

NEWSLETTER



Sussex
Digital
In-Reach
Team

Supporting Care Providers in Sussex

Welcome to The Sussex Digital Team Newsletter. We hope you find the information here helpful as you explore and grow your digital journey within your care setting. QR codes and website links are available in this newsletter to enable you to access more information.

Your Free Cyber & Data Healthcheck - **THIS MONTH!!**



Keeping information safe is a legal, regulatory and contractual requirement. But are you confident that your data protection and cyber security arrangements and practices are up to scratch?

We're offering a FREE Data Protection and Cyber Security Healthcheck to help you verify that your organisation is not only meeting the requirements but also embedding these practices into your daily operations.

We are part of the government-funded Better Security, Better Care programme so you can be sure that our advice and support is up to date with current requirements.

What's in it for you?

- **In-Depth Assessment:** Our experts will review what policies and procedures you have in place, and what you're actually doing in practice.
- **Boost Security Confidence:** Get actionable insights to strengthen your data protection and cyber security measures.
- **Confidential report:** We will identify areas that can be improved and signpost you to support.
- **CQC Recognition:** The health check provides evidence that can be used to demonstrate proactive efforts in data security and working in partnership, which can support your CQC inspection and potentially help you achieve higher ratings, including "Outstanding."

***Book your free Health check today
before the rush!!***

nada@sussexdigitalteam.co.uk

DSPT 1:1 SUPPORT SESSIONS

Did you know that we offer a completely FREE DSPT service to all CQC registered Care services?

Whether you are an individual establishment or a group chain, we can support you and your team with your Data Security Protection Toolkit (DSPT)

DSPT or Data Security and Protect Toolkit is an annual online self-assessment of your organisations data and cyber security arrangements.

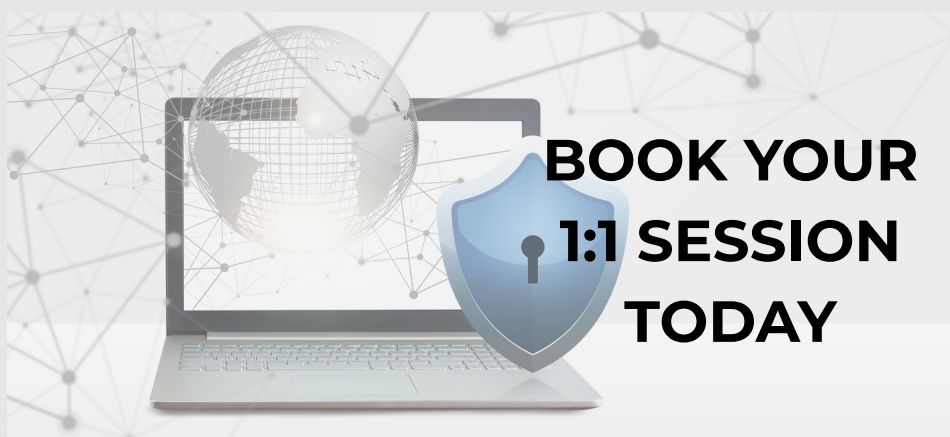
It demonstrates compliance with 10 data security standards and the Data Protection Law but completing your DSPT does a lot more than that.

It is your gateway to the future.

The DSPT opens up opportunities for your service to:

- Share information digitally across health and care networks
- Be part of projects that allow care services to directly access NHS patient information systems, for example, GP records and shared care records
- Save you and your staff time and therefore improve the quality of care for the people you support.

Central and local government bodies, local authority and CCG commissioners, the Care Quality Commission and the National Data Guardian recognise The Toolkit as the official tool to evaluate care providers' compliance with legal requirements, Data Security Standards and good practice.



IF YOU NEED TO REPUBLISH JOIN US ON

THURSDAY, NOVEMBER 6

INTERACTIVE WORKSHOP: REPUBLISH YOUR DSPT

REPUBLISH YOUR DSPT, AUDIT YOUR ANSWERS, ASK
QUESTIONS, AND ACCESS IN-DEPTH SUPPORT



WHAT SOCIAL CARE PROVIDERS CAN LEARN FROM THE KIDO NURSERY ATTACK

In late September 2025, the UK childcare sector was shaken by a brazen cyber-attack on the Kido nursery chain. A hacking group calling itself Radiant claimed to have stolen the personal data of roughly 8,000 children — including names, photographs, addresses, and family contact information and published the profiles of ten children on a dark web leak site as proof of their access [Reuters](#) - The attackers, demanded a ransom in Bitcoin and threatened to release further data on additional children and staff.



