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.

THE 12 SCAMS OF CHRISTMAS – STAY VIGILANT THIS FESTIVE SEASON

SCAMMERS THRIVE DURING THE FESTIVE SEASON, EXPLOITING THE FLURRY OF ONLINE SHOPPING AND CHARITABLE GIVING. OLDER ADULTS ARE ESPECIALLY AT RISK, WITH A FRAUD VICTIM REPORTED EVERY 40 SECONDS IN ENGLAND AND WALES. OUR GUIDE OUTLINES 12 COMMON SCAMS AND HOW TO AVOID THEM

Book Now!!

THE TWELVE SCAMS OF CHRISTMAS

ON THE FIRST DAY OF CHRISTMAS A SCAMMER SAID TO ME
A COURIER NEEDS YOUR DETAILS NOW SO CLICK THIS DODGY FEE

ON THE SECOND DAY OF CHRISTMAS SOME HACKERS TRIED TO PLAY
WITH PUBLIC WIFI "HOTSPOTS" TO STEAL MY DATA AWAY

ON THE THIRD DAY OF CHRISTMAS A GIFT CARD LOOKED SINCERE
OPEN YOUR FESTIVE BONUS — THEN IT WIPED MY LAPTOP CLEAR

ON THE FOURTH DAY OF CHRISTMAS A WHATSAPP COUSIN CRIED:
"MY PHONE IS SMASHED, SEND SOME CASH!" — A CHEEKY SNEAKY LIE

ON THE FIFTH DAY OF CHRISTMAS A FACEBOOK SHOP POPPED UP:
SHINY BARGAINS GALORE, THEN MY DATA THEY SCOOPED UP

ON THE SIXTH DAY OF CHRISTMAS A RANSOM NOTE ARRIVED:
"PAY IN GIFT CARDS QUICK!" THE OLDEST TRICK CONTRIVED

ON THE SEVENTH DAY OF CHRISTMAS A CHARITY APPEALED
GIVE KINDLY FOR THE SEASON BUT MY BANK ACCOUNT WAS PEELED

ON THE EIGHTH DAY OF CHRISTMAS A WEBSITE GLEAMED WITH DEALS:
FANTASTIC FESTIVE OFFERS — MY CASH IT SWIFTLY STEALS

ON THE NINTH DAY OF CHRISTMAS A JOB AD LOOKED JUST RIGHT:
"SEASONAL WORK AWAITS!" BUT MALWARE STRUCK THAT NIGHT

ON THE TENTH DAY OF CHRISTMAS A CLAIM FOR LIVING COSTS:
"CLICK FOR GOVERNMENT PAYMENTS NOW!" MY SAVINGS LOST AND TOSSED

ON THE ELEVENTH DAY OF CHRISTMAS SUPERMARKETS PROMISED SPREE:
"WIN FREE VOUCHERS HERE!" — STOLE MY ID WITH GLEE

ON THE TWELFTH DAY OF CHRISTMAS SCAMMERS DANCED WITH CHEER:
BUT WE STAYED SCAM-FREE AND SHARP WITH DIGITAL CARE HUB NEAR!

WITH THE DSPT TOOLKIT YOU ARE SAFE AS SAFE CAN BE
AND SUSSEX DIGITAL'S ON HAND TO GUARD YOUR PRIVACY
WE WILL NUDGE YOU NOW AND THEN TO KEEP YOUR RECORDS KEY
SO HAVE A JOYFUL CHRISTMAS SECURE AND SCAM-FREE

BARGAIN HUNTERS are being urged to bolster their cyber security in the approach to the festive season after new figures revealed victims of online shopping scams lost on average £1,000 per person in the same period last year.

Scams ranged from one shopper losing more than £150 trying to purchase a mobile phone on social media to another being duped out of more than £7,000 during an attempted online campervan purchase. Meanwhile, another victim lost almost £500 when trying to buy shoes on a social media platform, and a fourth lost £145 trying to make a similar purchase.

