THE
CYBER
RESILIENCE
CENTRE
NETWORK

Personal Devices, WhatsApp & Data Sharing:

Are You Putting People at Risk?

Delivered on behalf of the CRC Network by:
Jim Stevenson, *Head of Cyber and Innovation*
Sapphire Little, *Business Development Manager*
Emily Bevan, *Community Engagement Lead*

THE
EASTERN
CYBER
RESILIENCE
CENTRE

WWW.ECRCENTRE.CO.UK

Agenda

Why personal device use can be risky

Social media and messing apps

Safe data sharing practices

The CRC Network – who we are & how we can help

How to get in touch

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Why is using your personal devices risky?

WWW.ECRCENTRE.CO.UK

Understanding the scale of the problem

Key facts

41%	of health or care organisations fell victim to cybercrime in the last 12 months	**58%**	cite cost as the main driver
50%	of care providers use BYOD; only half of those have a policy	**40%**	recall signing any policy/guidance
39%	of staff regularly use their own devices to store sensitive information	**70%**	of staff delivering face-to-face care are most likely to use personal devices. They also have high levels of access to the data of the people they support.

Stats from the UK Cyber Breaches Survey 2025, Digital Care Hub and The Department of Health and Social Care

What is BYOD and why is it growing?

- **Bring Your Own Device (BYOD) =** staff using their own phones, tablets or laptops for work tasks.
- Seen as a **flexible** and **low-cost option** for providers.
- Enables staff to **work remotely** and use **familiar technology.**
- COVID-19 **accelerated** personal device use.

But - BYOD brings extra cyber risks if not properly managed

Why care providers are a target?

- Care data is **high-value** e.g. medical history, personal details, and access information.
- **Tight budgets** and **limited IT support** make strong controls harder to maintain.
- **Staff turnover** and **agency work** mean personal devices are commonly used.

Cybercriminals exploit pressure – knowing providers need to keep services running

Why using personal devices can be risky

The impact:

- 41% of health and care organisations faced cybercrime in the past year.
- 1 in 4 UK data breaches involve health or social care data.
- 63% caused by human error.

Key message:

The National Cyber Security Centre warns that rapid BYOD growth often outpaces security controls - **poorly managed BYOD can expose sensitive client data and critical systems.**

BYOD isn't the problem - **unmanaged BYOD is**.

With the right policies, training and secure tools, providers can keep people and data safe.

Source The-state-of-BYOD-in-adult-social-care-2025.pdf

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Let’s play a game!

WWW.ECRCENTRE.CO.UK

Scenario 1 – Password reuse

Situation:

A staff member uses the same PIN or password for their personal phone and the work app they use for care notes.

Poll Question:

How risky is this? (Low / Medium / High)

Risk Level:

High

Why:

- If one account or device is compromised, attackers can access **both personal and work** information.
- Makes **unauthorised access** much easier.
- Increases risk of **data breaches** involving sensitive service user data.

Mitigation:

Use **unique passwords, MFA**, and a **password manager**.

Scenario 2 – Public Wi-Fi

Situation:

A staff member connects to public Wi-Fi at a café to finish entering care notes for a service user.

Poll Question:

How risky is this? (Low / Medium / High)

Risk Level:

High

Why:

- **Public Wi-Fi** can be **intercepted** by attackers, allowing them to **capture data** in transit.
- **Sensitive information** such as care notes or access codes can **be exposed.**

Mitigation:

Use a **secure VPN, mobile network**, and **ensure device software** is up to date.

Scenario 3 – Storing sensitive info on personal phone

Situation:

A staff member stores a service user's lockbox code, care instructions, or photos in a personal phone note app.

Poll Question:

How risky is this? (Low / Medium / High)

Risk Level:

High

Why:

- Personal note apps may not be **encrypted** or secure.
- If the phone is **lost, stolen, or hacked**, sensitive information is at risk.
- Even photos of documents or care plans can be **leaked accidentally**.

Mitigation:

- Only use **organisation-approved apps or secure platforms.**
- Ensure **strong device passwords and MFA.**
- Follow training and guidance for **secure data storage and sharing.**

Risks of social media and messaging apps

Many care staff use personal phones or apps like WhatsApp or Facebook to make calls, share updates, or access work tools - often to help people more quickly.

