DSPT
Better Security. Better Care.

Northwest Cyber Digi-Tech Network

Liverpool Social Care Partnership
Community Interest Company Registration Number 7217998

Meeting Minutes

Date	**Wednesday, 19th February 2025**	**Time**	**10:00 – 13:45 PM**
Venue	**Online, Zoom**		
Theme	**Tech Enabled Social Care**		
Facilitator	**Mohamed Jaishan, LSCP**		

Time	Minutes
09:45	**Arrivals and Registration, Opening Remarks** The event began with introductions and housekeeping by Mohamed Jaishan – LSCP.
Session 1: Supporting Not Replacing — Responsible AI in Care	
10:05	**Interactive Activity 1: AI Impact Mapping** The first interactive activity began with AI Mapping. Attendees discussed in groups on the risks and impacts of 6 different AI tools (gen AI (ChatGPT, Gemini), AI chatbots, falls prevention AI, Care Planning AI, Emotion Recognition and AI Meds Reminders).
10:20	**Care in the Age of AI: Opportunities, Challenges and Change** *Daniel O'Shaughnessy – Head of Programme Delivery, Digital Care Hub* Dan outlined the role of the **Digital Care Hub**, a national not-for-profit organisation supported by government funding. The Hub provides policies, templates, digital and AI resources, robotics case studies, supplier guidance, and procurement support. He opened the floor for perceptions of AI, which included the words nervous, weary, and productive as some words that come to mind. Providing context, he explained that AI research dates back to 1956. He also clarified ChatGPT's positioning as an advanced predictive text tool. It does not create original content but generates from existing data. He raised concerns regarding the use of outdated information and referenced CQC discussions on innovation, highlighting potential applications in falls prevention. He emphasised that providers should not be fearful of its introduction. Examples of current use in adult social care included **rostering tools**, which reduced travel time, increased frontline care, and improved job satisfaction for carers, while complementing rather than replacing staff roles. He also highlighted risks, noting AI's dependence on data inputs and the issue of "hallucinations" in outputs. For instance, ChatGPT could fabricate academic

	references or introduce inaccuracies in care plans. He cited Australia's decision to ban AI in children's services due to such risks, which the UK seeks to avoid. CQC has introduced clauses to encourage innovation but remains concerned about the absence of safeguards, particularly the lack of risk assessments and data protection impact assessments. In response to whether AI can be used to generate care plans, Daniel noted it may support reviews and template design but is unreliable with reporting and prone to errors. He referred to a **project with Oxford University** on ethical AI use, which brought together care providers, tech suppliers, and stakeholders. A pledge has been developed for suppliers to follow agreed guidelines. He advised that the pledge should be used as a "litmus test" for organisational readiness and standards in AI adoption. **Key recommendations for AI use** included: ensuring high-quality data, maintaining human review, prioritising data protection, mitigating bias, assessing financial implications, equipping staff with appropriate skills, and implementing clear AI policies.
10:40	**AI and Ethics** *Paul Howell – Founding Director, Arquella* Paul spoke on the role of AI and ethics in fall management (FM). He highlighted that falls pose significant risks to independence with both human and financial costs, and that technology can be part of the solution. There is a lot of funding for AI and if we can make it work here, we can make it work anywhere. AI is not a new concept anymore; it is being talked about everywhere. This isn't a question about if, we *should* adopt technology, it's about *how* we adopt it. He outlined the building blocks of AI, clarifying the difference between AI, machine learning (ML), and generative AI. Most fall management applications currently rely on ML, while generative AI supports tasks such as summarising information rather than real-time detection. A comparison was made between ML (sensor-based, safety-critical, real-time detection) and LLMs (text-based, supportive, scenario-focused). The potential for ML technologies such as mmWave, IR, cameras, and PIR sensors was

