

Everyday Tech, Hidden Risks: Cyber security & data protection

Webinar transcript – 15th October 2026

Note: *This transcript has been produced from a recording of the webinar. It has been lightly edited for readability, including the removal of timestamps and the correction of obvious spelling, punctuation and capitalisation errors. As it reflects a live discussion, it may still contain grammatical errors, incomplete sentences, repeated words or minor transcription inaccuracies.*

Speakers

Katie Thorn, Director of Innovation, Digital Care Hub – Chair

Emma Nichols, Consultant, ECN Consulting

Christopher Ede, Care Technologist, Brandon Trust

Alice Dunning, Research Fellow, University of Sheffield

Sam Cattell, Technical Cyber Lead, Digital Care Hub

Katie Thorn

I think we will make a start because we have a lot of amazing content to get through from some of our speakers today. So good afternoon. Welcome. We're here from the Digital Care Hub and our webinar today is all about Everyday Technologies, Hidden Risks Cyber security and data protection when using everyday tech in social care. My name is Katie Thorne. I'm the director of innovation at the Digital Care Hub, and you'll notice my colleague Fiona is also in the chat if you have any issues, please pop a message there and she will come back to you straight away. Some basic housekeeping just before we get started. So this webinar is being recorded. We can't see any of the attendees and you are all on mute. So please put your name and organisation in the chat.

Say hello, provide comments, anything that you're particularly looking forward to getting out of this session And if you have any questions throughout, there's lots and lots of opportunity to ask questions. Please use the Q&A function rather than the chat, just so we don't miss anything. If you're on mobile or on a tablet, you might need to push the three little buttons to get to the Q&A section. We'll share an access to the recording and the presentation. And for anybody with access needs, you will be able to enable closed captions throughout.

And please just let us know in the chat as well if you'd like us to email a copy of the transcript to you after this session, and we can make sure the transcript goes out as well. For anybody who isn't familiar with the Digital Care Hub and who we are and what we do, we're a national not-for-profit and provide free support to adult social care providers on technology, data protection, cyber security. And our focus is working collaboratively with the sector and lots of different organisations to provide knowledge and support to people and to provide peer learning opportunities, which is why we do webinars such as this one. And really brilliant to have expertise from a lot of different people on today. So our agenda today is going to cover Emma Nichols from ECN Consulting, talking about personalised technology assessments.

We'll then have Chris Eid from Brandon Trust, who's talking about real life experiences with using everyday technologies. We'll then have Alice Dunning from University of Sheffield, who has been working on an academic project looking at everyday technology for people with learning disabilities. And then finally, my colleague Sam, who is sometimes known as Cyber Sam, is going to give some top tips and things to think about from a cyber security perspective if you are using everyday tech as part of your service. And plenty of time at the end as well for Q&A. Just to set the scene really briefly before we go over to our speakers for today, I think we're all familiar on this call that there has been a large priority around digitisation across adult social care for the last decade.

A lot of this is really focused on, sort of, operational technologies when we're talking about care homes, home care, and supported living, so things like digital care records, rostering, medication. But the reality is, we know that more and more people are purchasing technology themselves off the shelf, or also commissioners are increasingly looking at sort of everyday and consumer technologies, as well as specialised care technologies to support people to live independently for longer. So we might see things like, for example, Alexas are being used really widely across the adult social care space. I recently got to go to Madrid this year where Spanish Red Cross have rolled out nearly 100,000 Alexas across their entire estate to support people. And to kind of fill some of the gaps between care visits, which has been an amazing project, which they're working on there.

We know more and more people are using Ring doorbells, especially around safety, particularly people who are living with dementia, potentially, and who may wander or leave doors open. Families are finding this really reassuring. And also smart watches as they get increasingly good in terms of their ability to record biometrics and falls and that sort of thing are sometimes being relied on by individuals and by their families rather than more specialised medical technologies because sometimes people just think they look cooler or they look nicer or less medicalised and they have the functionality that they wish. So that's the reality that all of us are working in.

But that also then has unique risks when we're not talking about specialised medical devices or technologies which have been specifically designed for social care. We might

have to think through some complexities around people's consent to have the data shared from these devices, or consent to use these kind of technologies. Data protection becomes quite an interesting thing to think about in terms of who's the data controller on an Alexa device, for example, if you're a care organisation or a commissioner who's purchased that behalf of somebody who's receiving support in the community. And also a variety of, sort of, horrifying cyber security considerations, which I'm sure Sam will make less scary in his talk at the end. That's my hope, anyway. But really, I think we need to focus on the benefits of this and why getting it right is important.

And so Emma, who's one of our speakers later today, has provided this really short video just to really highlight sort of some of the opportunities around everyday tech and care My Alexa, isn't it? Oh, she is lovely. What do you ask her? The weather. Time? A time. All that sort of thing And do you ask for songs sometimes? Yes. How do you use it? What do you have to say? Alexa Do you know what the time is, please? It's 5:28 p. m. So a lot of our speakers today are focusing on more working-age adult services with learning disabilities, but I did want to be clear as well that for those of you who are working more in older adult spaces, there is a lot of crossover as well in the technologies which are being used. So please don't feel like this is not a webinar for you. But without any further ado, I think we will move on to Emma to give her first presentation. Thanks so much, Emma.

Emma Nichols

Thank you, Katie. Good afternoon, everybody. Yep, so my name is Emma and I'm an independent consultant supporting organisations in the implementation and sustainability of care technology. So for the majority of my career prior to that, I worked for a large support provider for adults with learning disabilities called HFT and for about 20 of those years, I led personalised technology service or their care technology service. So today we're going to be sharing some of those lessons that I've learned along the way And also, I guess to say as well, when I first started doing this work, there was very little choice in the mainstream market in terms of technology, but today it does look really different.

So I've seen over the last few years quite a lot of change, and it's great that people have got choice now In terms of, you know, being able to buy, buy things off the shelf and even for themselves, but there's just some key things that we just need to think about in order to support them to make those informed choices, so the technology supports them in the right way, really. So So I'm not going to go through a lot of this in detail. If you have not got anywhere near enough time today. But this is the model that I follow and how I approach sort of embed it within my work really. And you'll see that it's a circular model, so it's an ongoing process in terms of as people's needs change, the technology might need to change. So you need to be going back and revisiting. And it doesn't matter whether it's mainstream or specialist technology.

It doesn't matter what the condition is that the person has, it's really about the person and what they need. So today I'm just going to be talking about the assessment and the sort of

solution selection. And if we have time, maybe a little bit around consent and the policy, well, definitely around consent But also maybe a bit about policy and practice as well. The other thing just to say, actually, you'll see around the outside that the consent tech awareness training, culture change and policy and practice are sort of running. They're sort of a thread that runs through this whole process. So they're certainly Not a one stage, you know, one step action. So what does it take to implement technology well? It's really important that we have at the forefront of our mind. It's about the person, it's not about the technology.

So as I go through this, I'm going to be talking more generally, but I just wanted to introduce you to Sam, who's a fictitious person, one of our goals is to answer our own front door, but she gets very anxious. She lacks confidence, and she also has some mobility issues as well. And a smart doorbell is one possible solution for Sam, but it needs to be assessed, selected and implemented appropriately. So as I go through, I'm just going to be sort of linking things back to this just so it makes it a bit more real really So the first thing really is To understand the person. It has to be person-centred. So what matters to Sam? What are Sam's goals? What are our aspirations? We need to be taking that strength-based approach. So what can Sam already do? So it might be in terms of the smart doorbell, goal that she has, that she's already able to operate a tablet device.

