DSPT
Better Security.
Better Care.

Digital
Care Hub

The PSC

The state of Bring Your Own Devices (BYOD) in the Adult Social Care sector

Published October 2025

Content

- Executive summary
- About this report
- Case for change
- Aims of this report
- Research methods
- Understanding the current state
- Detailing the risks
- Outlining improvement measures
- Conclusion

1. Executive summary

Executive summary (1/5)

In January 2025, the Digital Care Hub, which hosts the Better Security, Better Care programme, commissioned The PSC to conduct a nine-week discovery to understand the current state of Bring Your Own Device (BYOD) approaches in Adult Social Care (ASC), explore the risks associated with the current state, and recommend improvements measures to begin to address the risks.

The Better Security, Better Care programme is funded by the Department of Health and Social Care.

1. Case for change

- Bring Your Own Device (BYOD) approaches have become increasingly popular in the Adult Social Care Sector as they allow organisations to reduce the costs associated with providing staff with devices.
- While there is data on the extent of BYOD usage in ASC available from 2021, uptake has likely increased significantly since then, meaning that little is known about the current extent of usage. As well as questions of extent and distribution, additional gaps in knowledge exist around what devices are used for, what policies and technical controls are in place, and what the risks associated with these might be.
- Anecdotally, there have been reports of BYOD creating risks to data protection and cyber security, but little is known about the scale of these risks due to the shortage of data.
- Social care already experiences higher numbers of data breaches than other sectors (with the consequences being potential fines and reputational damage) and the insecurities that can be created through BYOD can compound these problems.
- As BYOD approaches look likely to stay in social care, we must understand the current state and ensure improvements are in place for the cyber security of the sector.

Executive summary (2/5)

2. Aims of the report

This report aims to offer three main contributions:

i. A detailed review of the current state of BYOD usage in the ASC sector, encompassing the extent and distribution, the types of usage, user perspectives, organisational policies, and the existing technical controls that can be leveraged for security.

ii. An analysis of the risks involved with BYOD, with the aim of developing a sorted list of risks that considers where the risks arise, how frequently, who they affect, and how they consolidate.

iii. A list of improvement measures that address the outlined risks, prioritised by the magnitude of their impact and the effort involved in their implementation.

3. Research methods

- Our desk-based research phase explored prior research into the extent of BYOD in ASC, as well as later in the project, into examples of technical best practice
- We shared a survey on BYOD which received a total of 775 responses, divided between 606 managers and 169 staff. The survey has two branches to gain input from organisational managers and staff. The number of responses make our survey the largest conducted on BYOD usage in ASC.
- We hosted a provider workshop to understand experiences of BYOD in detail, which was then supplemented by 7 further 1-1 interviews with providers and 11 interviews with staff
- We also completed 7 interviews with technical and policy experts to discuss what BYOD best practice looked like; assisting us in our process of formulating improvement measures

Executive summary (3/5)

4. Understanding the current state

- We found BYOD is more prevalent amongst smaller providers and home care organisations.
- Cost is the primary driver of BYOD adoption, with 58% of respondents citing this as a reason.
- Phones were the most common BYO Device, with 97% of individuals following BYOD using personal phones.
- Personal devices were used at work for a variety of purposes, but most often for specific care applications as well as generic communications ones; raising concerns about patterns of blended usage.
- Technical solutions to ensure security already exist but are not well adopted within the sector, with only 20% of organisations availing of Mobile Device Management (MDM) solutions.
- Similarly, specific BYOD policies only existed in 50% of organisations following a BYOD approach (50% of the total sample), with only 40% of staff remembering having signed a policy that governs their personal device usage, even so, many of them still use their BYOD in a non-compliant way.
- 70% of staff surveyed reported they would prefer to use organisation-provided devices, raising in the interviews questions around the equity of paying for mobile data used at work.
- Over 70% of managers surveyed perceived BYOD to pose a 'low risk' to the security of their organisation, with only a handful reporting data breaches. Interviews however illuminated that due to managers not interpreting situations correctly as data breaches, the actual numbers may be much higher than reported.
- Staff interviews highlighted various high security risks such as using devices to take photos, accessing care software through public WiFi and communicating service user data in WhatsApp groups.

Executive summary (4/5)

5. Detailing the risks

- Analysis of risks began through developing a comprehensive list of risks and contextual reasons for them to arise. We categorised reasons into: limited knowledge of risks, limited understanding of secure practice, cost restricting security, and insufficiently secure technical solutions.
- We accessed the frequency of these risks occurring alongside reflections on whom these risks affect most. At present, service users (an already vulnerable group) as well as staff are highlighted to experience risks most frequently.
- Into the future, providers may begin to face greater consequences - such as potential fines and CQC inspection markdowns - if non-compliance becomes better regulated.
- Risks also overlap and consolidate, highlighting that small providers who face financial constraints and lack in-house IT or data protection specialist knowledge see the highest risks of data breaches.

6. Outlining improvement measures

- We developed a list of improvement measure to address key pain points in different points of an organisation's BYOD adoption journey.
- We prioritised the list against two criteria: the scale of impact (considered as the number of providers affected and the number of risks mitigated) and the "effort" involved in implementation (capturing the cost of the measure, the number of actors involved, and the timescale of implementation).
- We identified four measures which carry high impacts but require low levels of effort as the areas for immediate action (next slide).

Executive summary (5/5)

Top 4 measures to take forward in the short to medium term

"Have you thought about this risk as part of BYOD" guide

BYOD guidance product including a specific policy development tool that can be tailored to organisations

A "what technical solutions does my organisation need?" interactive tool, plus advice on the security features providers might want for each of their technical solutions

Educational piece illustrating bad practice and highlighting consequences

7. Conclusion and next steps

- Our conclusion brings together each section of the report; emphasising the prevalence both of BYOD within the ASC sector, but also insecure behaviours.
- It outlines the risks, who they affect, and how they consolidate to create particular patterns of vulnerability.
- Finally, some improvement measures are proposed that look at increasing education and awareness both of the risks associated with BYOD and of what secure practice looks like.
- As a series of next steps, we recommend that BSBC decide how many of the recommendations they are ready to take forward now and to reflect on what internal and external resources they might need to mobilise to facilitate these.
- The long-list of measures should be revisited regularly to see a process of continuous improvement of BYOD security.

