. But yeah, your One Drive – great place for you to work on your files that are just for you.

Again, for students, really great place for them to work on their files that are safe and secure. Managing those files is really easy, you know. When you e-mail a document as soon as you hit send on the document, if you've attached the file to the e-mail, you've lost control of that file. However, if you share the file via the cloud whether that's in One Drive or Teams or SharePoint you have a lot more control over that file – you can see who's made updates to it, you can control who has access to it, when they have access to it and when the access is removed. If you are using e-mail to share your documents around, you have version control issues and like I said, you sort of lose control of who has access to it as well. So, having your files saved in the cloud is powerful. Now once upon a time the only place you can save your files in 365 was OneDrive but we now have amazing platforms for collaboration and so Teams is the space where you can work securely on your files as a team and then SharePoint becomes, depends on the department that you work in, how you can access SharePoint, but SharePoint can almost be like a school intranet and I know quite a few schools in NSW DoE who are using SharePoint as sort of their published document space and making that available for staff but also for students depending on the content.

So, to a certain extent, this and this becomes, all these become obsolete. So, for those of you in the New South Wales Department, you would be familiar with going to File Explorer and selecting faculty and you see all these files. These T drives as they are known fondly, and they're known as different drives across the country but specifically in New South Wales DoE are retiring one day soon and I'll need to be moved to the cloud. But a lot of schools have already started that transformation and have started moving their files into the Microsoft cloud. Not only is it more secure but it also means that your staff can more easily access those files anytime, anywhere, on any device if it's in the Teams or SharePoint space. And when it comes to these things, they are one of the most insecure, they're one of the most terrible ways of storing files.

I will never forget a workshop that I ran at a school that I shall not name, where the Principal actually came in after lunch, and their face was just green and they'd had a student in their office at the lunchtime break. He was in trouble and you know they dealt with student, student went off back into the world and the Principal realized that a USB with sensitive data was missing and I don't know what happened next cause I was running a workshop. But yeah, I just I will never forget that and I always think that USBs are the most terrible ways to save, to store secure information. Of course, it's fine, you want to put some photos on it and take it to Officeworks and, you know, print some photos. Great not a problem! However, you can sign into the Microsoft cloud through Officeworks printers these days, but USB is just very insecure. So, think about how you can secure your files using these spaces and I don't think it's just a matter of you know saying to your staff, “Oh you know we use the Microsoft cloud now. May the force be with you.”

It is really important to come up with a strategy for how your school uses the cloud and, you know, we've got lovely Learning Delivery Specialist team across Australia – Andrew Balzer in New South Wales, Troy Waller in Victoria, South Australia and Tassie and Amanda Frampton up in Queensland and Stephen Payne looking after the central and western states. They are here and ready to support your schools in running workshops, they just, you know, they run workshops all the time that you can attend, or they can actually customise workshops for your team as well around building a strategy for using these technologies so that your files are, sorry your Teams structure is set up effectively. But also, that the transition to using these technologies is effective as well.

Just yeah, again something to keep in mind but I do just want to mention the security of Teams this looks very unexciting and boring cause it's so texty! So, let me tell you the story in a slightly prettier way but the Teams platform - built on our Microsoft365 security principles. Basically, the idea is the security principles need to be built in across so that it works across all platforms including all devices. So, while yes, I did mention Windows devices earlier, our file management security can take place on any device whether it's an iPad, a phone or watch, a Chromebook a MacBook, you know, Office365 works on any of those platforms, so that's security exists across all of those platforms. There's a lot of AI and automation built into the experience now which can make your life a lot easier.

So, when you, sometimes there is a little bit of trepidation in moving to the cloud but some of the automation available now through Power Automate and the like can actually make working with technology easier, not harder. And again, like I said, integrating across everywhere is the principles of our M365 security. So, whoops love slides at build out! So yeah, when it got us the security and compliance stuff probably just more technical sort of things, but just you know, when your files live inside the Team space, it has to you've got a sign into the Teams interface you can put in, the departments can put information protection on certain files, there's risk management and archiving of the files as well so even if you know you delete files, for example, accidentally that can be retrieved. The cloud, the Microsoft cloud and Teams specifically, is a much safer place for your documents to be saved. And then when it comes to that element of protecting people, data and your school, even just the online meetings are safer as well from a cyber security perspective and being able to you know lock people out and not have people jumping on those, which is a cyber safety issue. Being able to protect your documents and restrict the access to them are all really important parts of the Teams platform. Like I said, not just Teams platform and saving files to it or part of Teams but also meetings as well. So, there's actually been some new updates to meeting options, when you're running a Teams meeting in under the ellipses, during a Teams meeting, you're able to control the entire meeting. You can even lock the meeting so that people can't come in anymore once it’s started. But you can control who presents, you can control who turns on the video and audio so that it's as secure as possible. You can also restrict the lobby, which is an important part of that cyber safety approach as well and have different roles and moderations within the calls.