	contrasted with LLM opportunities like automated insights, personalised prevention plans, and improved training and communication. Paul stressed key ethical considerations, including privacy, consent, bias, fairness, and balancing autonomy with safety. He highlighted drug dispenser technology as an example that works great in concept until the fact that it's connected to the web is realised. He also urged the notion of not using ChatGPT in care environments in a routine, day-to-day, immediate care delivery due to the risks such as hallucinations, etc... He noted that technology should support, not replace, carers, and that transparency and dignity are essential. Looking ahead, he emphasised responsible innovation, convergence of AI and ML, and the importance of involving residents and families in adoption, with ethics guiding all developments
11:00	**Interactive Activity 2: Prompt with Purpose** Following the speakers, attendees were invited to reflect on whether their views had shifted since the AI Impact Mapping exercise and to share their updated choices with the group. In the Prompt with Purpose activity, participants worked in groups to consider practical scenarios of AI adoption in care. Each group explored the potential benefits, risks, ethical concerns, and regulatory implications, before feeding back their key points to the wider discussion. Some feedback from groups included: Scenario 1: Using Generative AI (eg: ChatGPT) - Risks highlighted around AI use in data mining and potential data breaches. - Concerns raised about information being exploited on the dark web and used for ransom. - Identified need to provide carers with opportunities to upskill. - Noted that AI-generated records may raise issues of safety, accuracy, detail, and misrepresentation. - Suggested that AI should be limited to use as templates or guidance only. - Preference expressed for staff-written notes, even if imperfectly worded, over computer-generated text. Scenario 2: Using Falls Prevention (eg: NOBI Lights, CCTV) - Emphasis on clear communication with service users

	- Usage is on demand, and works well when used appropriately - Importance of documenting usage and implementing robust policies, with agreements and terms in place for all parties. - Need for strong service level agreements, including daily security updates. - Requirement for appropriate staff training.
11:25	**Break**
Session 2: From Inbox to Impact — Cyber Resilience in Care	
11:40	**Keynote Panel 1: Inside the Breach — What Every Care Team Should Know** *Niomie Haynes – Commercial Manager, NW Cyber Resilience Centre* *Lewis Desmond – Ethical Hacker, NW Cyber Resilience Centre* *Lisa Washer – Head of Cyber, IntaForensics* **Q. When you try to break into systems, what's the easiest way in — and why do you think care teams are especially vulnerable?** *Lewis:* with hacking it's all about how things can be manipulated; social engineering there's a huge psychological element **Q. From your work across the region, what's the single biggest cyber threat you're seeing right now for small organisations like care providers?** *Niomie*: social engineering, phishing – 89% of attacks, social media accounts locally in the NW as the highest reported attack pathway *Lisa:* phishing- a trigger for the biggest things in cyber (ransomware, etc..) **Q. How can I identify between a phishing email and normal 'spam'/marketing?** *Lisa:* Be paranoid! If you are expecting something from someone, high possibility it is from that person, if you have the gut feeling something is wrong, report it, rather over-report than be compromised. *Niomie*: 5.5 billion phishing emails globally, google 100 million emails stopped; air of caution, double checking especially with things like financial information. **Q. Walk us through what a breach looks like in the first 24 hours. What actually happens once a breach is detected – what does day one look like? What are providers expected to do first?** *Lisa:* Preparation is key. With policies and plans, response is smoother. Involve the DPO, identify compromised data, contain and disinfect systems, check for backdoors, and complete patching. *Niomie:* Follow incident response steps. Outcomes depend on preparedness and having the right people involved.

	Lewis: Think like a hacker — anticipate next moves and block those pathways to limit damage. **Q. Does turning off the Wi-Fi stop the attack?** *Lewis:* unplug it. Isolation is key, make sure it doesn't spread, be proactive not reactive. *Lisa:* Don't turn the computer off; as then you will lose the logs and ability to recover is difficult. **Q. What should providers not do?** *Lisa:* Don't panic, which is very hard not to do but panic will worsen the chaos. Have a step-by-step plan prepared/ checklist. *Niomie:* No Blame Culture. Create a safe space for your team to come up to you. Remove the shame, fear and embarrassment will help you a long way. **Q. What's one good thing you've seen or would like to see?** *Lisa:* A particular instance takes me to the importance of Teamwork. The team worked long hours to recover systems, no blame culture, working together well. Stronger team for it and weren't panicking. *Niomie:* Would like to see organisations keep track of what type of data and the value of that data. *Lewis:* Reactions of people about cyber security is really good to see. Making this culture stick.
12:10	**Interactive Activity 3: Exercise in a Box** Attendees took part in a group exercise using adapted NCSC *Exercise in a Box* scenarios with a care focus, exploring the risks of unsecured public Wi-Fi and how organisations can protect users through awareness, alternatives, updates, and access controls, as well as a third-party compromise scenario, discussing ransomware response, business continuity, backups, supplier risk, reporting, insurance, and ransom considerations.
12:40	**Lunch and Networking**
Session 3: Not Just Tech-Savvy — Care-Savvy with Tech	
13:10	**Keynote Panel 2: Building the Human Firewall in Social Care** *Ann Garvey – Key Account Manager, LSCP* *Lynne Horton – Digital Skills Development Lead, National Care Forum* *Beverley McGowan – Founder and CEO, Specialist Skills Hub*

Q. Care Technologists, what's that all about?
Lynne: mimicking a scheme from Scotland; Care Technologists. I've got to develop role, resource, exam for care technologists in residential settings and community side. Its not anything new, it's using what we got out there, to improve people's care outcomes.