In a dramatic move, the hackers later claimed to have deleted the published data following public [Guardian](#). Nevertheless, the incident raised immediate alarm among data protection regulators, the childcare sector, and social care organisations. Two 17-year-olds were arrested in mid-October by the Metropolitan Police on suspicion of computer misuse and blackmail in connection with the breach.

Why this matters to social care providers?

Although the Kido breach happened in a nursery setting, its implications resonate strongly across social care settings:

- **Highly sensitive populations are at risk** - Social care providers often handle personal, health, and safeguarding data for vulnerable adults, children, or residents. A breach can expose intimate details and endanger client privacy, safety, and trust.
- **Data held across systems and by third parties is vulnerable** - The Kido breach reportedly involved “third-party systems used to process certain data,” including the nursery software provider Famly (though Famly denies their core systems were compromised). Read from the [Guardian](#) here:
- **This highlights a key risk:** even if you manage your own systems well, integrations and external platforms are a weak link unless they are held to the same security standards.
- **Extortion tactics are evolving** - The attackers used double-extortion strategies: data theft plus threat of publication. They even phoned parents to pressure the nursery chain. That kind of personal, emotional leverage is especially disturbing in social care settings, where trust and relationships matter deeply.
- **Regulatory risk and breach response are non-negotiable** - Under UK GDPR and the Data Protection Act 2018, serious breaches must be reported to the Information Commissioner’s Office (ICO) within 72 hours, and affected individuals may need to be notified. Read more from [Cripps](#):
- **In social care**, failure to respond transparently can compromise safeguarding, professional reputation, and legal compliance.
- **Smaller organisations are particularly vulnerable** - Many care providers are small or medium-sized operations with limited IT budgets or cybersecurity expertise. NDNA (National day Nurseries Association), in its response to the nursery breach, underscored how many nurseries (and by analogy many social care settings) are under-resourced in cybersecurity and need support to meet the heightened risk [NDNA](#):

WHAT SOCIAL CARE PROVIDERS CAN LEARN FROM THE KIDO NURSERY ATTACK -

CONTINUED.....

WHAT SOCIAL CARE PROVIDERS SHOULD DO NOW?

- **Review vendor risk and data flows:** Map all systems that hold or transmit personal or sensitive data, including third-party platforms and integrations. Verify that those systems use strong encryption, access controls, and incident response plans. [Attend our Supply Chain event on 3rd December at 1400 hours:](#)
- **Adopt “least privilege” policies:** Ensure users only have the minimal access needed for their roles and restrict administrative rights. [Read more here:](#)
- **Enforce multi-factor authentication (MFA)** for all accounts, especially remote or high-privilege ones. [Digital Care Hub](#)
- **Maintain secure, isolated backups and test restoration.** Make sure backups can't be altered or held hostage. Join us on this online event: [Business Continuity Plan - cyber attack survival guide, 25 November 2025 at 14:30 GMT](#)
- **Train staff** and leadership on phishing, social engineering, and incident escalation protocols. [E learning](#) can be found from the Digital Care Hub :
- **Have a breach response plan:** Identify roles, external forensic/messaging support, stakeholder communication strategies, and regulatory obligations before an incident occurs. [ICO:](#)
- **Engage supporting bodies:** Seek guidance and support from regulators, local authority cybersecurity units, or umbrella organisations to share resources and best practice. [Sussex Digital In reach team:](#)



The Kido attack is a stark, disturbing signal: when cybercriminals target the most vulnerable, they cross a new ethical threshold. Social care providers must not wait until disaster strikes — safeguarding data is not just a legal duty, but a core component of protecting those in your care.



CYBER ATTACK SIMULATION: CAN YOUR CARE SERVICE SURVIVE THESE 5 THREATS?

LEARN HOW TO SPOT AND STOP PHISHING ATTACKS AND SCAMS IN OUR EVENT - DON'T FALL FOR THOSE SNEAKY TRICKS!



Phishing is when attackers send scam emails (or text messages) that contain links to malicious websites. The websites may contain malware (such as ransomware) which can sabotage systems and organisations. Or they might be designed to trick users into revealing sensitive information (such as passwords), or transferring money.

Guidance on the **National Cyber Security Centre website** is aimed at technology, operations or security staff responsible for designing and implementing defences for medium to large organisations. This includes staff responsible for phishing training.

Staff within smaller organisations will also find this guidance useful, but should refer to the **NCSC's Cyber Action Toolkit** beforehand. The toolkit is FREE to use!!