So actually, maybe we could build on that and look at how we can hone on those skills to support her to answer her door We need to be making that... taking that holistic approach, so looking at all areas of Sam's life, at home, out in the community, at work, and within education, wherever she spends, you know, her life, and the important parts of her life as well As well as the least that's the things that she sees less important, I guess, because we need to be looking at what support she needs as well around that, and what, you know, what... where her... where are the risks? Where are the barriers that Sam faces in her life? So For example, at the moment, one of her barriers is answering her front door and she's really sort of finds that really difficult and is that about hearing the door? Is it about the fact that she's unsure or feels unsafe, or she's anxious?

So really looking at those barriers And also the risks. So, you know, there may be a variety of risks that Sam faces in her life, but for this specific example, it could be that she's at risk of falling if she rushes to the door. So thinking around all of those sides of things as well And it has to be co-produced. So Sam's obviously at the centre of this, but we need to be involving family advocates and the staff that know her best so that we can really build up a really clear picture. And it also needs to be outcomes focused as well. So for Sam, she wants to feel safer. She wants to know who it is at her door, and she wants to be able to feel more confident.

So if we can set those outcomes from the start, we can then revisit and check that we are meeting those outcomes And the other really important thing to say is that sometimes the assessment may show that technology isn't the right solution. And if we are taking that

person-centred approach, then that is absolutely okay, and it should be, you know, technology is not a solution for everything. It's simply just a tool to enhance somebody's life and their support. So, So just in terms of choosing the right solution, we need to make sure that it's accessible for Sam. Is she able to control a smart doorbell, for example, or if it's a smart speaker, is she able to speak Clearly enough to get a response from the smart speaker. I know that I've got multiple smart speakers or Alexas in my house, and they don't... she doesn't always answer me, or actually do what I ask her to do.

So we need to be really careful about setting people up for success. We need to be making sure it's reliable and that it's affordable. And also that the connectivity, the connectivity is strong enough. So at Sam's front door, are we... is this... is the Wi-Fi strength strong enough there? And also about compatibility as well. So thinking about if we got a toolkit of ideas for tech for Sam, will they talk to each other where they need to? Would Sam's smart doorbell link to an Alexa, or if we're thinking about using an Alexa to support it, do they talk to each other? And we also need to be thinking about when we set up What the tech support is like. So with the mainstream technologies, this can be quite an issue because their main customer base is general consumer.

They're not used to offering us sort of a more robust tech support for vulnerable people And you might end up talking to a chat box, which for a lot of people is a real barrier. And we need to be setting realistic expectations as well. So maybe phasing the technology over time and giving people enough time to be able to learn how to use it and not overwhelming people with too much technology all at once. Obviously, it needs to be personalised, and if we're, you know, we're looking back at that assessment and get, you know, that person at the centre, we need to make sure that the solutions are personalised to them, that they're set up in the right way. I think one of the other the sort of key things to think about as well when we are thinking about these more mainstream technologies is how people are going to set up accounts.

How are they going to, you know, do they already have an Amazon account, for example? Have they got means of remembering their password and all of those things need to be considered because I know when I've forgotten my password, it can be really frustrating, but also quite difficult to gain access and things like that. So we just need to be really thinking through all of those things, not just about the actual device, but those things in the background as well in order to the setup and the sort of continued use of it. And we also need to be thinking about restrictions. So we need to be using technology to support people taking the least restrictive approach, but we also need to be thinking about if we're putting in, so for example, a smart doorbell Installing that into a supported living service.

And there's video and motion alerts set up on it, which would need to be need to be for Sam to be able to see who's at her door and be able to communicate with them If staff support staff start using that to monitor and see when Sam's coming and going and potentially then maybe, you know, restricting her from going, that could or confronting her

and saying, you know, about her leaving and all the rest of it, that would be a restriction. So we just need to be really careful that when we put technology in, that we are not then creating we're using it to create independence, but actually is it creating an additional restriction as such? So just thinking about all of these scenarios and it doesn't have to be complicated, it's just really about The planning and sort of thinking about all of those things at the start.

Just in terms of consent, of course, involving the person absolutely as much as possible throughout the whole process. And you'll remember it's an ongoing goes round that circular model. It's a thread throughout We also need to be supporting staff and family to understand the technology so they can then support the individual to make informed choices about the technology. And sometimes that can be quite, quite difficult in terms of asking people to understand about data protection and privacy and things like that.

So we need to be providing that and accessible communication in accessible way for people to understand as much as possible, as well as, you know, you'll all, you know, I'm not trying to, you know, you all know about capacity and things like that, but if the person doesn't have capacity, then you'll obviously need to be looking at best interest, decisions We absolutely need to be thinking about privacy and data sharing. And there may be a data privacy impact assessment might be required. So, for example, if somebody is needing a... wanting to use a smartwatch and their health and their location information's being shared. We need to be really thinking about that and thinking about, you know, what... how that's implemented. And also, you know, about the sort of privacy side. So with Sam's situation, with the smart doorbell, If where's that video recording if it's...

if we are paying for the recording service, where is that being stored? Who has access to it? Is Sam happy with that? And also the impact on others. So it's obviously going to be monitoring maybe other people coming and going from the property, other housemates as well. So we just need to be thinking about all of these things And you might actually need consent from landlords and definitely other housemates if there's a technology in there that's going to have an impact on them. So we need to be thinking about all of these scenarios, not just about the person, but the impact on other people around them. And it needs to be ongoing review as well. It's not just a one-off step.

Just really briefly in terms of implementation, we just need to be clear that this is all recorded implemented in support plans and risk assessments and doing your regular technology health checks if it's a factory operated device, checking that that's working, if it needs charging, all of these things, and also building it into existing policies and procedures as well And also making sure that the guidance is there in an accessible way for the individual. So we need to be thinking about who sets up the device and supports its use on a day-to-day basis, what happens if it fails, what are those, you know, mitigations that you put in place? How are risks managed and who reviews it as well. So, yeah, lots of

things to consider. And just very briefly in terms of sort of reviewing the outcome, we need to be making sure that we're reviewing that. Does the person want it?

You know, we don't know until we try sometimes, and actually they might absolutely hate it. They might hate the smart speaker talking to them in their house So we need to be, you know, we need to be checking in. Is it being used appropriately? We talked about those restrictions earlier. Is the person using it in a way that's, you know, supporting their independence, or do they need a bit more training Is it meeting their need and what outcomes have been achieved? And we just need to be really clear that success isn't installing the technology, it's making a meaningful difference to someone's life. And you remember that strap line at the beginning, it's not about... it's not It's not about the technology, it's about the person, and we just need to be really, really focused on that throughout the whole process. So that is

Katie Thorn

Over to Christopher now Thanks, Emma. That was absolutely fantastic. And it's actually just a comment come through as well in the chat from Jackie who said that This would be really, really great information for unpaid carers to hear as well. So which I think it's true, and I think your comments about how it's about the broader impact, and sort of not just the one individual or the one care service or the one commissioner, but how this interacts with everybody who's involved is really important

Emma Nichols

Yeah, I think it's well just to add on that really briefly is that's some of those stages in that process are very much sort of care provider, but actually focus for the care provider, but actually they're really important if somebody lives at home as well with their family around the assessment Checking in with them and making sure it is meeting their needs and things. So, yeah.

Katie Thorn

Great point. Thank you. Thank you so much. So yes, I will pass now to Chris, who is a care technologist, which if anybody isn't familiar with that role, I hope you do familiarize yourselves with it because it's very interesting. And Chris, over to you.

Chris Ede

Thank you. Hi, yeah, my name is Chris. I work for the Brandon Trust as a care technologist. A little bit of background, I was a support worker for the Brandon Trust who moved into line management. I was managing a few houses in the Gloucester and Forest of Dean area When I was initially I was presented with an opportunity to join our digital champions group, which was just a group of volunteers who met to talk all things digital techie within the trust. And from that came the opportunity to do care technology training And I quite like training, so I said yes, and I took it up, and as a result of that, I was asked to do care technology one day a week, and then keep doing my job four days a week, and that quickly

changed to two days a week, and that quickly changed to three days a week And then it was, could you please do this five days a week?