2. About this report

About this report

This report was written by The Public Service Consultants (The PSC). Founded in 2006, we are the UK's longest-standing specialist public services consultancy. For 18 years we have been privileged to support a wide variety of clients across health, social care and central government, driven by our mission to make public services brilliant. Our work spans three main areas:

The PSC Digital

- Digital and futures research
- Service development (Discovery / Alpha / Beta)
- Data, Digital Strategy, and AI

The PSC Strategy

- Investment cases
- Health and Care capital development
- Clinical Model Innovation

The PSC Transformation

- Performance Transformation
- System-wide Transformation
- Capability Transformation

For more information contact hello@thepsc.co.uk

3. Case for change

What is Bring Your Own Device (BYOD)?

Bring Your Own Device (BYOD) refers to the practice of allowing or encouraging staff to use their personal devices (e.g. phones, laptops, tablets) to complete some or all of their work

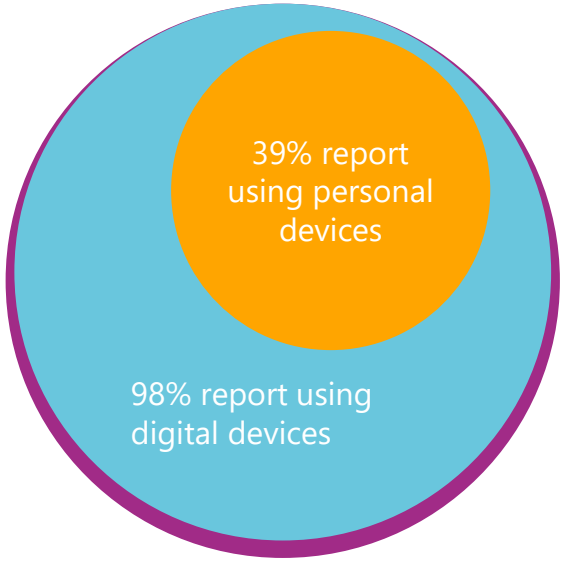
BYOD is perceived by some to be a 'win-win' for organisations and employees, where organisations save on the cost of providing devices and enable their staff to work 'flexibly' (i.e. not just while at the main premises), while employees are able to use technologies that they are familiar with

COVID-19 has been identified as a key driver of the increasing popularity of BYOD approaches due to the need to move beyond traditional ways of working

The National Cyber Security Centre do however observe that the practices that have facilitated the rapid expansion of BYOD may not be sustainable due to their insecurity. While BYOD may bring organisations benefits, it also creates new risks and challenges around security

In 2021, an NHSX report highlighted that BYOD usage is prevalent in Adult Social Care (ASC)

The NHSX Technology and Digital Skills Review 2021 has comparatively the best information available on BYOD in ASC in England. Using a sample of ~500 providers, it finds:



When combined with the Skills for Care workforce data, these figures see **a total of 650k personal device users:**

The report also finds that **care setting**, **employer type**, **digital development** level and proportion of **agency staff** were all found to influence the prevalence of BYOD usage

However, personal devices are riskier than corporate devices, particularly in the ASC context

BYOD risks arise from devices being **less regulated**, **blended with personal use**, and having **lower levels of security**. Personal devices might also be at great risk of **loss or theft** given their greater use compared to organisation provided devices

Adult social care also carries some particular risks in relation to BYOD usage:

- Data is highly sensitive (e.g., medical history, protected characteristics).
- On average, knowledge of cyber security across the sector is low, meaning providers are not always informed to use secure software.
- Policies on secure use of personal devices are often reactively developed in response to incidents.
- Tight budgets mean that cost often leads decision making.
- Staff report having low digital skills and digital confidence.

However - simply banning BYOD is not the right solution. Some staff need to use their own devices due to their contracts, because they are agency staff under IR35, and others simply prefer to. The key is therefore to ensure that risks which come with BYOD are understood and mitigated.

We need to understand the current state of ASC BYOD in order to improve its security

Why we need a better understanding of BYOD in ASC:

- The National Cyber Security Centre sees BYOD approaches as here to stay.
- At present, we know BYOD approaches in adult social care are prevalent but there is much less knowledge about actual usage and the associated risks.
- There is also anecdotal evidence that these approaches often operate without specific policies, training, or appropriate technical controls to govern their use.
- Given the types of data worked with in Adult Social Care and the vulnerability of service users, the consequences of data breaches are great.

This means:

- We need to better understand how BYOD approaches **play out in practice** and the **risks associated** with these patterns of use. This will allow us to develop the **recommendations** needed to bring BYOD usage in line with the recommendations made by **Better Security, Better Care**

Not managing BYOD risks may result in damaging data breaches and fines for providers

Health and social care is consistently one of the most affected sectors for data breaches. ICO data from 2019-2023 highlights that over 1 in 4 data breaches are of health and social care data

211 digital data breaches reported by the ICO in the social care sector between 2019 & 2024 (ICO 2024)

→ **63%** of these were attributable to human error

900 people receiving care at home had the details of how to gain entry to their houses leaked in a 2022 ransomware attack

→ **£6 mil** fine issued to the IT provider involved in this incident (ICO 2024)

While this data is not specific to BYOD, it demonstrates the pre-existing vulnerabilities within the social care sector and the consequences that come from insecure digital practices

4. Aims of the report

We will develop improvement measures through understanding the risks arising from the current state

Section:	What will be addressed:
Understanding the current state	Through the survey, workshop, and interviews, we will develop a picture of the current state which answers questions of extent, distribution, usage practices, and the policies and technical controls in place to govern risks
Detailing the risks	From this view of the landscape, we will address the risks; exploring the means through which they arise, the frequency with which they occur, who they affect, and how they stack/coalesce
Outlining improvement measures	With our knowledge of the current state and the associated risks, we will propose a series of prioritised improvement measures, examining how we can have the greatest impacts while accounting for the limited resources available in the ASC sector

5. Research methods

775 individuals working in care responded to the research survey, and we gained more insights through 1-1s & workshops

Existing research

We reviewed all available data and reports on BYOD usage in ASC and researched regulatory contexts, technical solutions, and best practices

Care providers

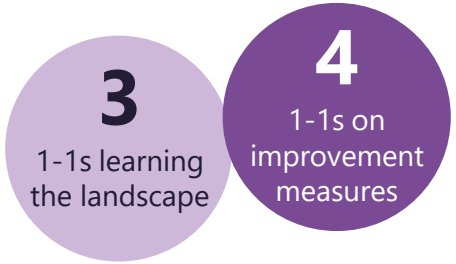
Our main methods for engagement with care providers were a survey and interviews, to capture both quantitative and qualitative feedback