The cyber security toolkit includes quick and actionable guidance to keep your money and reputation safe.

JOIN US ON THURSDAY 20TH NOVEMBER 12:30 - 1:30PM

In this 1-hour interactive workshop, you'll gain the practical skills to recognise and respond to phishing attacks and scams that could target you or your organisation. We will walk through real-life scenarios and work together on identifying red flags and implementing effective responses to these threats.

KEY TOPICS COVERED:

- Recognising Phishing: Learn how to spot phishing emails, phone calls, and messages, including common tactics used by cybercriminals.
- Scenario-Based Learning: We'll work through different phishing attack scenarios, allowing you to identify threats in real time.
- Practical Responses: Discover the best course of action when you or a colleague encounters a phishing attempt, from reporting to preventing further damage.
- Protecting Sensitive Information: Understand how to protect sensitive data and avoid exposing your organisation to risk.



BUSINESS CONTINUITY PLAN - CYBER ATTACK SURVIVAL GUIDE

YOUR GO-TO GUIDE FOR NAVIGATING AND SURVIVING CYBER ATTACKS IN THE CARE SECTOR

Technology has changed the way we work together. Sharing data digitally and communicating with others remotely are just a couple of examples of how we use technology in social care. As we continue to use technology in this way, we must do it safely and put steps in place to reduce the risk and impact of a data breach or cyber attack.



A business continuity plan details what you would do if your services were disrupted by something out of your control. Ideally these situations would never happen, but a good plan would cover what you would do in the event of an incident so that you could continue to operate your business.

From floods to fires, power outages to cyber attacks, and everything in between – it's about preparing your business for all eventualities. Read more from [**the Digital Care Hub**](#)

Did you know that 93% of businesses without a Business Continuity Plan (BCP) fail within a year following a significant disruption? With the growing sophistication of cyber threats, businesses face increased risks of operational downtime, data breaches, and reputational damage. [**Read more with KeepNet**](#)



JOIN US ON TUESDAY 25TH NOVEMBER 2:30 - 3:30PM

This practical session is designed to help providers understand how to test their BCPs effectively, with a focus on real-world digital risks. We'll walk through examples of how to prepare for and respond to scenarios such as:

- Loss of internet or phone lines
- Power cuts
- Cyber or ransomware attacks
- Stolen or hacked computers or mobile devices
- Failure of critical systems like electronic medication administration records (eMAR), digital social care records (DSCR), care planning software or websites

We'll cover:

- ✓ How to design and carry out realistic tests of your BCP
- ✓ What evidence you should keep – what was tested, when, and the outcomes
- ✓ How to record any remedial actions taken following a test
- ✓ When and how to review and update your BCP – annually, or whenever there's a major change to your digital systems.

MEET MARK TOPPS & THE CARING VIEW



Many of you may already be familiar, but for those who are not, [Mark Topps](#) is a highly respected social care leader with over two decades of experience in the sector. He is the co-founder of The Caring View, a free online platform and YouTube series launched in 2021 to share best practice, explore sector challenges and celebrate innovation across social care.

Nada says *"I first met Mark at the beginning of the pandemic, when he supported us and many other providers by generously sharing resources, including his Business Continuity Plan, which helped so many of us navigate those difficult and uncertain times. Since then, his passion for working collaboratively and sharing his knowledge has continued to have a real impact across the sector."*

The Caring View produces regular episodes, blogs, and resources covering everything from CQC preparation and leadership to digital transformation and staff wellbeing. Mark also serves as Social Media & Marketing Director for the National Association of Care & Support Workers and is widely recognised as a passionate advocate for the care workforce.

We are delighted to share some of Mark's resources with you — his practical insights and honest reflections continue to inspire and support care professionals across the country.

- Common CQC inspection failings and what you can do to resolve them - Visit his [You Tube Channel](#) or Scan the QR Code to find out more:



theCaringView

- Cyber Awareness Blog - [Cyber Awareness Month](#) - The Caring View
- Fair Pay Agreement Update/Blog - [Adult Social Care Fair Pay Agreement - The Caring View](#)
- The Oliver McGowan Code of Conduct – what you need to know - [The Oliver McGowan Code of Practice: What Care Providers Need to Know and Do - The Caring View](#) but also a live webinar we did on this which is shown on [YouTube](#)

YOU CAN SEE MORE ON THE CARING VIEW WEBPAGE

[THE CARING VIEW - EDUCATING, ELEVATING, AND CELEBRATING ALL THINGS SOCIAL CARE](#)

FREE EVENTS THIS MONTH

Don't forget to book onto our FREE online events this month. Use the QR codes to go straight to each booking page.

eventbrite



Tuesday, November 18
WhatsApp in Care: Safe or Sorry?