We need more than one person, but unfortunately, budgets are a thing, and they... it was one person, that's what they went with. So I've been doing that. That sort of took place between April and June of this year, and I've been doing it four times since July. A lot of what I've been doing is setting up the sort of foundations for this job to really kick on in the coming months. So getting familiar with procedures, with practices, GDPR law, which I'm going to sort of touch on a massive thing, especially in supported living And also building a knowledge base of what's out there. I echo what Emma said earlier about it being about the person, not the technology.

But I felt I needed to get a more in-depth sort of view on what's out there, just so I could go into each case arms a bit more So during this time, I had a lot of demos, a lot of people trying to sell me their wares, and sort of, get trials off the ground. A lot of people very keen to give tech to trials, and you've got to slow them down a lot One of the first things I was shown was a smart speaker It's, not one of the biggies, but it's a decent sized company. They wanted to move into the supported living world, and they felt they tailored some software towards that I had a few concerns, and I initially, I said I'm not sure the impact is worth a risk, so Probably not right now. What they actually come back with, we'll give you one, pull it in your house And we think that's going to win you over. So I said, why not? I'll go along with that. And they weren't far wrong to begin with.

I fell in love with it. It was and it is an amazing bit of kit But it's probably four or five weeks in, I was working from home And another little bit of background, I've got 3 teenage daughters. So working from home in the school holidays with three teenage daughters always goes smoothly, never a problem. They never ever fight, they never ever get in the way. They're brilliant. But the one day, I was at my desk, where I had this speaker And I look to my right, I could see them a hallway. And my teenage daughter came out and she had her phone and she was, she had the camera open and she was sort of looking at herself like that And it sort of went on and it went on and it went on. And after about a minute, I stood up and I looked down to her and she looked, that got her attention. She looked at me And she said, well, I love myself. Which...

I hope there's a little bit of dry humor in there, but I'm not convinced. And what happened then, this smart speaker woke up And it said, oh, Christopher, that's great that you love yourself. Self-love is very important, and it sort of went on and tried to engage me in a conversation. Now, I'd been assured the only way to wake up this smart speaker was by saying two distinct words And outside of that, it does not listen or process to anything that is said. Those words weren't said. This other person wasn't in the same room as me. She's 20-ish years younger than me.

And does not seem like me, but it woke it up and it thought it was me and it had processed exactly what has been said, because it was then trying to engage me in a conversation And interestingly, when I told it that I didn't say that Just went very quiet and it didn't, it stopped engaging with me when it is, sort of, the highlights of this particular speaker is, at the end of the day, it gives you a rundown of your day. So, and that can be tailored to the individual. It can include medication, it can include general well-being, it can include hobbies, weather, anything you want it to And it put it in there, so it put in Christopher told me today that he loves himself So it retained it and it had put it in there. Now, in this instance No harm, no fail, it was just me at home. It thought I had a better opinion of myself than what I do. So it wasn't the end of the world.

But had we put that into a supported living setting and had that been my housemates down the corridor who had told me they told their support worker they'd just taken their medication And it woke up and assumed that I had taken my medication And medication was a sort of inbuilt software part of this, where it would engage with you around your medication, so it would almost fill in a MAR chart for you as well. So, if I woke it up and said, I'd take my medication, it would do a MAR chart, it could text family members, it could text support workers to say Christopher is taking his medication That would have been a false alert, that would have all been false information. Moreover than that, if I had then If I had then to try to tell it I've taken my medication.

One of the inbuilt safety features is actually it will warn me that I'm about to overdose Now, in this situation, that wouldn't have been true. It can trigger 111 calls, 999 calls, calls the family, calls to support workers to warn them that I'm potentially in danger However, I would have been in no danger at all. Obviously, there's a lot of sensitive data spoken about in supported living settings, especially from an individual point of view and an organisational point of view So This is something I've always been hyper-aware of, devices listening in, because we know devices have the capability to listen in. Any smart device has that capability. So when I come to do my risk assessment, that then became a big risk that I was no longer aware of. I spoke to the company and they were honestly said, we think it's a bug that shouldn't have happened. And I believe them.

I honestly believe them, but it did happen it did process that data, it did keep that data, and it used that data. So when I come to do my risk assessment I was unsure... when I got to the mitigating section Hope it doesn't happen again. Just Cross my fingers. There's not a lot I can do, I'm not in control of it. I'm not in control of that aspect of the support. So I felt very uneasy around putting this into anybody's house that we support. And in fact, I haven't, because to me, it was too big of a risk. The fact that it shouldn't have happened and did happen was actually more worrying to me than if they'd have held their hands told me, well, not the truth I honestly believe that was the truth So yeah, that was very real incident that had no bearings on anything, but could have Which brings me on to my second example.

And that is we did find a smart speaker that we put through its paces and we thought is all right to go for a trial into people's houses, the people we support. We went about that. We did the processes, best interest work where needed, but a lot of it was people with capacity who could consent to... as I think the troll should be. Two months went by all positive feedback. There was... nobody wasn't enjoying their smart speaker. It was adding independence to people's lives, it was... it was giving people, companionship It was just making a lot of people, their lives better, even if it was a small amount, it was having a positive impact I had a call from the person who I've been liaising with at the company who Was told me there was a software update coming. And she was very excited, giddy with excitement about this software update because it was going to bring the smart speaker to life.

It was going to give personality, the cadence was going to improve. You could choose accents. The knowledge base was going to increase It was a lot of things were going to come from this update and she, yeah, she was really, really excited about this. And then towards the end of the call, she just mentions the company were taking over the software And a few alarm bars weren't ringing, because I thought I'd seen in the news that this company had issues on a data level. So I immediately called my data protection officer, who told me that device will no longer be GDPR compliant Now, should that update happen, and should that company take control of the software?

Now, we're talking about hidden risks This was a risk that wasn't just hidden, it wasn't there I did my risk assessments I did my best practice, I did best interest work, and it flew through all But something changed after it went into people's houses. And I think that speaks to we need to reassess. It's not just about risk assessing, it's about re-risk assessing constantly, going back, especially with tech-enabled care, because we have It has that ability to change on you for things to be added in, taken away. And that's something that we can't rest on.

We need to be hyper aware of it Especially around devices that have got this capability for my money I've only got a few minutes left, so I'm going to skip over to talking from a colleague point of view, and I'm going to go with the biggie, WhatsApp Now, I I'll use WhatsApp in my personal life is imagine most people do in the work arena, I absolutely detest WhatsApp. I do my best when I was team leading, I was doing my best to not have WhatsApp groups And, to keep things on the email and our rostering system's got a messaging system. So I wanted to keep it there and just two weeks ago, an example of something that happened came up. In one of my houses that I left, I'm mentoring the person who's coming to manage it.

First thing they did was set up a WhatsApp group First thing all I did was say, I think this is Bad idea, but it's their management, their time, so they did it A few bit of time went by and then we got to a message come through. I was leaving the office actually and I just happened to be looking at my phone. Message came through. I think I'll change your

name. I think Jenny's medication's wrong. It was from support worker And then came through a picture of the blister pack And it's I think, you know, there's an extra pill here. The blister pack was placed on a table just below the blister pack was the top and a MAR chart. Which contained name, address, date of birth, NHS number, GP All of that sensitive information, and with all the best will in the world, this person was not trying to expose that.