Q. What's the one barrier for digitisation you've seen across the sector?
Ann: We didn't need tech as a sector until Covid. Especially in the NW the demographics are SMEs as care organisations. The thought of digitisation is terrifying to a lot of people. People forget they can do social media, and online banking, smart phones, etc.. but is terrified of adopting the new tech coming into care. Bigger organisations have IT departments and IT savvy people, but is not the same for SMEs

Q. From a training and apprenticeships angle, what do you think makes digital and cyber awareness 'stick' so staff change their habits — rather than just passing a course?
Beverely: learning needs to be individualised, and targeted and relatable to people. Bringing situations to life, like today. E-learning doesn't really bring it to life, but collaborative working does along with shared experience. Learning in group environments and applying it to workplace goes a long way.

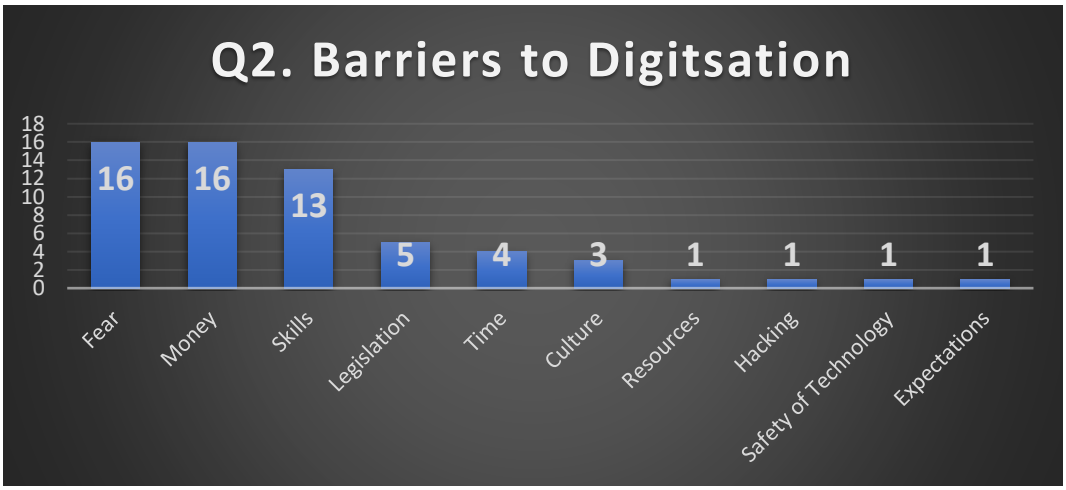
Q. How do we make cyber awareness part of daily routines like logging in, handing over shifts, or using care records?
Ann: Show how digital security in personal life (e.g. online shopping) can translate to professional practice. It's about demonstrating ease of use.
Lynne: Use team champions and different learning styles — visual, auditory, and hands-on — to support colleagues.

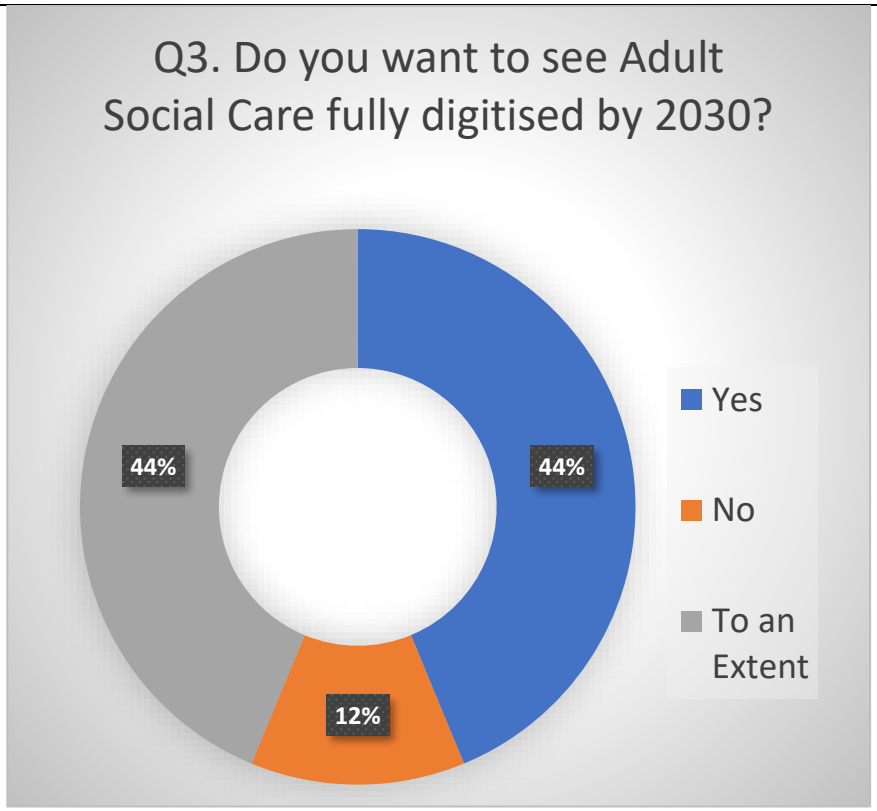
Q. What role do peer champions — like apprentices, digital leaders, or care technologists — play in creating culture change?
Beverley: Peer champions provide practical support, share updates through activities like "lunch and learns," and act as local points of contact.