Staff working in ASC

We had 169 staff working in care organisations respond to our survey and we conducted 11 interviews with staff working across a variety of care settings

Expert 1-1s

In addition, we conducted 7 interviews with experts across the policy and technical landscape to understand the constraints of the sector and what best practice looks like



Full detail on our methodology is available in the appendix

6. Capturing the current state

These are the elements we needed to capture in order to understand current state

Extent and distribution

- Distribution of BYOD across:
  - Care settings
  - Organisation types
  - Organisation sizes
- Drivers of adoption

Types of usage

- Devices used
- Applications / software used
- Tasks completed
- Types of data accessed and generated

Users

- Choice to use own device
- Who the cost of BYOD sits with
- Preferences for BYOD

Organisational policies and knowledge

- Stage of policy development
- Means of implementation
- Staff engagement with policies
- The existing regulatory landscape

Evaluation of risks

- Manager and staff awareness of risks
- Number of incidents
- Desired security improvements

Existing technical controls

- Mobile device management
- Mobile application management
- Quality applications
- Additional features

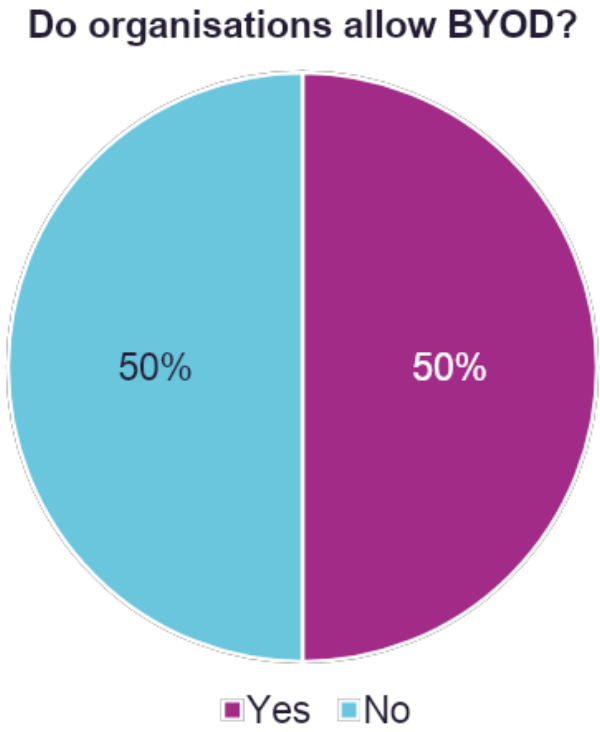
BYOD approaches were reported in 50% of surveyed organisations

Respondents	#
Total managers	606
Total staff	169
Total respondents	**775**

Of the 606 managers, 303 (50%) reported that their organisation followed a BYOD approach

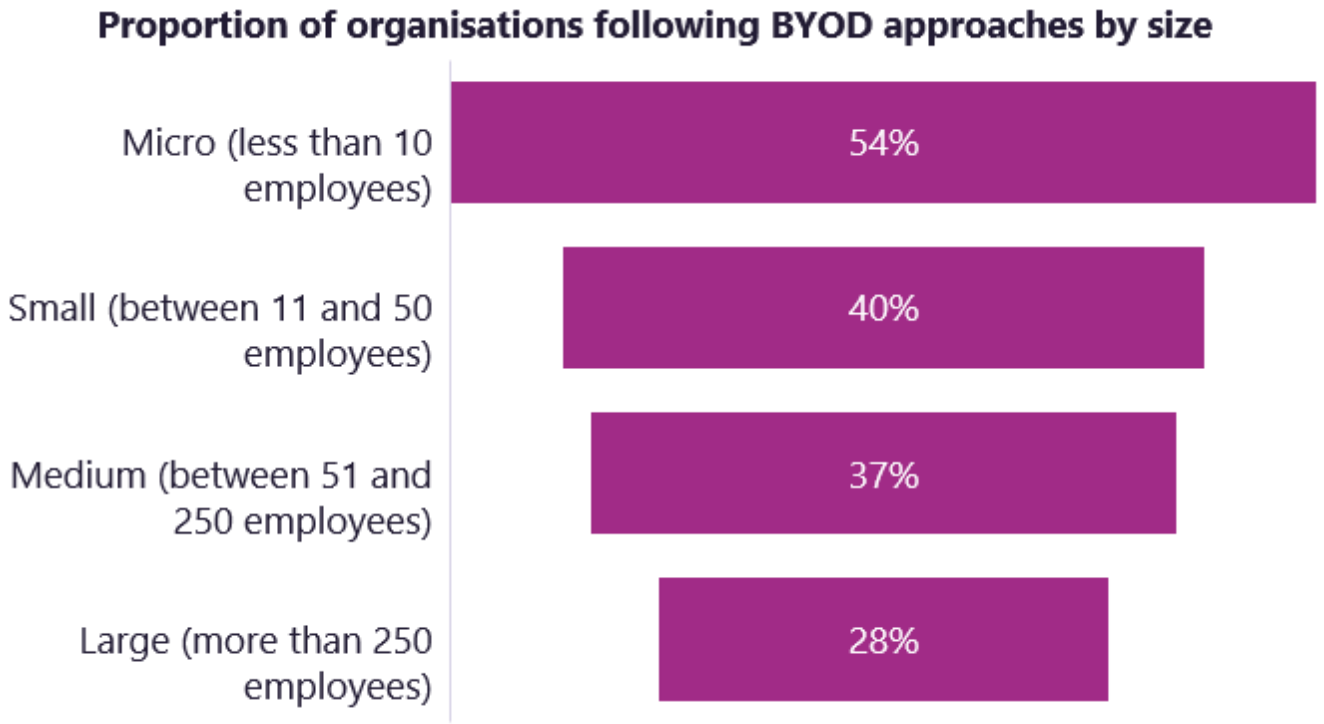
In organisations without BYOD, only 25% suggested they would consider its use in future