They were trying to help and they were trying to get this person's medications right And they accidentally put that there just so happen. I, like I say, I saw it pop up, and I was able to delete it very quickly. But one of the features inbuilt to WhatsApp. It downloads pictures straight away. So for the 12 members in that group, they would have got that picture to their phones, and I know Android quite a lot. They sync with Google That gallery could have synced with Google, uploaded that image to the cloud. All without anybody actually opening their phone. The staff members didn't have to actually even look at their phone for all of this to happen automatically. So That just why I really, really do not like WhatsApp in the work environment at all. I think you need your own, whether it be email, or whether it be through your rostering system You need Something that is GDPR compliant.

I know our digital care records has a messaging system on there, and it's locked down, it's on only available on work devices, you need MFA to get onto it, it's fully locked in And those are the type of messaging services that we should be using for my money, and it keeps everybody safe and secure. Not to mention the people we support, but also our colleagues, who wants to be the subject of a data leak You know, especially if it wasn't even intentional, if that person didn't do anything towards it, but that data came from their device, it's not a good position to be putting people in. And I think that's roughly my time.

Katie Thorn

Thank you so much for that, Chris. Really, really good examples and illustrations. I mean, for one, I admire the confidence of your teenage daughter and wish I think I had that same level of confidence. I think, you know, all of your examples really resonated. There's people who have been commenting the chat about sort So if they're surprised about there not being devices being able to listen without hearing a wake word, about how updates can affect GDPR. I think these are just things that there's so much to think about when talking about technology, and so unless you hear examples like these, they might not be things which are on your radar. So Yeah. Really appreciate you sharing. I mean, I know we talk as a team at Digital Care Hub a lot as well about WhatsApp, particularly the automatic image download, because also

Chris Ede

Yeah.

Katie Thorn

Their staff using their own personal phones, you don't know who else has access to their phone, if they're really happy to, like, hand over that phone to, like, a friend or to kids and that sort of stuff, and those kind of risks can be really hard to mitigate.

Chris Ede

Yeah, I mean, even just being on public transport and opening up your messages, you know, it's so easy to unintentionally share data.

Katie Thorn

Oh yeah, absolutely. We've all definitely, I'm sure, sat next to somebody on a bus or a train who's got a very interesting text message going on like next to you. I should cover that really. Thank you so much. Anyway, so we will then pass to Alice Dunning who is going to talk all about sort of building moral and ethical frameworks for this kind of technology.

Alice Dunning

Brilliant. Thank you so much, Katie. Those have been two amazing presentations. So yeah, my name's Alice. I'm a research fellow based at the University of Sheffield. Today, I'm going to talk a bit about our work on using mainstream technology with people with learning disabilities. Particularly, I'm going to talk about our moral, ethical and legal framework, and the kind of considerations that arise from using this technology. So, TechLD is a two-year project that's co-led by myself and Professor Liz Crewt, and we're interested, as this webinar is about, in everyday and mainstream technology, so those things that many of us use regularly. We know, obviously, from these presentations that these technologies are already being used by and for people with learning disabilities. And we know that they weren't necessarily designed with their needs in mind.

So our starting point really is that technology adoption is happening faster than the evidence, so there's still really important gaps in our understanding about privacy, surveillance, consent, data ownership, and algorithmic bias. So the Tech LD project has three main questions. We want to know what are the technologies that are being used? What are they being used for, and what are those moral, ethical and legal considerations in using them? So we've been going for kind of over a year now. So far, we've conducted a participatory scoping review of 38 sources. So that's kind of academic and grey literature. We've also focused on policy and included legal cases and legal documents. We've also developed and refined, like I said, this framework which we use kind of existing information and existing frameworks and evidence and co-design with our knowledge user network.

So this knowledge user network is really central to the project. It comprises of 3 groups. So adults with learning disabilities, family carers and support providers, and they've been really engaged with the project throughout. Just to ensure that our work really reflects that lived experience. We've used this framework as a lens for analysing our review. So to help

us identify really those tensions between people's rights, professional responsibilities, practical concerns about different technologies. I think just before I talk more about the project, it's really important to say that the project is not about restricting technology. We really want it to be about supporting people to make informed choices about how they use it. So, in terms of the policy landscape, so I'll look at...

I'm going to talk very, very briefly about this, but I'll look at, kind of, national and local policy, highlighted attention between the really positive ambitions for technology, and then those realities of using it in social care. So National policy tends to position technology as a way to promote independence, choice, control, and efficiency. And we see these ambitions also appear in some of the local authority strategies. But kind of those local authority policies or strategies were really fragment fragmented, varied, and very non-specific. So there's much less attention to the specific support that people with learning disabilities may need to access and use everyday technology meaningfully. We found tensions between protecting people from harm and supporting their autonomy and inclusion.

So discussions in the policies about vulnerability and capacity can sometimes kind of reinforce those assumptions about what people can and can't do So I think for providers, the practical issue is that positive policy ambitions don't automatically translate into accessible technology, trained staff, or ongoing support. I think it's really important that we need to be careful not to assume that everybody already owns a suitable device or that they have the skills to use it. So our scoping review identified kind of broad areas of use of these technologies. So they can be really great in terms of connection and identity.

So tech like WhatsApp, video platforms, social media can help people with learning disabilities maintain relationships, develop friendships and express their identities It can be great for, kind of, daily routines and independence, so smart devices can provide reminders for appointments, medication, travel, and household tasks. Participation and safety, so GPS tools and sensors can support navigation provide reassurance, and then you have kind of tablets and emerging AI tools that can support learning and access to information. It's also examples that include a kind of music and relaxation tools for entertainment and online communities or dating spaces For exploring identity and relationships. So, we know that technology can therefore support social participation as well as those practical tasks.

But we know that those benefits come with potential risks, so that can be surveillance, privacy concerns, or online harm. So, one thing that our review really showed was that access did not equal digital inclusion. So, providing a device is only the starting point, really. People also need, kind of, accessible interfaces, ongoing digital skills support, and opportunity to make their own choices And I think it's this idea that Independence doesn't have to mean doing everything alone. The right support can be what makes independence possible. So, to explore these issues, we developed a moral, ethical, and legal framework,

and this is organised into seven domains. And we try and distinguish between three related concepts, so we think about the moral, the ethical, and the legal. So moral is around our personal values and conscious. So what do I believe is right?

Ethical is thinking about those professional responsibilities. So what should I be doing as a professional And then legal questions are around kind of rights, legislation and statutory obligations. So what does the law require I'm going to talk a little bit more about the domains kind of coming up But I think this framework is really there to kind of help make those tensions visible. So particularly that tension between keeping someone safe and respecting their right to make choices. And the idea is that kind of as we've heard from these previous examples, there can be things that come up with technology that maybe we wouldn't have thought about And what we want to do from this framework is just have a way of identifying and, I guess, kind of provoking thoughts and conversations about what these possible risks or possible considerations might be when introducing or using this technology.

So, kind of going forward in the project, we'll really hope to use our framework to help adults with learning disabilities, their families, and support providers to have better conversations about technology. So conversations that recognise both its benefits and its risks, and really keep the individual person at the centre of those conversations. So the first domain that I'm going to talk about is privacy. So our review found that the desire to protect people from online risks could sometimes overshadow their rights to privacy, expression and online independence. So, for example, supporters might restrict access to consent or monitor online activity Because they were concerned about harm, but often these kind of blanket restrictions could undermine autonomy and potentially someone's human right.

At the same time, people might need support to understand privacy settings, recognise the risks and protect their personal information. So one example from our knowledge user discussions with people with learning disabilities was the difficulty of accessing online banking and online services because of kind of complex passwords and verification processes. So they were talking about how, you know, I have to give my auntie my online banking password Just so that I can access it. So, you know, people are sharing login details just to be able to access their own accounts. Some people may knowingly trade their privacy, so those studies that show that people with learning disabilities were kind of happily trading in their privacy in order to build and maintain relationships with people online.