The new figures from the National Fraud Intelligence Bureau (NFIB) come as the National Cyber Security Centre (NCSC) - which is a part of GCHQ – launched a nationwide drive to promote its Cyber Aware campaign to help shoppers protect themselves online.

The Cyber Aware campaign advises simple steps for shoppers to reduce their risk of suffering similar losses during this year's Black Friday (25 November) and pre-Christmas period.

Anyone who think they have been a victim of fraud should contact their bank immediately and report it to Action Fraud online at **actionfraud.police.uk** or by calling 0300 123 2040. More information is available by searching #FraudFreeXmas.

Action Fraud and the NCSC are urging online shoppers to protect their accounts, check before they buy, and use secure payment methods in order to stay ahead of the threat from criminals this shopping season:

- **Protect your accounts**: set up 2-step verification and use **three random words** passwords to prevent cyber criminals from gaining access to your shopping, bank or email accounts.
- **Choose carefully where you shop**: Research online retailers, particularly if you haven't bought from them before, to check they're legitimate. Read feedback from people or organisations that you trust, such as consumer websites.
- **Pay securely**: Use a credit card when shopping online, if you have one. Most major credit card providers protect online purchases and are obliged to refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected. Also consider using a payment platform, such as PayPal, Google or Apple Pay. And whenever you pay, look for the closed padlock in the web address bar – it means your connection is secure.

THREE RANDOM WORDS

The National Cyber Securirty Centre recommend that you use Three Random Words when creating a password.
Combine three random words to create a password that's 'long enough and strong enough'.

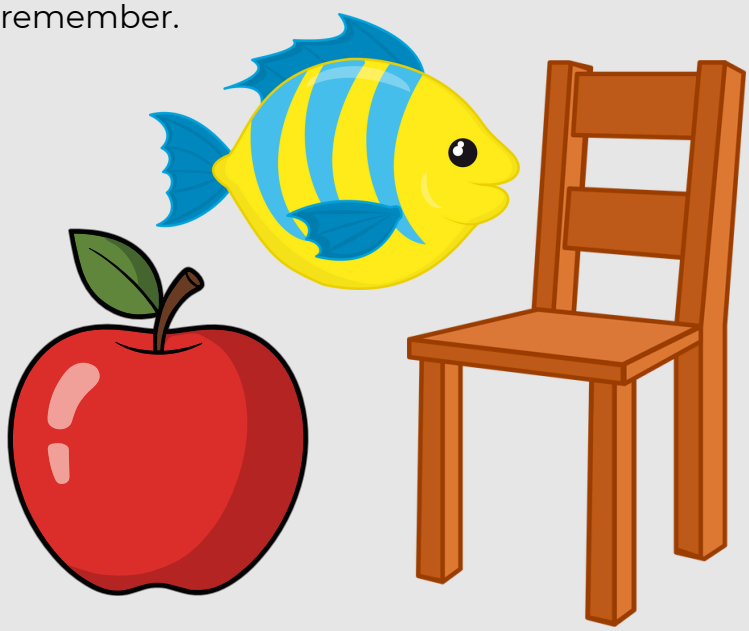
Part of Cyber Aware

Weak passwords can be cracked in seconds. The longer and more unusual your password is, the harder it is for a cyber criminal to crack.

A good way to make your password difficult to crack is by combining three random words to create a password (for example applenemobiro). Or you could use a password manager, which can create strong passwords for you (and remember them).

Avoid the most common passwords that criminals can easily guess (like 'password'). You should also avoid creating passwords from significant dates (like your birthday, or a loved one's), or from your favourite sports team, or by using family and pet names. Most of these details can be found within your social media profile.

If you're thinking of changing certain characters in your password (so swapping the letter 'o' with a zero, for example), you should know that cyber criminals know these tricks as well. So your password won't be significantly stronger, but it will be harder for you to remember.



Why does the NCSC recommend using 'three random words' as a way to create passwords?