Of the 169 staff, 79 (47%) reported using personal devices in their work



Extent and distribution

BYOD approaches were more common in smaller organisations



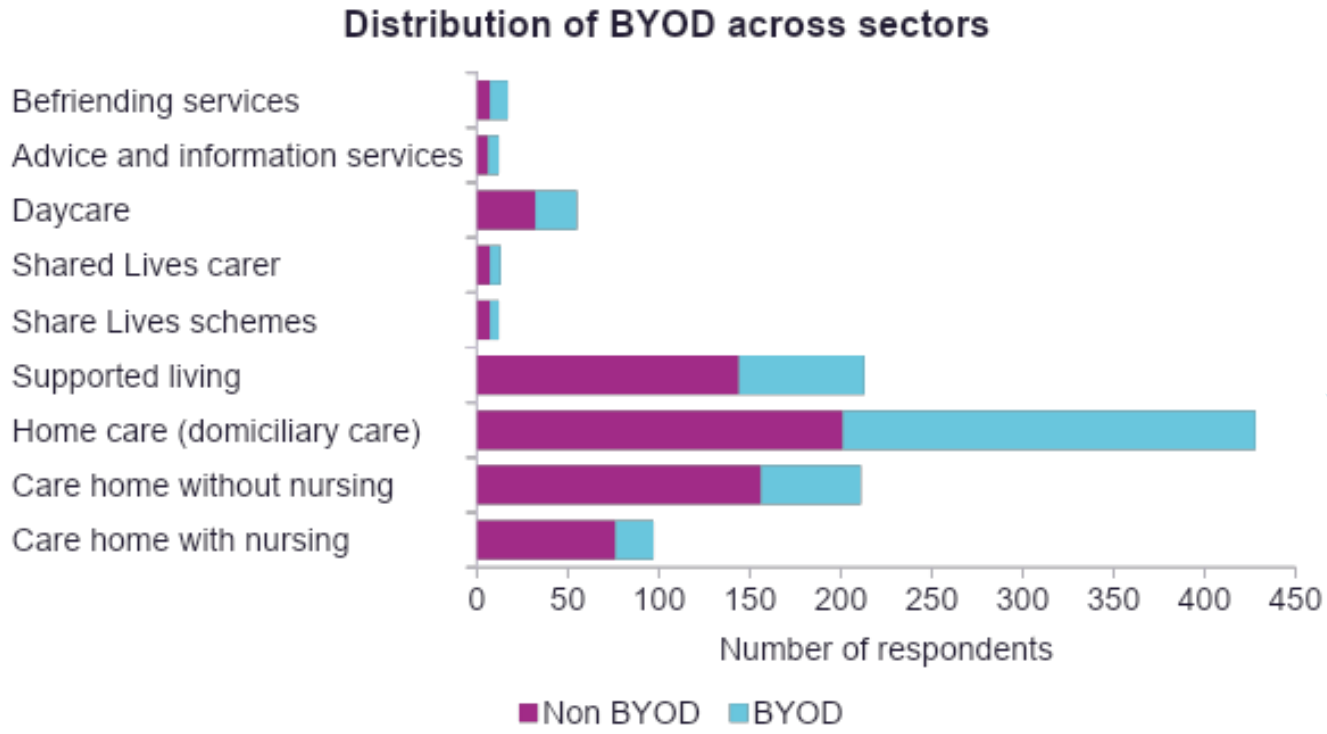
BYOD approaches became increasingly common with the decreasing size of organisations

From our interviews, we learnt that small organisations were typically motivated to follow a BYOD approach due to cost

In larger organisations where cost was less of an issue, devices were more frequently provided to staff

Extent and distribution

Home care saw the highest density of BYOD usage



Of the major care settings, BYOD was most prevalent in home care, with **53% of respondents in this category reporting the use of personal devices**

This finding agrees with the NHSX Technology and Digital Skills Review 2021.

Our results also illustrate the home care organisations are disproportionately smaller than other care organisations; which we know to correlate with increased BYOD usage

Extent and distribution

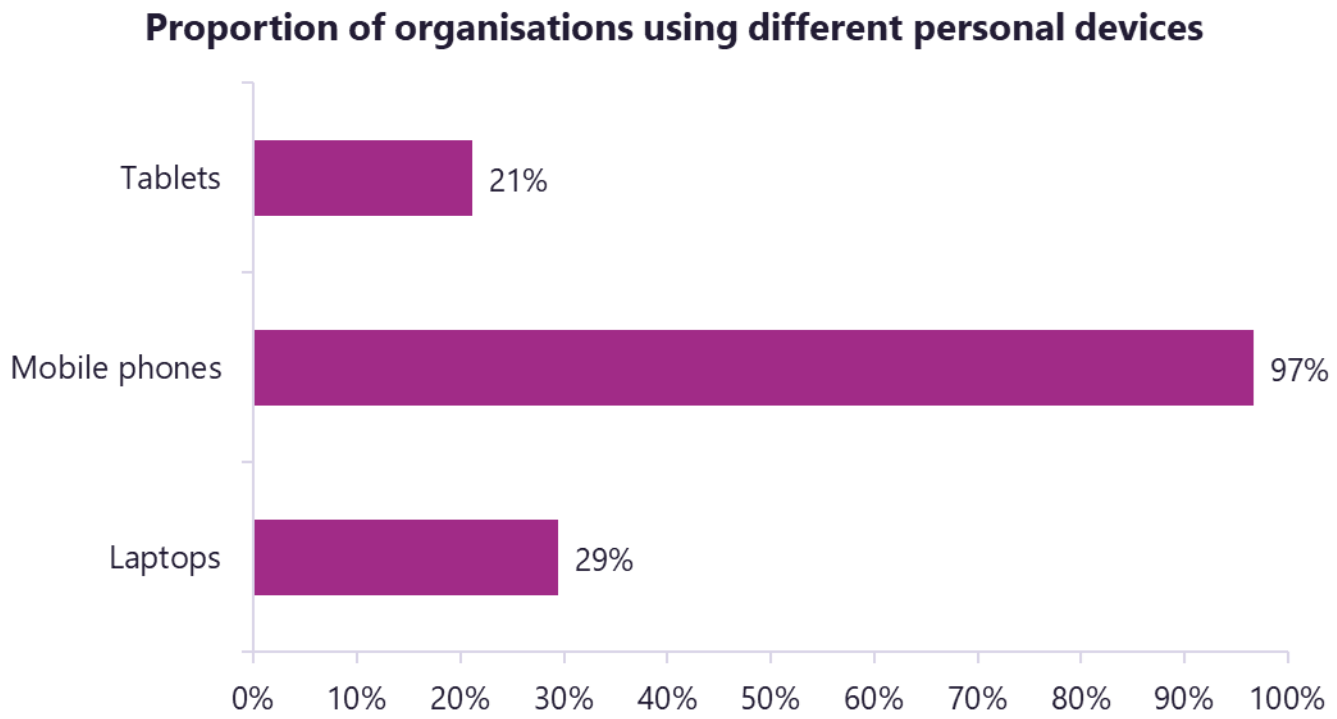
The leading driver of adoption was cost

Cost was the **primary driver** for adoption with 58% of managers mentioning this option