So support should really help them understand the risks and available protections that they can have while respecting their choices as far as possible. So there's really this challenge to enable informed choices and manage risks without defaulting to unnecessary monitoring or restriction. So the second domain is liability. We found that concerns about being blamed if something went wrong could lead to supporters

restricting internet access or removing devices altogether. This is really understandable in a context where providers have safeguarding responsibilities. But fear of liability can unintentionally limit people's opportunities to develop digital skills and confidence. Staff training and confidence are really important here, so where support workers are unsure about how technology works, or how to manage the risks, restricting access would feel the safest.

So, in one study, it showed that around quarter of the staff received no training whatsoever around technology. So kind of clear guidance on clear guidance can really help staff manage the risk without having to rely on kind of blanket restrictions. And our knowledge users really describe the importance of having a positive approach to risk, so we had a family carer talk about their son, kind of, using Google Maps to try and navigate independently, and they got lost, and rather than kind of stopping them from using that. She treated it as an opportunity to learn, and we're saying, you know, it's actually... it's okay to make mistakes. The third domain is transparency and explainability. So people need to understand what technology does, what information it collects, and how it is used, and what those potential risks are.

Our findings suggest that both inaccessible technology information and limited staff confidence can really make this difficult. So we had an example, again, from family carers who spent kind of over a year working towards their son giving informed consent to having an app that would track their location. So they found that kind of standard written explanations about what the app was and what it did just weren't enough. Genuine understanding about it was developed when the family created visual cartoons together to show how and what the app would be used for. So I think for providers, this means using accessible formats, demonstrations, easy read materials, hands-on learning. And it also means that recognising that understanding may develop over time and that the format should really depend on that person. So the fourth domain is relationships.

So mainstream technology can create valuable opportunities for friendships, romantic relationships, peer support and self-expression. Online spaces can allow people to explore their identities and build confidence in ways that may feel more comfortable than those face-to-face interactions. But people might need support to recognise deception, understand online intentions, and navigate potentially harmful relationships. Online relationships can provide that gradual route to meeting a person in person. However, some people in the review, kind of in some of the studies reported that online interaction did not reduce loneliness and could intensify those feelings of isolation. So I think that highlights. Kind of the impact of this digital space really depends on the person and their wider support rather than the kind of software or the platform itself.

We also found concerns about technology being used as a substitute or replacement for human support. So, you know, as we've spoken a lot about smart speakers being used to support routines and reduce feelings of loneliness, but they cannot replace that

meaningful human interaction And our provider knowledge users really highlighted the pressure that some of them were feeling from their local authorities. This kind of push to use technology to improve efficiency where funding was limited and they were really strong on the fact that technology should be there to complement relationships and support Not as a substitute for them The fifth domain is equality, so our findings highlighted several barriers to digital inclusion, including device costs, inaccessible interfaces, complex systems, and limited access to support.

So people may also experience exclusion where supporters restrict technology because of their own concerns about the risk. So one of the adults with a learning disability in our knowledge-user network described the impact of not receiving supporters You know, when you ask for help but you don't get it, you feel really trapped Digital exclusion isn't just about missing out on technology. It can mean missing out on relationships, information, community participation and opportunities for self-expression. People can also be excluded when they have a device, but no help to use it, or maybe, you know, they exclude themselves because they feel that the technology is difficult or unsafe. So inclusion really depends on confidence, accessible information, and practical support, as well as access to that device.

So for providers, digital exclusion should really be treated as an important part of support rather than an optional extra. And it means considering what access the individual has, what barriers they might face, and what practical support would help them participate. The sixth domain is sustainability. So technology can help people develop independence and may support services facing workforce and financial pressures. But buying devices doesn't guarantee that they will be used effectively or sustainably So again, in knowledge-user network, we took to providers who were talking about during the pandemic, you know, lots of smart speakers and other devices were handed out through short-term funding. These are now kind of in drawers and not being used because there was an ongoing funding to support, kind of.

Support around using the device, maintenance, replacement, software updates, staff training, so they just went unused. I think this really illustrates that difference between introducing technology and embedding it successfully into people's lives Sustainable digital inclusion requires that investment in the people around the technology, not just the hardware. So it's important that we consider the ongoing costs, staff confidence, troubleshooting, accessibility, and really what happens when a device fails. The final domain is personalization. So, technology needs to reflect the individual's preferences, interests, communication needs and goals. This is really around that kind of first presentation that we heard.

The review found that decisions about technology can sometimes be driven more by a supporter's confidence or their perception of the risk than by what the individual actually wants. Effective digital learning is usually ongoing, practical and delivered at the person's

own pace by somebody that they trust So, for example, online safety support is likely to be more meaningful when it relates to somebody's actual interests and the situations that they encounter, rather than kind of relying on generic warnings or generic conversations about that risk. The same technology will not suit everyone and support needs may change as people gain experience. So arrangements should be reviewed with the person rather than assuming one decision will remain right indefinitely.

So, this personalization means working with the individual to plan and decide how and what technology would be useful or suitable for their life. So I've pulled some kind of initial takeaway messages from this. So first, it's really important to start with the person, their wishes and their needs work with them to understand what they want to achieve, or how they want to use the technology, and what support they might need to be able to do this It's really important to take a positive approach to risk, discuss risks and safety strategies rather than automatically restricting access or removing devices. Making support accessible, so explaining privacy, consent, and online safety using formats that work for that individual. Building skills and confidence over time, so digital inclusion requires ongoing learning, not kind of a one-off introduction to a device.

It's really important to review restrictive practices, so ask whether monitoring and restrictions are necessary, proportionate and respectful of that person's rights. And finally, investing in staff is key, so support workers need training, time, and clear organisational guidance to support technology use confidently and safely and safely. So ultimately the aim is to help people use technologies in ways that reflect their own priorities while ensuring that the risks are understood and managed appropriately. So that's an incredibly kind of broad overview and whistle-stop tour of some of the initial things that we've been doing in the project, but I'd be kind of happy to talk to anyone about these in more detail. Kind of, I'll have my email... I'll add my email into the chat. Can I have the? But I'd just like to finish and basically plug the next...

the kind of current bit of the project that we're working on that you may or may have not have seen But we're currently doing a survey of support providers, family carers, and people with learning disabilities, where we want to hear about kind of their experiences of using technology, the benefits and the challenges. So there's a QR code there to the provider survey, and I'll add a link to it in the chat What's really great about this survey is you can answer via voice notes. You don't need to, like, type away, you can just record your answers. So yeah, it shouldn't take too long. You can also do it over the phone with me if you'd rather and kind of anything that you share with us will help us to understand more about people's experiences with technology, and we'll contribute to the next stage of the research which will be to co-produce some form of information and decision-making tool.

So, I'll pop that link in the chat and my email, and then I'm happy to kind of send people the links to the other surveys or talk about the research in more detail if they would prefer. Thank you so much.

Katie Thorn

That's amazing. Thank you so much, Alice. And I've also just popped the QR code into the chat as well. If anybody missed it while it's up on the slides, wanted to make sure that people did have access to it and obviously we'll circulate that in the slides as well. We do have questions coming through, but I think they're probably better for the panel, so I'll move to Sam next, and then we'll bring those all back in. So Sam's going to talk about his cyber experience and the things that you can be doing practically to sort of avoid some of the pitfalls that you've been touched on today, both in terms of where it's an organisation purchasing technology, but also lots of people who draw on care and support purchase their own technologies, which may also have its own risks as well. So Sam, over to you.

Sam Cattell

Thank you so much. So I think this is the first time we'll be using... well, I'll be using Poll's Zoom polls to go through some quick scenarios. So just a little bit of interactivity for 10 minutes. It's on the screen there. It's going to be a quick scenario that I've set up Pick an answer you think's right, and then we're going to discuss it as here together, but I can't see or hear you, so I'll discuss it, and then we might discuss it as a panel, or if you have any questions, put it together like that. So if we can go to our first scenario, please There we go. Oh, there we go, it's popped up for me as well. That's brilliant. So, two care workers are having a conversation outside someone's home, discussing their next visit and some details about the person they're supporting.