By using a password that's made up of three random words, you're creating a password that will be 'strong enough' to keep the criminals out, but easy enough for you to remember.
Longstanding advice around making your passwords very complex (which suggests we should create passwords full of random characters, symbols and numbers) is not helpful.

This is because most of us have lots of passwords, and memorising lots of complex passwords is almost impossible.
Passwords generated from three random words is a good way to create unique passwords that are 'long enough' and 'strong enough' for most purposes, but which can also be remembered much more easily. If you want to write your password down, that's also OK, provided you keep it somewhere safe.

CQC WARNING: AI RISKS IN SOCIAL CARE

AI is not a shortcut to good care – and recent CQC findings underline this.

Many providers explore artificial intelligence to save time, boost accuracy, and ease staff pressure. When used well with proper governance, it can support care delivery. Without checks, however, it risks data privacy breaches and unreliable outputs.

A CQC inspection published around August 26, 2025, rated a homecare provider Inadequate overall, citing multiple failures including uncontrolled AI use. Inspectors flagged AI applied to confidential care records for auditing templates and reports without risk assessments, raising reliability and privacy concerns that undermined safe care. This was one factor among broader governance shortfalls leading to poor decision-making.

The key CQC takeaway remains clear:

AI tools demand robust risk assessments, data protection policies, and staff training on limitations.
Providers retain full responsibility for governance and safe implementation.
This is new territory for many, which is why regular sessions on safe AI use – aligned with CQC expectations – help organisations prepare.

You can read the **CQC report here:**

Join us in Our Next Session: Artificial Intelligence and the CQC AI Strategy

TUESDAY, 13 JANUARY 2026 AT 14:00

What you'll learn and do:

- Current context: What CQC and partners have said so far about AI use in health and care
- Provider responsibilities: How AI links to existing compliance requirements (governance, safety, consent, data protection)
- Practical exercise: Mapping where AI or "AI-like" tools are already in use (e.g. monitoring, rostering, decision support)
- Risk and assurance: Simple steps to document oversight, risk management and safe use – useful if asked by CQC
- Future-proofing: Questions to ask suppliers now about AI-enabled products and data handling
- Group discussion: How providers can share experiences and prepare together for inspection and regulation

CLICK HERE TO REGISTER FOR THE EVENT

YOU ARE INVITED TO OUR DSPT IN PERSON WORKSHOPS!

ARE YOU STILL IN NEED OF REGISTERING FOR THE DATA SECURITY PROTECTION TOOLKIT? ARE YOU HAVING TROUBLE PUBLISHING? WHY NOT JOIN US AT ONE OF OUR IN PERSON WORKSHOPS?

Wednesday 21 January 2026
The Palace Workspace, Hastings
2.30 - 4.30p.m.
Book Here

THERE IS LIMITED AVAILBILITY SO PLEASE BOOK NOW TO RESERVE YOUR PLACE!

What's in it for you?

This workshop is designed for social care providers who want to publish or republish their DSPT (Data Security and Protection Toolkit).

We will take you through each section of the toolkit, step by step, providing practical guidance on how to meet the required standards.

Whether you're publishing your DSPT for the first time or updating it, this session will give you the hands-on support you need to ensure your toolkit is complete, compliant, and ready for submission.

This workshop isn't just about ticking boxes – it's about making the toolkit a valuable, actionable tool that improves your service's data security and care practices.

SECURING THE SUPPLY CHAIN

WHAT IS SUPPLY CHAIN CYBER SECURITY RISK?

A supply chain is the extended network of trading relationships relied upon to deliver products, systems, and services. The Cyber Security Government Strategy (2022 – 2030) has recognised the growing risk within this area and is actively taking steps to better understand its dependencies on suppliers in a way that takes full account of their impacts on security and resilience.
Watch the video below to understand what we mean by supply chain cyber security risk.