A practical session on the risks, rules, and real-world use of WhatsApp in care settings — and how to avoid a data protection disaster..



Wednesday, 19 November
Record of Processing Activities (ROPA) and Information Asset Register (IAR)

Join us if you want to learn more about your legal obligations as a care provider under The General Data Protection (GDPR)



Thursday, 20 November
Artificial Intelligence -safe and practical applications in social care

What are chatbots and how can I use tools such as ChatGpt safely to support my day to day work



Wednesday, November 26
NHS Mail: Essential Tips for Social Care Providers

A series of quick, practical 30-minute sessions showing you how to manage your NHS Mail account and resolve common problems



Book Now!

OTHER UPCOMING EVENTS....



Thursday 6th November

Identifying Critical Suppliers: A Key to Business Continuity in Social Care

Have you considered what would happen if one of your suppliers suffered a cyber attack or outage, leaving you unable to access critical information?



Thursday 27th November 2025

Caldicott Guardian Learning Network

This session aims to bring together a range of Caldicott Guardians to learn, share and explore the growing role of a Caldicott Guardian.



Tuesday 4th November

Spotting Human Error: Building a Cyber Aware Culture in Care

This free police-led webinar focuses on how to spot, reduce, and prevent human error in your organisation. You'll learn how to build everyday cyber awareness across your teams, strengthen your digital culture, and reduce risk - no technical expertise required.

CARE WEBINAR – THE DIGITAL SWITCHOVER – UPDATE AND GUIDANCE

TUESDAY 4TH NOVEMBER



In 2015, BT announced the phased shutdown of ISDN (Integrated Services Digital Network) and PSTN (Public Switched Telephone Network) services. This means that traditional landline connections will be discontinued, and all voice calls will need to be made over the internet (IP-based) in the future.

It is crucial for care homes to prepare in advance by ensuring they have a reliable broadband and telephony service in place. This will provide the necessary speed, bandwidth, and scalability to support daily operations seamlessly.

Additionally, any systems currently connected to a phone line—such as intruder and lift alarms, telecare systems, Emergency Red Phones, EPOS machines, CCTV, or even some half-hourly electricity meters—will also stop functioning and must be upgraded to digital alternatives.

Our session will cover:

- Recent update announcements
- The switchover explained
- Implications for your care home
- What is replacing this and the benefits
- Ensuring you are prepared
- Questions from the care sector
- and much more

Please feel free to forward our invitation over to any of your contacts who will benefit from this informative session.

OTHER UPCOMING EVENTS....

EAST SUSSEX CARE AWARDS 2025

We're delighted to announce the return of our Annual Care Awards & Dinner, taking place on Thursday 13th November 2025 at the East Sussex National Hotel, Golf Resort & Spa.

This special evening celebrates the dedication and impact of our amazing local care workforce, with 12 award categories including Care Newcomer of the Year, Care Leadership Award, and Outstanding Unpaid Contribution to Social Care.



We're thrilled to welcome renowned host Joe Fisher as our MC — bringing over 20 years of experience from events including the 2012 Olympics and London Marathon. Our special guest and other distinguished sector figures will be announced soon.

MIKE DERRICK, CHAIR OF EAST SUSSEX PARTNERS IN CARE, SAYS:

“LET’S MAKE IT A NIGHT TO REMEMBER AS WE CELEBRATE THE INCREDIBLE COMMITMENT OF OUR CARE COMMUNITY. HUGE THANKS TO OUR SPONSORS FOR MAKING IT POSSIBLE.”



FACEBOOK

Did you know that we have our very own Facebook page?

We post daily our FREE event links, relevant news and other exciting media.

Follow our page using this QR code to keep up to date.



We are almost at 200 followers and would really appreciate you taking these few steps to help us grow

- Follow our Facebook page
- Like our posts
- Share our posts
- Share our page with other Carers and Care Homes



FOLLOW US NOW AND SHARE OUR PAGE WITH OTHERS

CONTACT US



Nada Wakeford
nada@westsussexpartnersincare.org
Sarah McNally
sarah@sussexdigitalteam.co.uk
Claire Badzek
claire@sussexdigitalteam.co.uk
Natasha Fowler
natasha@sussexdigitalteam.co.uk
Georgie Ind
georgie@sussexdigitalteam.co.uk
Sam Harper
sam@sussexdigitalteam.co.uk

Or phone visit our website
www.sussexdigitalteam.co.uk