When it comes to that document protection and information protection one of the great things about Teams is you can pin websites – click on the little tab in Teams in a channel and you can pin a website. If that website is being deemed malicious according to our technology, it actually won't display in Teams so that can protect you against those web-based cyber security threats. I always talk about Teams being one-stop-shop so even being able to pin websites means that you know students can view a website that's safe and secure and pinned but by looking at it within the Teams interface, they're not going off on the web and clicking other things which can be not so safe.

So yeah, then there's also communication compliance as well another one from a safety perspective for example in New South Wales Department of Education, chat is turned off for students and so the departments and the IT departments have the ability to restrict the controls on these technologies. So again, just a safer way to work. And then, just from our perspective you know, Microsoft we have another sort of saying where we – Microsoft runs on trust – and we're pretty passionate about that in regards to not using your data in negative ways, I don't know how to term that correctly, but the idea is you know with Teams we never used Teams data to serve up ads. It's just not how we make money. We make money from our subscriptions and your Department of Education has already paid for Microsoft365, that's where Microsoft made their money. We don't need to make money by data mining or serving up ads or anything like that. So yeah, we don't, there's no participant attention or multitasking tracking or anything like that. We don't access customer data at any time, there are strong measures to ensure that your data is restricted in regard to where your data sits on servers in Australia is completely secure and there's no, you know, no back doors, there's no government access or anything like that and we have absolute transparency as well.

If you're interested in that whole data piece and the way it plays out in the world, our, I think he's the Vice President Legal, or something like that. He has a very, oh! Far out. Brad Smith is his name and he wrote a book which I would normally think would be a boring book but it's actually really cool. Admittedly I listen to it as an audiobook. It's called weapons of mass destruction! No, it's not called that. It's definitely called weapons or something like that. Anyway, look up Brad Smith and there's a book about weapons and destruction, information? Something like that anyway. I found it really interesting cause it's a really interesting look at the way data is used and how protective Microsoft is of it. So yeah, check it out I thought it was pretty cool and I'm not that nerdy.

And then just the last little piece is around the compliance. We're very compliant with Microsoft Teams in regards to aligning to the expectations of the web and the like. So yeah, just that last little slide on that one. So, what I wanted to just show, let me go see how we're going for time. Yes, what I will do is you know, I think the goal of all schools should be to move away from these two things – this one will be forced upon you and this one you really need to drive students and teachers to not be using those as much. So, what I will just do is open up Microsoft Teams and just give one example of the protection of the document. And so, whether its Teams or whether it's OneDrive or SharePoint, if the file lives in one of those three places. 'Tools and weapons' thank you Kathleen Morgan! I don't know why I said weapons of mass destruction. Thank you, Kathleen! So yeah, as long as your file lives in OneDrive, Teams or SharePoint, you can do what I'm about to show, all right. Let me get there. Oh, come on! You know what, I might just go to my OneDrive instead. I didn't tell all my children to get off the Internet. Alright so this is just my OneDrive files.

So, let me just go into a random file here. So, there's some files happy days I at the moment no that that is only for me from sharing perspective it says private so only I can see that. I've got the ability to click on share and at the moment if I was to click that link it's anyone with the link can view and that's not anyone with the link in NSW DoE, that is anyone with the link in the world, all right? It's not something that I would never share really any, any document, except if I was needing to collaborate with people outside of the Department of Education, right? But if I wanted to share this just with teachers in the department interesting because if I select people in the department that includes students so you need to be aware that if I applied that and copied the link and shared it to a teacher they could ultimately share it with, you know, that could be shared to anyone with the Department of Education e-mail

address, and they would be able to see. So, you need to be very, you know, specific in how you share your files. If I click share again. Oh, lovely Mona! Mona says it's very important to share with care. I love that!