40% of managers also reported that BYOD usage came about because of staff preferences – **a finding we do not find support for amongst staff responses!**

Extent and distribution

Phones were the most popular BYO device



Of the organisations who followed BYOD approaches, **97% used mobile phones,** with much smaller proportions using tablets or laptops

In interviews, it became apparent that phones were typically used by staff delivering frontline services, while other technologies were used by managers

Types of usage

Very few organisations use MDM

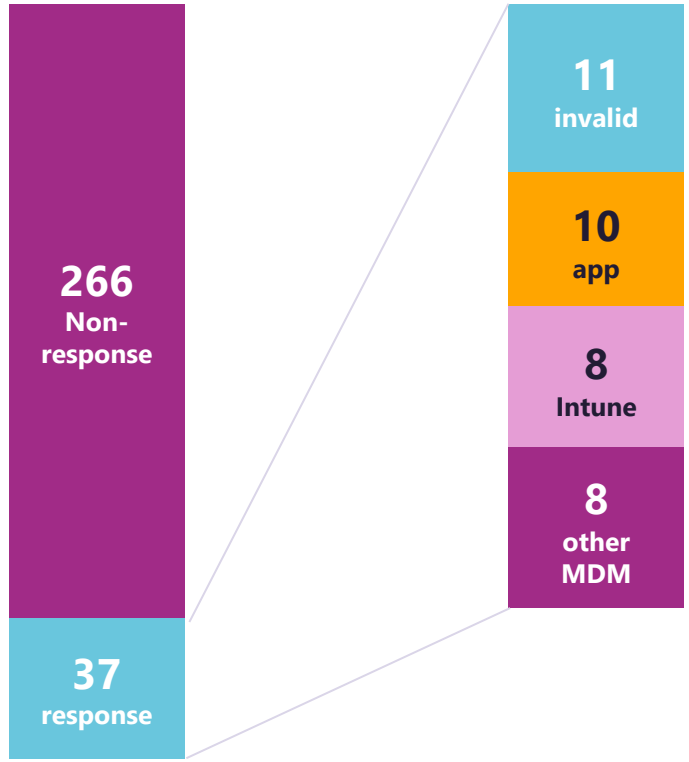
In our survey, we asked, **if respondents used Mobile Device Management approaches, which software they used to facilitate this?**

Only 37 out of 303 **(12%)** managers with BYOD responded to this question

11 of these gave responses which did not address the question (perhaps indicating limited digital knowledge) and another 10 left the name of the application used rather than MDM software

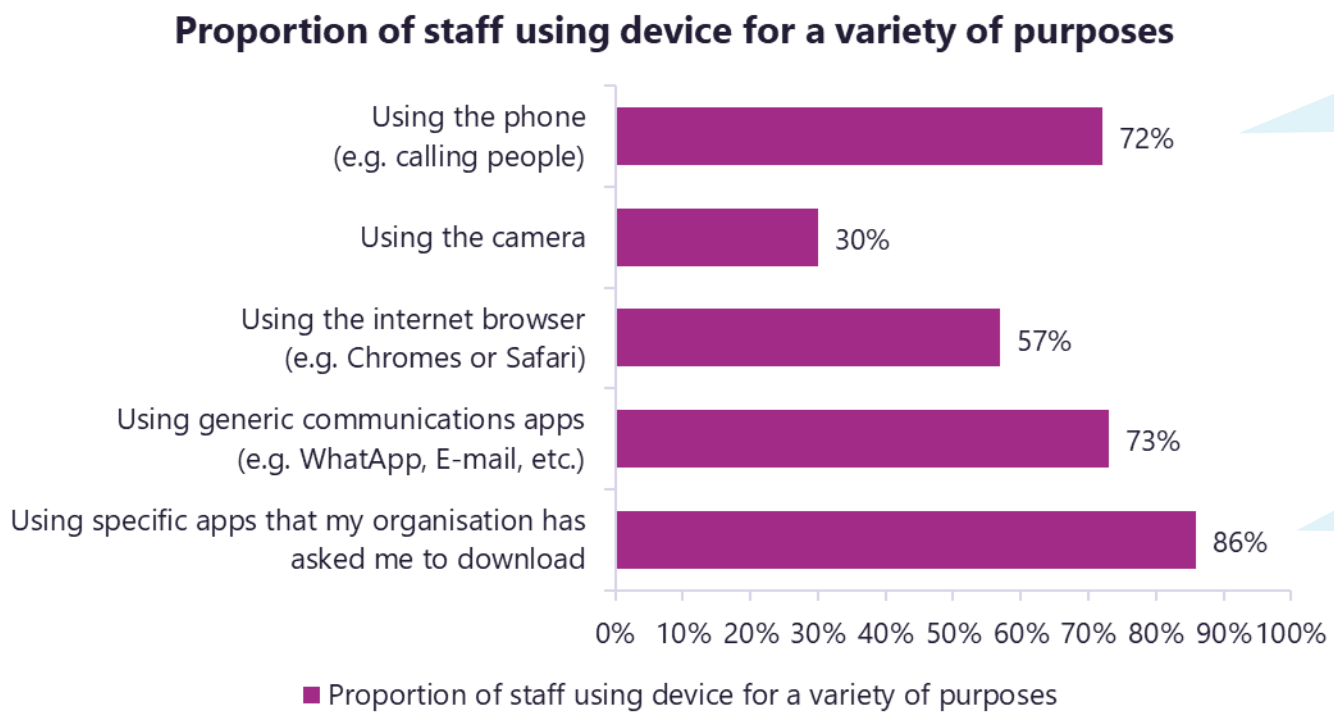
Of the 16 providers who provided valid answers to the question:

- 8 mentioned Microsoft Intune as their MDM approach
- The remaining 8 reported the use of a range of different management systems



Types of usage

Staff use their personal devices for a variety of purposes to complete a diverse list of tasks



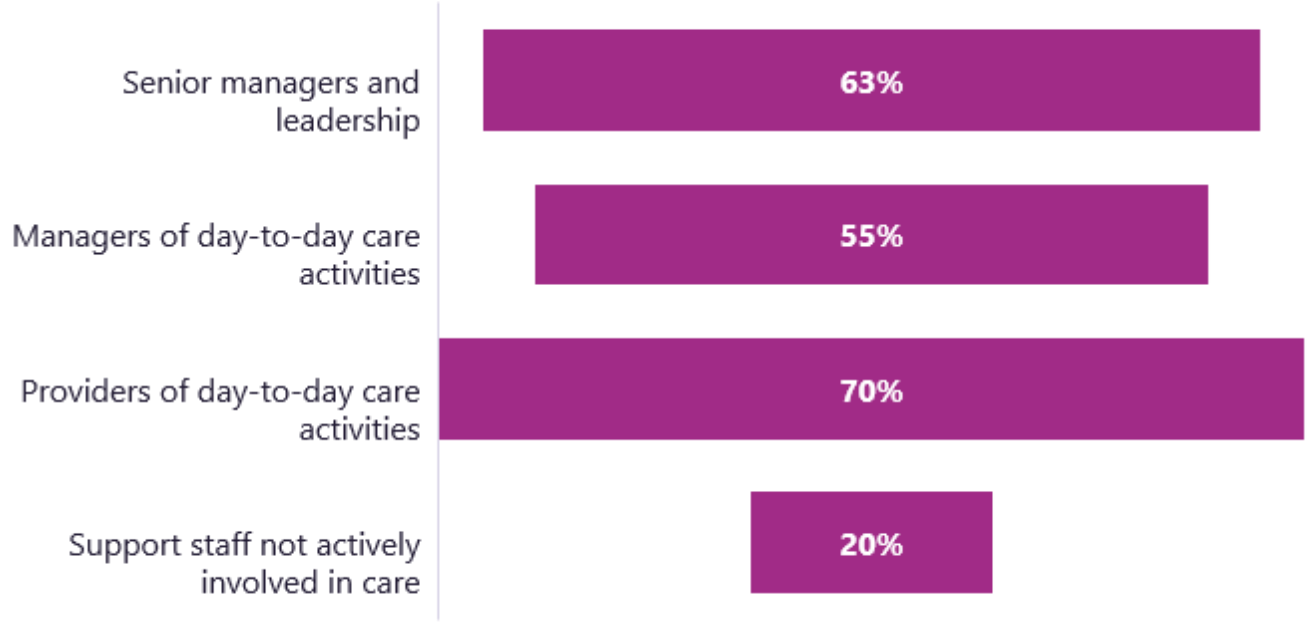
In interviews, staff expressed concerns about their personal phone numbers being shared with other healthcare professionals to communicate about service users

Specific care and **generic communications apps** (e.g. WhatsApp or phone calls) are what personal devices are most frequently used for – with the latter raising concerns about blended usage

Types of usage

Managers and those involved in day to day care most likely to use personal devices

Proportion of different staff groups using personal devices in organisations where BYOD is permitted

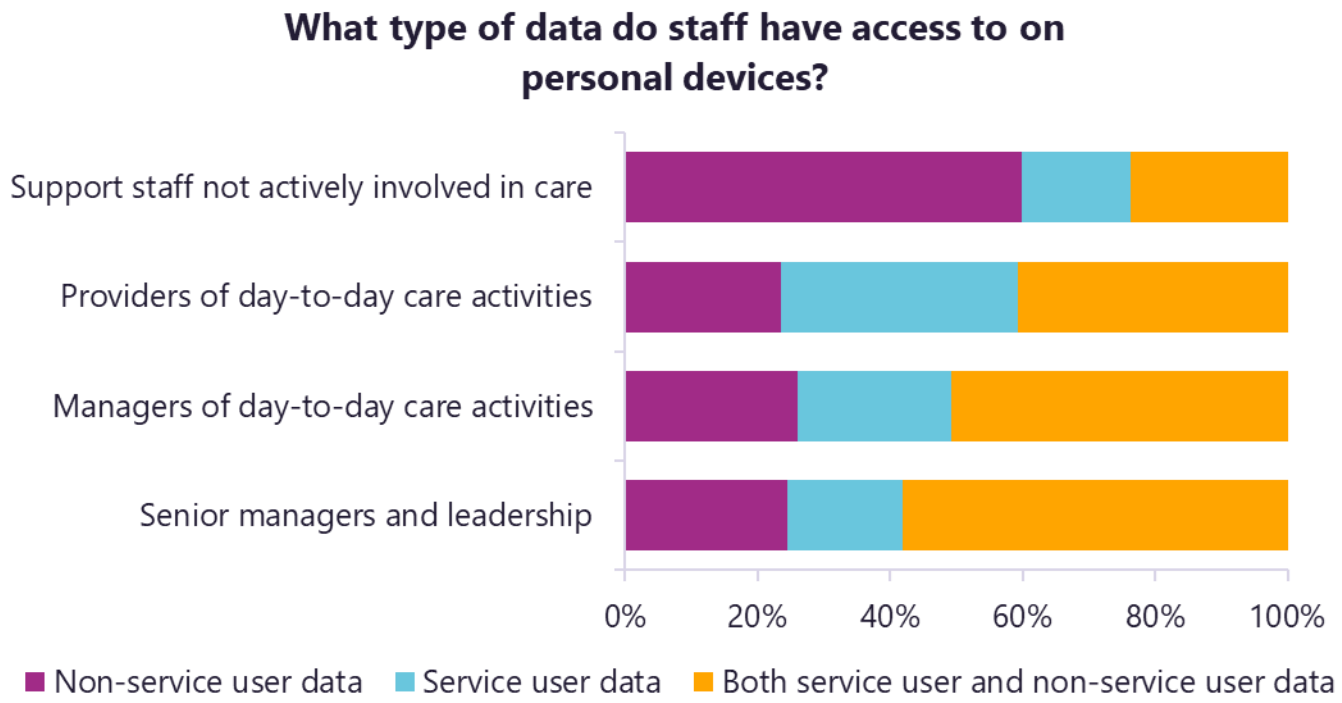


The key BYOD user groups were those **directly involved in care** and **senior managers** - groups identified by the NHSX Technology and Digital Skills Review 2021 to have two very different digital skill profiles