But even with the best intentions, these tools can create unintended risks.

Why can it be risky?

- **Personal devices** mix work and private data.
- **Photos or messages** about **service users** may be stored **insecurely.**
- **Free apps** aren't always designed for **handling care information**.
- Using **public Wi-Fi or weak passwords** can expose data.
- Many people don't realise when a **data breach** has actually occurred.

Key Message: These risks aren't about blame - they're about awareness.

THE CYBER RESILIENCE CENTRE NETWORK

How to share data safely

WWW.ECRCENTRE.CO.UK

Safe data sharing practices

Key principles for handling sensitive information

- **Share data** only via approved apps and platforms.
- **Avoid storing service user info** on personal note apps, messaging apps, or unsecured devices.
- **Use encryption for** emails and documents wherever possible.
- **Follow organisation-specific rules** for who can access or share data.

Goal: Protect both service users and staff while maintaining workflow efficiency.

Additional Guidance

- **Train staff regularly** on secure communication and data handling.
- **Ensure staff understand the risks** of using public Wi-Fi, free messaging apps, or weak passwords.
- **Apply technical controls** such as Mobile Device Management (MDM) to secure devices accessing work data.

Key Resources: NHS Data Security and Protection Toolkit & NCSC BYOD Guidance

What your policy should include

Core policy elements

- **Scope of Use:** Specify which devices, apps, and work tasks are permitted.
- **Security Requirements:** Strong passwords, multi-factor authentication (MFA), device encryption, and software updates.
- **Data Handling:** Rules for storing, sharing, and deleting sensitive information safely.

Further policy considerations

- **Staff Responsibilities:** Clear guidance on protecting service user and organisational data.
- **Incident Reporting:** Steps to report lost/stolen devices or suspected data breaches.
- **Monitoring & Compliance:** How usage is monitored and consequences for non-compliance.
- **Training & Support:** Ensure staff receive ongoing guidance and support for secure device use.

Tip: Align your policy with **NCSC BYOD guidance** and **NHS Digital standards** to maintain security across all data sharing activities.

Key resources to help you create a BYOD policy:

NHS Data Security and Protection Toolkit

Online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

NCSC BYOD Guidance

Guidance for organisations on how to choose, configure and use devices securely. Includes platform guides and policy recommendations