I can go back into share and click the ellipses yet again and manage my access and I can see that I've given access to everyone in the department. If I click my little ellipses again, I can stop that link being shared anymore. If someone clicks on it, it won't work for them anymore. I have control over my files. So, if I go back and share again and just drop down once more. Oh, come on Internet! You can see me now. Anyway, the other two options are people with these existing access – I don't really use that one as much, or specific people – now obviously that one is going to be a much more restrictive way of sharing your file. I also have the ability to grant them permission to edit or not edit and very importantly there's that ability to lock the download. So again, if you want to make this, you know, it's maybe got some sensitive data in it you don't want people to be able to download a copy of it but you do want them sorry to either edit or view it, then you can still select that button. Not a problem. Again, you have the control. So, then I would jump in and I can start searching. OK, so it just depends on your global address book. So, if I search for Mona there she is, cyber security awareness and education manager, and I can click send and she'll get an e-mail. Always nice to add a message. Here is the file. And I can click send but I also have the option then later to go in and again click on my ellipses, the ellipses is very important in Microsoft and manage access and if for some reason you know say Mona had deleted her e-mail, the e-mail that she received or something like that, I can easily just click copy and I can send that off to Mona in a Teams chat or an e-mail or however I want to send it. But that link is unique for Mona. No one, even if I gave that link to Joe who I can see on the call as well, he could click on it and he won't be, even if he logs in, he won't be able to see it. I've only given Mona access. It's all about your profile and your identity. So, I'll just remove access. Quite sure Mona doesn't need to see the team structure set up for a distance Ed school and I can delete that link again. So yeah, just wanted to talk to that a little bit around granting permissions.

The other one that's important is version history. So, if I now jump into Teams, version histories are amazing. Now one of the concerns that a lot of people have in any cloud platform, is when you've got 1000 people having access to a file. Sorry I had shut up. I just needed to make sure they didn't load while we're all here. If you yeah have lots of people accessing a document, there's concern right that someone or even you know a student might sabotage that document. Again, a cyber safety issue. With version history you can protect any updates made to your file. Oh my gosh, I love seeing calendars in teams for NSW Department of Education. It's been recently made available with that mail migration project. Very exciting people, very exciting!

So, here's Teams. That's the lovely example of a setup this is Jordan Springs Public School and their Team set-up. Just give them kudos for that. Well done Jordan Springs! But in my little Microsoft community Team, I'll use this as an example. I can, there's one there, if I right click on a file here, I can't see version history, alright. What I need to do when I'm in Teams, is actually open it up in SharePoint view. It is hidden on purpose. You know, you really should only be able to access version history – one as an owner of a team and two through the SharePoint view of the files. But if I right click this file now, I get this beautiful version history. And so, with version history, overtime as people go into and out of a document a version is created. Let me find another one. Presentations? They are probably all me. Anyway, let’s right click on that one as well. Oh, there we go!

So, overtime, you know, if I decided that the change that Jody had made to this document wasn't yeah, it wasn't good, didn't want it. I wanted to go back to this moment in time, all I needed to do is drop that down and I can click on restore. Now watch what happens when I restore, instead of you know deleting Jody's and going over the top, what I get is an eighth version. So, if I now go to version history again, there's my 8 version from today and not a problem. If for some reason we needed to revert back to Jody's, not a problem, we just restore that. I can obviously view it as well, just in the interest of time, I'm not doing that. But I can click on restore and get that version back as well. As the owner of the Team, you have the power to do that.

Another important one I'll mention is the deleting of stuff. Again, from a security perspective if someone does delete something on purpose or accidentally, right? They delete it. Again, not a problem. As long as there, and this is where it's actually safer than your T-drives or any on-site, most on-site servers if someone deletes something from your T drive, it's pretty much gone forever, right? There's pretty much no way of retrieving it unless the person who deleted it knows they deleted it and can retrieve it. When you delete something from SharePoint or Teams, right? Let me delete something random. Awareness. That sounds like a great idea. Now that's fine if someone knew. Let's not delete those. I probably don't want to delete any of these. I'm not going to delete anything. What I'm going to show you is that if you do delete or anyone in your team deletes something, over in your SharePoint view, right so I can be in any team here. When you open up your Team in SharePoint view, on the left-hand-side, pretty sorry, brand-new Team, haven't gone to SharePoint view yet. Over on the left-hand-side there's a recycle bin, Ok. So, if anyone in your team was to delete something it would go into this recycle bin and from there, you're able to just right click and restore it back to the Team. It's not a problem. Again, it's just about educating your teachers that if they delete something that's OK. It's still available to you through the recycle bin as an owner of the Team and you can restore it.