JOIN US ON WEDNESDAY 3RD DECEMBER

SECURING THE SUPPLY CHAIN TO SAFEGUARD CARE

Essential guidance on managing supply chain cyber risks for social care providers.
This tailored session focuses on the critical importance of supply chain cyber security in health and social care settings. The session will provide practical guidance on identifying and managing supply chain risks, ensuring your organisation remains resilient in the face of growing cyber threats.

Participants will gain a clear understanding of:

– Why supply chain security is essential to DSPT compliance and broader data protection.
– How cyber incidents affecting suppliers can impact your organisation.
– Key questions to ask when assessing supplier security.
– What good cyber hygiene looks like in supply chain relationships.
– Steps to take when working with third-party providers, including contract considerations and risk assessments.

The session will also highlight tools and frameworks available to support your supply chain, including Cyber Essentials and other government-backed standards.

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

Wednesday 3rd December
Lunch & Learn with Nourish DSCR

Join us for a virtual Lunch & Learn session with Nourish DSCR offering peer support, Q&A and practical insights for social care providers.

Wednesday 10TH December
Lunch & Learn with Nourish DSCR

Join us for a virtual Lunch & Learn session with Nourish DSCR offering peer support, Q&A and practical insights for social care providers.

nourish

This is an informal Lunch & Learn session designed exclusively for social care providers in Sussex using the Nourish DSCR system. Following the recent evaluation report, these sessions aim to provide a space for peer learning, shared insights, and direct support from the Nourish team.

During the session, you'll have the chance to:

Explore system functionalities and ask questions directly to Nourish experts

Share your experiences and learn from other providers across Sussex

Discuss ways to make the most of your DSCR data for everyday improvement

Shape future support and training opportunities

LIVE WEBINAR

Book Now!

OTHER UPCOMING EVENTS....

Home Care Themed Webinar

Thursday 11th December 2025

Second of our bi-annual themed webinar for home care providers/managers. These webinars offer opportunities for sharing the latest service updates, best practices, and networking.

ONLINE DAILY

Top Tips for Staff: help your staff keep your organisation safe online

Our accessible cyber security training package is for organisations of all sizes and sectors.

CQC UPDATE – WHERE ARE WE NOW AND WHAT DO I NEED TO KNOW?

TUESDAY 2ND DECEMBER

In this update session, Hempsons head of social care, Philippa Doyle, will update you on the current CQC position regarding any changes to the quality statements and the Single Assessment Framework and what adjustments you might need to make in your service to prepare.

SMART CARE INTEL: LIVE DEMONSTRATION WEBINAR – TURN INSIGHT INTO ACTION IN ADULT SOCIAL CARE

TUESDAY 2ND DECEMBER

TUESDAY 9TH DECEMBER

MONDAY 15TH DECEMBER

Join Care England for a live walkthrough of SMART Care Intel – the new platform transforming how care providers, consultants, and commissioners drive quality, evidence compliance, and prepare for regulatory expectations.

In an increasingly complex regulatory and operational environment, SMART Care Intel offers clarity and control. Developed in collaboration with sector experts, the platform brings together tens of millions of data points from trusted sources to give you an unparalleled view of performance, compliance, and quality improvement.
This session will offer a practical demonstration of SMART Care Intel's key features, showing how the platform supports better care outcomes and operational confidence.
The live demo will cover:

- A "roadmap to outstanding care" with real CQC examples mapped to quality statements
- Tools to generate procedures, conduct self-assessments, and evaluate policies
- Mock inspection features to support CQC readiness
- A 6,000+ question quiz bank to build and test care staff knowledge
- Search and analysis across 100,000+ CQC reports
- Local benchmarking against other providers using live performance data
- Identification of service risks, trends, and improvement opportunities
- Alignment with the Single Assessment Framework, NICE guidance, and NHS best practice

Reserve your place today and see how SMART Care Intel can support your service in delivering, evidencing, and sustaining outstanding care.

FACEBOOK

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

Spread our page this CHRISTMAS!!

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