Unbeknownst to them, it took me a while to spell unbeknownst, the property smart doorbell has recorded their conversations. A few days later, a family member uses footage from the same doorbell to challenge whether a scheduled care visit actually took place. And based on the video's timestamp, which of the following should you consider? Smart doorbells only record when someone presses a button If the timestamp says a visit didn't happen, the footage is definite proof. Smart doorbells can capture conversations without people realising, and timestamps aren't always reliable or smart doorbells only record clear images and audio during light daylight hours. So if you could select one of those for me, please, which one you think it probably is. And then we'll go through it together.

Sadly, fellow panellists, I'm afraid you can't take part in the poll, but if you would like to, please do just message us on Zoom and we'll add you to the totals.

Alice Dunning

I was just trying to click it then, and I was like, oh, it's just like a screenshot to me.

Sam Cattell

Yeah, yeah, sorry, no functionality for you guys, just for the people who are attending today. Okay, this will only be about 6 minutes or so, then I'll discuss about them and then we'll go through some tips and tricks. Tips and tricks. of Cyber which you want to have already been covered mostly by Christopher, Alice, Emma and stuff like that, which has

been fantastic, so I can link back to what they've said. Should we have a quick look that people have put

Katie Thorn

That's an option

Sam Cattell

Sorry, so I'm getting there. I think that that should show now. Can everyone see the final Results

Katie Thorn

Showing for you Nope. There is for me. Would you like me to take you through the answers, Sam?

Sam Cattell

It should be showing. Good. You go through, Katie, that makes sense.

Katie Thorn

And then you can then, I don't know if these are the right answers or not. So for A, smart doorbells only record when someone presses the button. Only 3%, 3% as well for B, 93% for C, smart doorbells can capture conversations without people realizing Yes And nobody went for D the daylight hours one

Sam Cattell

Yeah, a lot of doorbells now have nighttime modes and all sorts of stuff. So yeah, fantastic. You all got that one as a good warm-up. Yes, absolutely, smart doorbells can capture conversations without you realizing they don't always light up, they don't always give you an indication There's not always a warning outside to say that being recorded, but yeah, absolutely, if there's a smart doorbell, it can hear you when you're nearby. In fact, so if we go

Katie Thorn

Sam, can you also share with us, because you told me a really useful insight, which I didn't know about the changing of metadata at the back end of footage

Sam Cattell

Yeah, oh yeah, that was part of it, I forgot about that. So yes, this is a real things that have happened in the past, especially when I worked in the police, is that metadata is just the name of the stuff that you don't really see. So, on photographs, on videos, things that are captured like that, it'll have date, time. Where it was, the place, maybe a name of a user, all sorts of stuff. That stuff can actually be changed before being exported, or as part of being exported. So I could change the time to lie, basically, to say, well, you said that you're going to turn up at 3 o'clock and look at my video camera at 3 o'clock, there's nobody there All I've actually done is change it an hour later or an hour earlier, but the data

looks like I'm telling the truth, but it's easy enough to manipulate, unfortunately. So you can't always rely on it.

If it ever went to court, touch wood, it wouldn't ever go that far. You would get somebody like me to look through it and be able to prove that one way or the other, but it's just something to be aware of that just because somebody says, look at the data, that's not necessarily 100% what it's going to be. If we have a quick look at the next scenario. There's only 3 of these guys, don't worry. So a care worker is working somewhere in their visiting someone in their home. The person has a smart speaker in the living room. I see all these have been gone through. This is brilliant. It's almost like I listen to this before I wrote these. Which they use to remind us of music and everyday tasks. During a conversation with... about the person's care needs, the smart speaker suddenly lights up, despite nobody deliberately activating it. What might have happened?

Is it that all smart speakers record every conversation constantly? Is it that a smart speaker may activate unexpectedly and process part of conversation? Is it that smart speakers cannot process anything unless the owner presses a button or says a key word? Or it's probably just charging or updating itself, so don't worry about it.

Judging by the last answers, it's unlikely anybody will push D, but that used to be a thing that things would light up just because you're charging them.

Katie Thorn

Seeing the results come in, Sam, so yeah, you're right, C and D aren't getting any takers right now when we were about 70% of people have taken part, but we do have

That's all.

It seems to have steadied itself. Oh, no, as soon as I said that, more people have put their answers in. So sorry to keep you on Tinder. To be absolutely fair, although

Sam Cattell

I'm saying there's a right answer and a wrong answer, the best thing about working in cyber is that there's very rarely right and wrong. There's more secure, less secure, and the best answer for everything is, it depends. So realistically, you could get some of these as well. But in that case. Nice. Where we've got to then is all smart speakers record every conversation constantly. A, got 13% of the vote and 87% of the vote went for B. I feel Chris's earlier story may have given some of the game away. Yes. Perfect. You gave it away, Chris. You spoiled my little scenario. But yeah, absolutely perfect. Yeah, absolutely. A smart speaker may activate unexpectedly and process parts of conversation.

It could be all sorts of reasons for it. Now, I know what the people, I imagine the people who say they're listening all the time. They have to be to listen for a key word, but that doesn't necessarily get recorded, that's more of a trigger point, but I assume that's what you mean. But yeah, absolutely. It can just turn on, listen, process it, whether it's

somebody else speaking, it can't In fact, I made a note of this while you were talking, Chris. See if I can find my notes quickly I'm still here, don't worry, Sam. I thought I'd close Zoom then, which was really useful as I meant to be speaking to everyone. But yeah, I'm still here. Yeah, good. You disappeared for a bit, but I am still here. Yeah, absolutely. Smart speakers can turn on, turn off stuff like that.

And as you say, they can't always differentiate different people in a household, so if somebody might say something, somebody might have an accent, they can click on, and sometimes they just randomly hear a vibration that sets them off. There's all sorts of things. So, if we go to the final one, which is a big part thing that you said, Chris I said Chris, rather than Christopher. Sorry about that A care worker has joined the unofficial work WhatsApp group. Now, originally, this was used to arrange drinks and social events, but it's gradually become a really convenient way to organize shifts, share updates, sickness, and just generally gossip. The group has been running for years. Some former colleagues are still involved, and some of the numbers in the group are unrecognised. What should concern you most about this?

Is it staff well-being that bullying, harassment, or inappropriate messages could go unnoticed or unreported in unofficial and unmonitored groups Is it shared files, as we were saying earlier, shared photographs, screenshots, documents could automatically save or back up to personal cloud storage, depending on device settings, potentially accessible to family members using the same account. So not even just the same phone, but just the same account In situations like that. Is it who's in the group? Former colleagues and unknown numbers could still receive confidential information, or is it information requests work related WhatsApp messages, even on personal phones may need to be searched and reviewed if someone requests a copy of their personal information i. e. a subject access request. Or could it be the cheating one of E, all of the above?

As our organisation's data protection officer, I feel you put this in specifically to scare me, Sam. So thank you for that one. I did a little bit. That's why everything else was following this one I was like, I'll just put this in for the DPO to sweat over Okay, up to 71% of attendees have participated now, so give it another minute if you like. Fantastic.

Katie Thorn

I think we might be there, in which case, yeah, we're 89% have gone with E, all of the above, Sam.