We heard in interviews how devices were used differently dependent on seniority. While managers used personal devices to work flexibly (e.g. checking emails from home), personal devices were central to the work of care / support workers

Types of usage

These groups also are most likely to have access to patient-data systems



A surprisingly large proportion of support staff are reported to have access to service user data, likely creating additional risks through unnecessary sharing

Senior managers and providers of day-to-day care are also the most likely to have access to patient data systems on personal devices

Types of usage

Staff members' ability to choose to use their own devices is often restricted

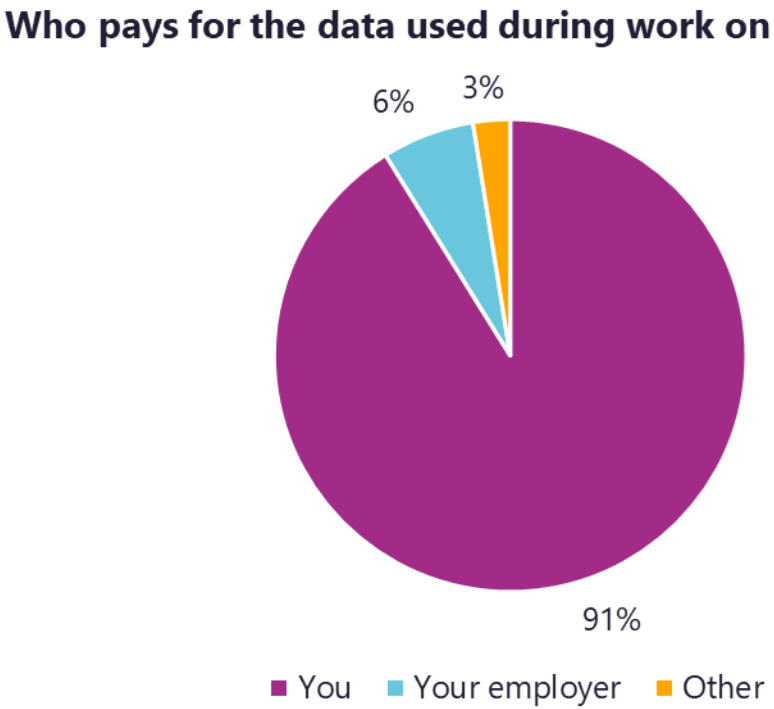
10/11 staff members interviewed described having a phone as a condition of their employment. Some had asked for an organisation provided device and been refused

One provider mentioned giving her staff the choice of an organisation provided versus a personal phone and no one had yet chosen an organisation-provided one

We wondered whether this option would only be the case amongst providers who have sufficient financial margins to purchase devices

Users

The cost of BYOD often falls onto staff members, with most paying for their own data / maintenance

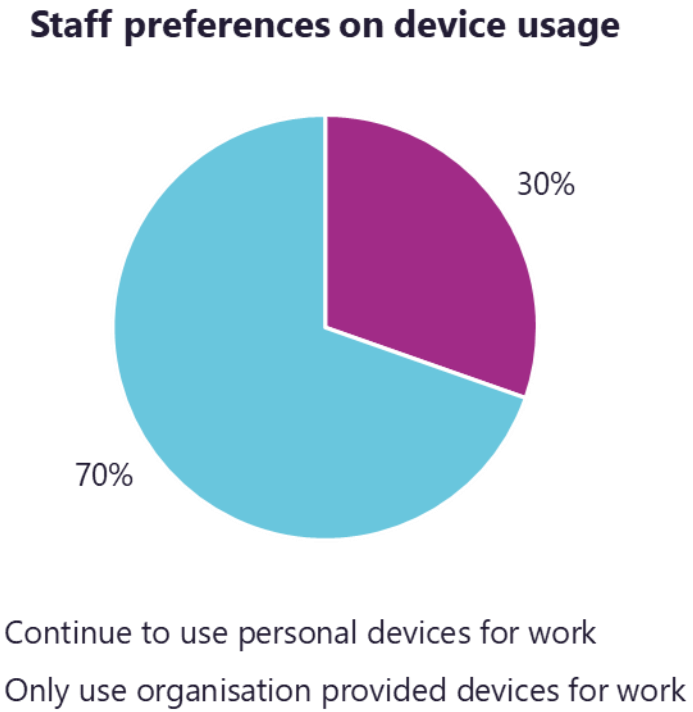


In 1 of the 11 staff interviews, a staff member mentioned that they were currently being given an additional £5 per month in salary to partially cover their data costs. The others received no support

One staff member described their phone screen breaking during a work incident. They asked their employer about help repairing the screen, but they were told it was their responsibility to have a working phone

Users

70% of staff currently using personal devices would prefer to use organisation provided ones

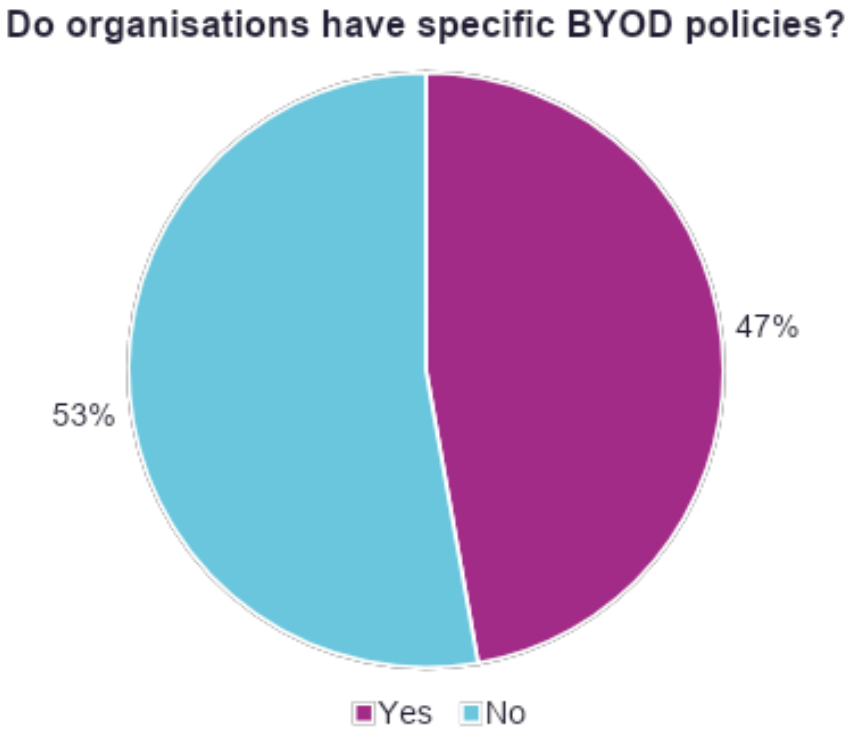


Despite managers reporting that staff preference is an important driver for adopting BYOD, **we see the opposite from front line respondents**