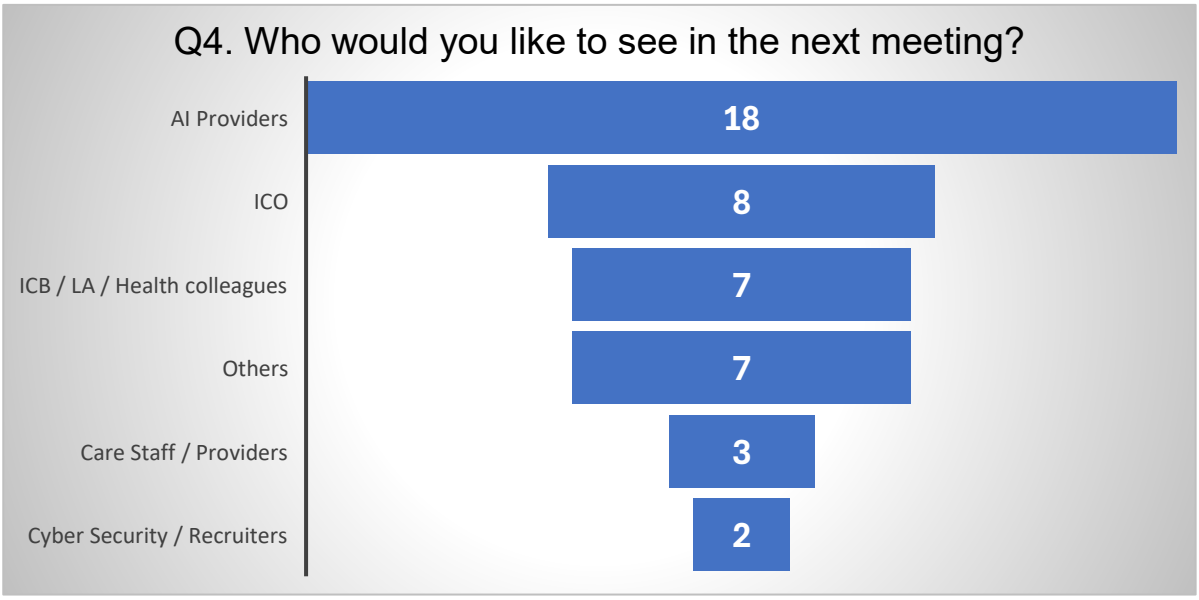
Q. How do we future-proof the workforce — so staff keep pace with digital risks without feeling overloaded?
Beverley: Culture, Collaboration, Communication. Don't feel like you can solve everything yourself, there's other people who can help and skills building exercises like today.

	Ann: Accountability; we all learn from mistakes and should be able to say I've done this wrong, what training can I do to improve. Working together without repercussions unless you are a habitual offender. *Lynne:* Fear. We've got acronyms for everything. Empathy: and asking questions like what's this for, what does it do? Care's going to have to change and adapt to tech. Culture to not be afraid of tech adoption is key.
13:35	**Closing Remarks and Feedback** A feedback exercise was done through Mentimeter where participants answered some questions about digitisation and the event in various formats. Below are the results of the exercise. **Q1. Rank these in order of importance on what's next for practical cyber security and data protection in Adult Social Care.**

Rank	Priority
1	Robust business continuity planning and testing
2	More In-depth Training
3	DSPT Audits
4	Third-party supplier checks
5	Cyber Resilience Exercises







Next Meeting Date: 19/02/2026, 09:45 – TBC (face to face, venue: TBC)	
Facilitator	**Mohamed Jaishan, LSCP**