Sam Cattell

Yes, fantastic, absolutely. The issue with WhatsApp, and there was a question earlier which I know will go into the panel, but very briefly I'll bring it up here. Somebody was asking, well, what other services can you use? The truth is, when it comes to GDPR like services Technically, WhatsApp could be one of them. It's less about the system. It's more

about how the systems are used. You can set up WhatsApp to be safe and secure, but you'd have to have control of everyone's devices. You'd have to set up that backups went on You'd have to set up all sorts of... so technically it's less to do with what system you use and more to do with how it's used and how you configure it. But yeah, absolutely, that was everything. All of the above. So yeah, quick top tips. Risk assess big one across everything It's all right, Leslie. I'm sure you were going to pick the right one.

There are no wrong answers, but that one they were. Top tips, complete your risk assessment, obviously, before introducing technology and review it regularly. These have all been covered by these guys fantastically, but from a side point of view, people first, choice and dignity start with the person, not the technology, value the person's choice, and involve them in decisions, such as co-production Respect the person's privacy and dignity. It's not just a case of like, am I data protecting? Have I followed GDPR? Actually think about what you're saving. As it was said earlier, where's this data going? What you're doing is you're taking somebody's digital sovereignty and giving it to somebody else. Are you giving it to somebody trustworthy Do you know where they're sending that data? That's the kind of thing that you need to start thinking about. Same privacy and consent.

Assess privacy and security risks before use. I would like out Christopher, you had it in your house and it seemed to be okay. And then obviously that happened and it's it's The thing about quality assurance from suppliers is that it's never exhaustive. There's always going to be bugs from suppliers. It's not their fault, it's just it happens. It doesn't matter how much you test a product, there's something you haven't thought about or an issue that you might not have done. So you have to be prepared for that kind of stuff. So consider what information is shared with whom and why. Obviously, secure by design, check privacy settings before use. I said earlier, you can set up WhatsApp and things like that to be secure, but you need to configure it correctly. Probably wouldn't recommend WhatsApp exactly the same reason as Christopher, but that's just the example.

Obviously, change default passwords and control access. Not everybody needs to be an admin. Katie knows this, as I keep chasing everyone in our team, and I'm like, nobody needs admin unless absolutely necessary. Keep devices and software constantly updated. And ongoing, think about it, review risks and help staff manage them, plan for incidents, failures, and decommissioning. I really liked earlier that was brought up the fact that suppliers do change. They can be bought out, they can be merged, software is patched, data centres are moved, procedures streamlined risk assessments are never a one and done. It's a constant, is this still okay? Is this still working for who we're working with? If we just go to the next one, a few tips about tech from care. So it's Everyday Tech done by the people you support. Respect people's choices. As I said, like some people do like Google Maps.

Some people do want to use WhatsApp, some people do want to use a smart speaker because that's what works for them. And that's fine. Just be open and respectful with the

person considers everyone's rights and privacy, the person you're looking after, and the care work you may be sending to them, and understand the tech without taking control. One of the things that I've made a note of Back here is that sometimes the engineers that go and install this kind of tech, they don't know the technology 100%. They know how to install it, and they know a basic list of FAQs, but they don't know the encryption that's going on inside. They don't know where the data is being sent to. If you say, oh, is it doing this? They're not sure. Because that's not their job, their job is to install it and leave.

So just be careful, like, if you are speaking to a supplier, make sure you really understand what the tech is doing, rather than just assuming that the salesperson is telling you everything that they can confidentiality, so conversations and activities may be recorded, just meet that Treat smart tech like there's another person in the room, whether it's on, off, or whatever, you just don't know. So just treat like there's another person in the room. Would you have this discussion with them if there was somebody stood in the corner protect confidentiality and professional boundaries. Obviously, confidence of care workers have clear policies and procedures that ensure staff understand the risks and how to manage them, trained staff and provide ongoing guidance and support, learn, adapt, and improve.

Include everyday technology in all risk assessments When you're thinking about it, you don't have to go into minute detail, but you need to know enough to be like, okay, this person has this. Listen to staff, learn and adapt. It's new tech, new review, new update, new review, and you get into that cycle of constant learning And that just keeps you a little bit more secure. You never... nobody's ever going to be 100% secure, but just edge yourself up so that you're more secure.

[Katie Thorn](#)

And that's it from me at the moment. That's to the Q&A now. Thank you.

Wonderful. Thank you, Sam. Really, really helpful. And yeah, just as a reminder, please do keep questions coming through everybody. I also wanted to signpost people, Lynn Horton has helpfully shared a link in the chat to the Good Things Foundation and their data hub because there's been some discussion in the chat going on about lack of access to data to the internet and connectivity and ways that we can support around digital inclusion with that. So please do take a look But I think probably following on quite nicely from the last few presentations, there's a question here from Lily. It'd be good to sort of get your viewpoints about how you might approach this yourselves.

So it's if you have a resident who lives with other housemates and has their own mobile phone How can you reduce the risk of them accidentally taking pictures that would be a GDPR concern without monitoring what they're doing with their own phone? So, for example, people choosing to take selfies with their friends when they're in a supported living situation, maybe, but then also putting that on social media and balancing people's

right to privacy. So I don't know if this is a situation anyone has had to deal with or has any sort of tips on how you may approach that at all.

Chris Ede

I think that's, that is what support work is. You're there supporting people to Perhaps understand the risks or or to see their housemates viewpoints and to guide them. That is in a nutshell what support work is. So I think it's just being proactive and being aware as a support worker that this may happen and just doing your best to mitigate it. I hate to say it on the grains, but on the grain in the moment I think that's the best way you can go about it. Inform support

Katie Thorn

Thank you, thanks and support in the chat for that one as well, Sam Rosa said an open and honest conversation maybe would be a really helpful approach on this one. Yeah, thank you. Emma, did you want to come in on that?

Emma Nichols

I was... yeah, I was just going to echo exactly what Chris said, but also it's around supporting the staff to understand as well, because if you go back to that wheel that I showed in the first place with that sort of ongoing training, but really understanding Supporting the staff to understand the risks around the technology because they might not even pick that up necessarily or sort of think about what the actual impact could be around that. So it's really about supporting them and also absolutely about talking to the individual and Supporting them to understand the the the potential implications from doing that sort of thing.

Katie Thorn

Brilliant, thank you. And then this one is more for Alice, but sorry about that, but everybody else, please do chip in as well. So, I think one of the things which you mentioned was around liability and people's sort of fear of liability, possibly then adding to digital exclusion. I just wondered If you could share some more about that as a concept, and also whether you had anybody from the Knowledge User Networks sort of saying how they were helping people to get over a concern about liability and that staff training piece, maybe.

Alice Dunning

Yeah, definitely. I think from the kind of knowledge user's perspective, I think in our In the provider group, this idea of like who holds responsibility, it was like Probably their biggest concern around some of this stuff. So Examples of stuff like if you have Supported living and somebody has their own like a bit like that example that's just been spoken about, like, who holds responsibility when themselves or a family member have bought a device that is then going in a shared living space. So somebody spoke about some family

member buying an Alexa that then went in a lounge, but the rest of the people didn't have the weren't able to engage with Alexa in the same way.

And that became a bit of a kind of A challenge for them in terms of inclusion because they felt that having the Alexa in that shared space was then excluding the other people that lived there because they couldn't engage in that device. Ultimately, they made the choice To restrict having it in that space. And then we kind of as a group had a conversation about, well, then you're digitally excluding the person that could kind of engage with that device. So I don't in terms of there being like an advice around some of it. It was more just People sharing their concerns around it and I think also a lot around the fact that because these are everyday devices, you have to have an email account to set something up. Often you have to have a bank account that's linked to that. Whose is it if the provider has purchased that, or if a local authority has purchased it Where does that information go?

And how do you like have protections on kind of stuff being bought accidentally and things like that? And I think there was a lot of restrictions in local authorities because of that. So even though The national policy literally names Alexa as an example of a device that could be really brilliant in social care. Some local authorities have a blanket restriction on commissioning it because their kind of legal and procurement side can't kind of square that circle about kind of who holds responsibility for the data and who's the account would be if it's been bought by the local authority and who will be responsible if it goes wrong. So yeah, I think it comes down to for me, kind of what Emma was talking about at the beginning and it being that person-centred approach Having conversations with the individual and expectation setting around some of these things.