CRC Network Training

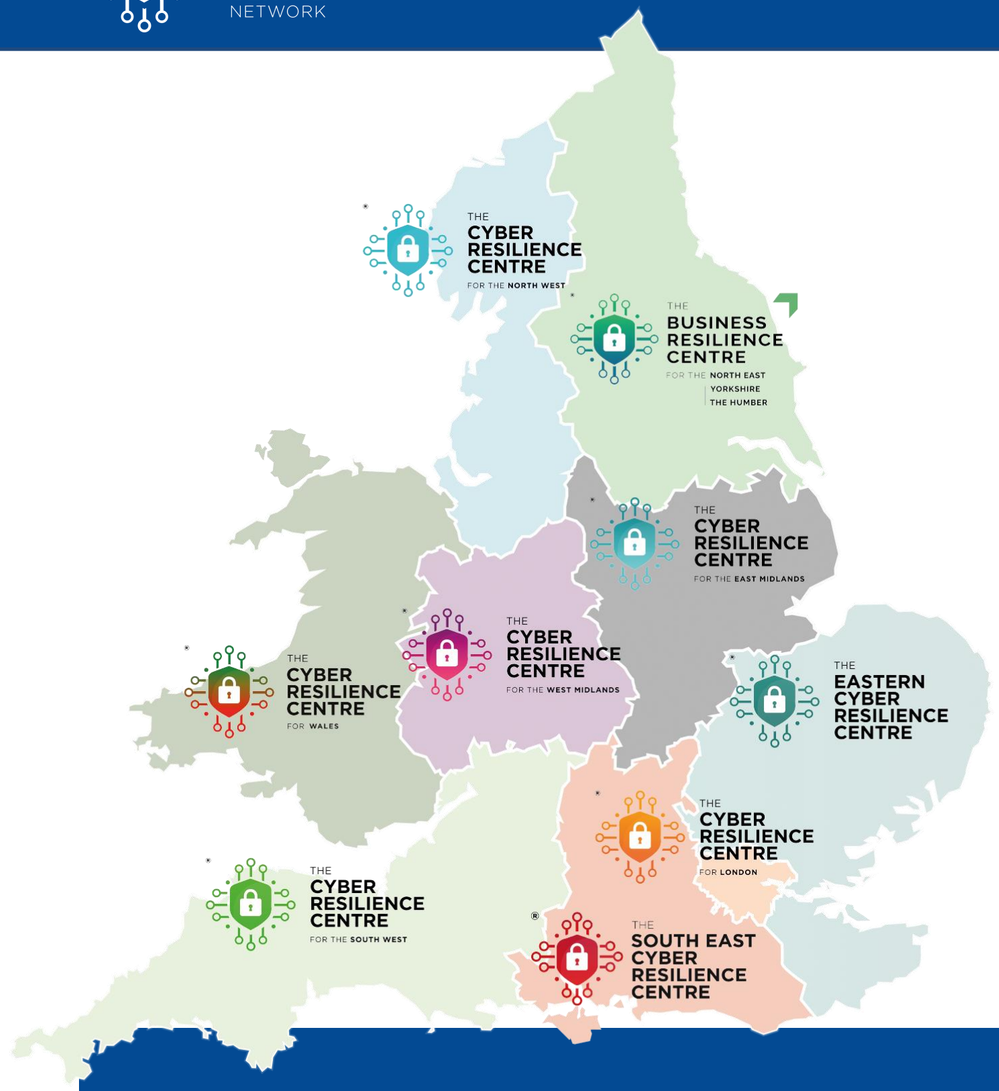
To help you understand the current threat landscape and tactics used by cybercriminals so you feel confident in recognising and drawing attention to any potential security issues.

THE
CYBER
RESILIENCE
CENTRE
NETWORK

How can the CRC Network support your organisation?

WWW.ECRCENTRE.CO.UK

How can the CRC Network help?



The CRC Network

- Cyber Resilience Centre Network
- Police led, government funded network of centres
- Collaboration between Policing, Industry Experts and Academia

The ground we cover

- Small and Medium Organisations
- Charities
- Schools

Free membership

- Free membership which includes newsletter, educational customer journey, signposting to free tools

Our aim:

To increase the cyber resilience of small and medium businesses, charities and the third sector

Police-led, **Business**-focused

CRC Membership

Provides members with:

- **Regional and national threat alerts**
- **Monthly Newsletter** featuring the latest guidance
- **Signposting to free tools and resources** from Cyber PATH, policing and the NCSC
- **Funded Cyber Security Awareness Presentations/webinars** to staff, customers and supply chain
- **Access to a wide range of Cyber Security Services** via our Cyber PATH programme including training, vulnerability assessments, Microsoft 365 reviews etc.

We have nine Cyber Resilience Centres across England and Wales

Four things to remember

Use only approved apps and platforms

Follow your organisations policy and Think before sharing, try not to mix personal and work data.

Strong passwords & MFA protect sensitive info

Even if a password is compromised, MFA adds an extra layer of security.

Review your BYOD policy

Ensure it reflects current risks, staff practices, and the latest security guidance.

Sign up for our Newsletter

To continue to receive the latest police guidance around cyber crime and access a wealth of resources.

Links

Reporting a suspicious website https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

Reporting a suspicious email forward to report@phishing.gov.uk

Reporting a suspicious text message send to 7726

Check your compromise www.haveibeenpwned.com

Cyber Action Plan www.ncsc.gov.uk/cyberaware/actionplan

The ECRC

www.ecrcentre.co.uk

https://www.linkedin.com/company/the-eastern-cyber-resilience-centre/

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Thanks For Listening

Any Questions?

Upcoming webinars in the Care sector Cyber series:

Spotting Human Error: Building a Cyber Aware Culture in Care

18th November 12-12:30pm

WWW.ECRCENTRE.CO.UK