So yeah, Microsoft Teams are really safe place for you to put your files but still relies on your teachers and students ensuring that the devices that they're accessing Teams on are also secure. So, hopefully, that's given you a good sense of how students, staff and community can protect their devices but also their data and how you can do that through the use of technology. So, it's not a bad thing it's a great thing and through educating those users about that technology. So, we've covered a lot today.

There are so many tools available to you. Not just Microsoft and not just Google and Apple either, you know. There are third party applications that are used extensively in education and it can become a lot to be using a whole lot of different tools all the time, a whole lot of different log on's. It's confusing for teachers, it's confusing for students. If you can refine it and as the amazing Mark Greentree says, make it simple, reliable and effective, you can not only ensure that your operating technology securely, it's actually a lot easier and experience for your staff, your students and the parents supporting your students. So yeah, Microsoft as a platform can be that simple, reliable effective platform. So, we've looked at Teams, we've looked at Windows, we've looked at Microsoft Edge, the security built into all of those and hopefully, that's given you a good sense of what's possible with the Microsoft platform and being a responsible cyber citizen but also educating your community and your students about these technologies so that, they can be those responsible citizens as well. So, this is my final slide. I'll leave it on the screen. Happy to answer any questions that you have. I can see them coming into the Q&A pod there. I can see Mona has shared a wealth of resources also. So, feel free to give those a click before you go.

But on-screen are our resources from Microsoft. The first one is our Microsoft Educator Center. You'll find more than 100 free online courses in there, OneStopEdu - aka.ms/OneStopEdu it's a fairly new page for us in our Educator Center. It has, you know, for example, if you click Microsoft Teams, when you click on that you get probably top three or four videos, our top resources and guides for using Teams in education and then there's sort of a do more with Teams. So, check that one out.

Teacher Training Packs - if you're one of those fun-loving people who gets nominated to deliver teacher training in your school we've built custom built teacher training packs that have got all the resources you need to deliver your own training. I've shared that with a few, I've shared that with many people over the years. But one teacher particularly in mind, comes to mind who messaged me saying, “Oh my gosh, you've planned my entire PD days for the whole year, using that resource.”

And then the last few support.microsoft.com/education are our step-by-step guides for our education tools but another one I've shared today which I normally don't share is just the public facing one for personal devices/personal experiences is really good one to share with community.

And then finally Mike Tholfsen, who is just a Microsoft legend if you like micro-PD via video, he is the man, he's amazing! So, happy, like I said to answer any questions. I see there's been some troubleshooting in regard to accessing some of these technologies but yeah know that – no matter which Department of Education you work in in Australia, you and your students have access to Microsoft cloud which is very secure and amazing. Any questions?

Sharon: Megan we have got one question that's coming to me. I am interested as well. I've always wondered about this my son’s laptop came with Microsoft Defender, I think is the built-in.

Megan: Yes, so really really really good question. Thank you for asking, Leone. like I remember back in the day, I always buy what is it called, the antivirus, Norton! I always buy Norton antivirus and then I started doing AVG free. But yes, since Windows 8 because I know there was always that Mac versus Windows thing where Mac books always had antivirus included. Since Windows 8, we've had antivirus included as well. So, Defender is our built-in antivirus. So, there's no need to buy third party. I actually find it slows down your computer now. So yeah, you just don't need it. It's built into Windows 10 and Windows 11 and Windows 8, if you happen to have a Windows 8 machine still. But yeah, make sure you keep it up to date cause then the antivirus gets updated as well. Thanks, Leone. Any other cool listings?

Mona: No there was only one question. But I think that was a really really interesting session because we learned so much to do with technology and how to, how to be powerful when using technology Megan so unless someone has any other questions. We do have a feedback link that I've put in the in the chat box so please give us some feedback because we really would like to offer this program to high schools and extend it to high schools next year but we want to know what we did good and what we can do better. So, if you could please give us some feedback that will be really really helpful. Thank you. There’re no more questions. Do you have anything to add Megan before we finish?

Megan: No, I'm sorry. I put that one back up. No, I think it's just you know there's plenty of resources out there. I think it's just consistent messaging to both your staff, student and parent communities around yeah working together and supporting each other to be good cyber citizens. Lots of tools that can do that.

Mona: Yeah, we've been very lucky to have you on board and Microsoft on board to deliver these Principal and teacher webinars for Cybermarvel and really excited to see what we can offer in the coming years.

Megan: Thanks everyone!

Mona: Thanks everyone! Have a great week. Enjoy your return to school. Bye.