There's lots of challenges for providers where charities have bought like a set of tablets for the people that they work with, and that's really exciting initially, and then it becomes a headache for the kind of provider organisation, because it's, well, what happens when they become reliant on this and it breaks, that money's gone, that support's gone. Are we then responsible for it? What does that look like? So yeah, sorry, that wasn't really an answer to your question. I think in quite a lot of this stuff, it often you kind of Yes.

Katie Thorn

hair at the edges, and then you keep going, don't you? And it kind of unravels more and more yeah I mean, if it helps, I think I asked more for reflections than a specific answer, so thank you, Alice, that was really helpful. A question that's just come through as well, should caveat I don't believe anybody on here is a GDPR expert, but just in case, please flag if you are. But this is a home care provi... as a home care provider, clients and their next of kin can install tech in their home without our knowledge, so as covert CCTV, like we hear about this a lot as well. And they're asking how we ensure we meet GDPR requirements and don't know if anybody has a view on this one. Or maybe just on sort of how you work with sort of families next of kin who are purchasing

Emma Nichols

Technology which you then care workers and support workers may not be aware of going into their home. Pretty tricky one, isn't it? I don't really have Nobody will take an answer. I think it goes back to that real co-produced approach, I think, and working with everybody to... for them to really understand the implications, but I'm not a GDPR expert, but we but you you need to be

Katie Thorn

I could say from a GDPR side that's right, but you can see from your personal experience side, yeah.

Emma Nichols

Yeah, so for me, it would be very much about I'd be talking to my data protection officer, obviously, or UK, because that's your role in your organisation, isn't it? But really Yeah, I think it's about that it's really about talking and unpicking like Alice was just saying, going through the scenarios and unpicking it and because Those cameras being put in by a family and then staff not being aware of it or not feeling comfortable with it It's a really difficult one, isn't it? Because they're there to deliver support and care Yes. But they're also being watched. But then you'd also be asking the question, this might be a little bit contentious. What are you hiding? And you know, so there's a whole raft of conversation around it. I don't think there's a clear cut answer as such That's my personal view.

Chris Ede

I, I did have a case similar to this where so we were going to use similar to metaglasses, so they were glasses that streamed support. And it was for a positive behavior support need. So the idea was PBS practitioner could sit in the office, watch the support, and then feedback, rather than go into the house, standing in the corner of the room, everybody acts a bit differently then, everybody's a bit unsure. So it may give a truer reflection of the support, and the staff team came to me with why are we being watched Hmm. Why are we being judged? Which I think was perfectly natural reaction. So it was...

I went to the house and it was sitting down with them and just explaining, we're not necessarily watching you, outside of you breaking the law In which case, yes, we will have to act on that, but outside of you breaking the law, this isn't about you as such, this is about the practice, the support that's being given. And it was more just reassuring them Hmm. That that's what we can do. Obviously, with the covert side of it, a lot of best interest work, a lot of the least restrictive practice work, that's all got to be done before you even get to the stage that you're Having these conversations.

Katie Thorn

Yeah, thanks, Chris. I think that's a really interesting use case. I mean, in the specific scenario, which is in the question as well, just to be clear, so if the individual or their next of kin has purchased a CCTV and it's covert CCTV in their own home and you have no idea

that it's there You're not on the hook from a GDPR perspective because you're not the data controller. You didn't choose that technology to be there. There is very extensive guidance in the ICO's website around where CCTV is appropriate and also on CQC as well, which we'll make sure we'll send out as links And what we have found is similar to what Emma and Chris have said, we see quite a lot of pushback from care and support workers, understandably about feeling quite surveyed at work.

And this normally means there's a broader breakdown of a relationship of trust, I think, between the care worker and like the family member and there's probably something you need to do there about having that conversation that's supporting and sort That's out. We also, they did a webinar earlier this year, which we could also share recordings of, which was a conversation between a care worker and a carer, a family carer about that distinction between privacy and monitoring and surveillance and sort or a family member, particularly when you're talking about people who may be nonverbal, would like to have surveillance is actually of security, but one from a care worker perspective, they feel like a lack of trust and transparency and lean down on their job. So We do have some resources that we'd be very happy to share with you all on this.

So, next question as well We've had one sort of come through as well about managing fluctuating consent when it comes to people's ability to choose technology. This always comes up in this topic, but whether people had some thoughts or resources on that at all

Chris Ede

Yeah I think I touched on it when I talked about assessing, reassessing. It's not set in stone. When I do mental capacity assessments specifically for tech, it's not a standard mental capacity assessment. It's a specific piece of tech, so zero in on that. And again, it's understanding that capacity isn't set in stone For example, somebody may get a better understanding of technology as they use it more, in which case it changes. So I would echo sort of going the long way around And keep doing it. Sort of get used to your processes and procedures, get comfortable with them, because hopefully you'll be doing them a lot

Katie Thorn

Brilliant, thank you, Chris. I guess it also goes back to the model which Emma shared at the beginning as well with having keep going back to consent and checking in and everything as well. Brilliant. So we are coming to the end of our session now. I'm hoping we should have a feedback poll, which will pop up in just a minute. We would be very grateful if people could tell us how this session has gone for you. It helps us to improve, to find out what's been useful, that sort of thing And while that's going on, I guess just one last one for Sam, if that's all right. Just a little bit more about your sort of points about when you're choosing technology as an organisation as opposed to when you're supporting somebody who's picked and purchased their own technology. Like what would be your sort Top tip for each of those in your starting place around being safe. Yeah.

Sam Cattell

When you're looking for technology From a Cyber point of view, the easiest way is to look for some sort of certification. It's not ideal, but you're looking for something like Cyber Essentials Plus, ISO 27001, SOC 2 type 2. probably mean people to it people if they don't mean anything, they're just certain certifications that sort of means that the company that you're looking at, or the supplier you might be looking at have a certain minimum level For me personally, I prefer SOC 2 Type 2 because it goes over a number of time rather than just a quick flashpoint. But just as a starting point, that gives you a nice sort of easier... it's not perfect, but it gives you a nice easy, okay, these people have gone to the trouble of making sure they've got certain minimum standards So we can at least move forward with that. But presumably you've all got different risk assessments.

And then it's what your risk appetite is and obviously make sure it's GDPR compliant, data protection, check all that DPIAs, that's all your stuff, Katie. But those are the kind of things you need to look for. But from a Cyber point of view. Don't just listen to the marketing people. They're very good at telling you what you want to hear and selling you their particular solution to whatever it is that problem that you happen to be having. Go to the engineers or go to the tech documents or stuff like that. And if you need it like translating, you can you somebody like us, or even you can potentially, and I know that we don't really like AI Katie, but you can use AI a little bit to help break down stuff. If they say we use this particular encryption, we make sure that it's at rest and you're looking at a load of words that you don't know Put it into AI, see if it makes sense to you.

If you've got an MSP or an IT or a cyber person, go to them. As I say, use... use one of us. I mean, nerds like me, we love to help out when we can.

Katie Thorn

Yes, safe use of AI.

That's really helpful to clarify, we don't hate all AI. We just want people to be cautious about how they're using it and having sort of governance. Yeah, exactly that. Brilliant. Well, thank you so much, everybody, for joining us today. As I mentioned at the beginning, we will share a recording and the slides with all of you afterwards. That'll probably be tomorrow. Now you'll get an email from us. And thank you as well to my amazing panellist speakers for sharing your time and your expertise. So, Emma Alice, Chris, Sam, thank you so, so much and take care everybody.