Interview participants responded emphatically to **preferring an organisation provided device**, or as an alternative, fair reimbursement for the money they spent on their data plans / phone maintenance

Users

Fewer than half of organisations have a specific BYOD policy in place



Under 50% of organisations responding to the survey had **distinct BYOD policies** in place

Even when organisations do have policies in place, we heard from providers that these are sometimes imported from other settings and are not tailored to organisational usage

Organisational policies and provider knowledge

Most organisations rely on passive management policies rather than active controls

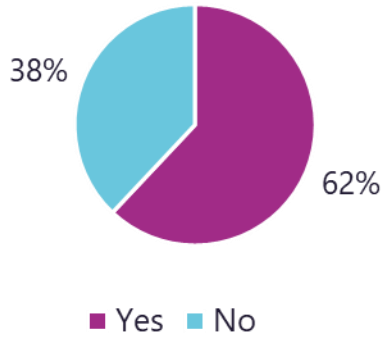
Of the organisations who did have policies, many followed **passive approaches** e.g. getting employees to sign a contract

A smaller proportion of organisations trained their employees about BYOD security (a concern we heard echoed in staff interviews) and **fewer still used technical controls like MDM (21%)**

Organisational policies and provider knowledge

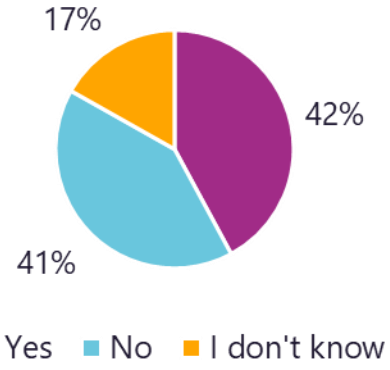
Staff knowledge of and engagement with the policies is limited

Are you aware of an organisational policy that covers the personal devices you use at work?



62% of staff who followed a BYOD approach were aware their organisation **had a policy** specific to its use, however leaving a large proportion **(38%) unaware of policies** or in organisations without them

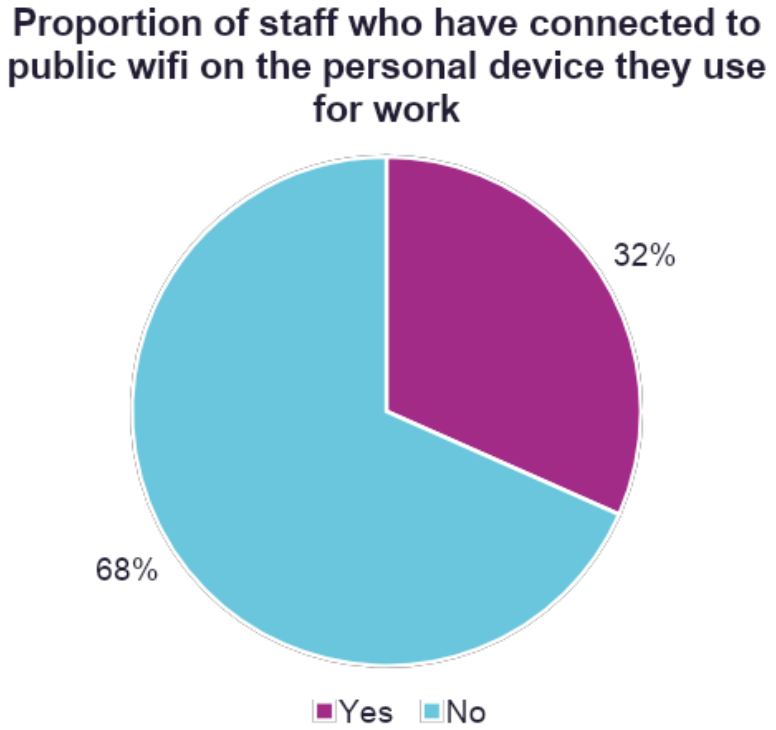
Did you have to sign a document / agreement in order to use your personal device at work?



A smaller percentage of staff still **(42%)** were clear that they had **signed a policy** about the usage of personal devices at work

Organisational policies and provider knowledge

The existence of policies only partially reduced the frequency of risky behaviours



We were interested to see whether having an organisational BYOD policy reduced the percentage of people who connected to insecure wifi networks and we did find an association:

- **32% of the overall sample did**, however:
  - Only **24%** of those in **organisations with policies** did
  - Compared to **43%** of those **without policies**

This suggests policies are a good first-step in changing staff behaviour, but need to be underpinned by technical controls to ensure safe practice

One IT manager described encouraging staff to comply with policies as a **"war of attrition"**

Organisational policies and provider knowledge

The existing regulatory landscape does not make BYOD security a priority

Adult Social Care as a sector is broadly regulated by the 2014 Care Act which is a 167 page document with no mention of cyber security or data protection.

The 2014 Care Act informs the evaluations of the CQC, who do investigate data protection and information governance, however they have no power of enforcement. As the CQC is the core regulatory body in care, the limited focus on data protection, and absence of regulatory criteria on BYOD approaches mean that providers do not view secure practice in these areas as a priority.

All care organisations *should* be registered with the ICO who do have the power to issue warnings and fines. Despite numerous recorded data breaches, the ICO have not yet issued any large fines to the social care sector due to the financial strains.

We heard from providers that their main motivator beyond delivering high quality care was **CQC compliance** as this had the greatest effects on their reputation and ability to operate.

One provider described reporting data breaches to the ICO with **little consequence** as although data had been breached, it had not resulted in any harm or financial loss.

Organisational policies and provider knowledge

Provider knowledge of the risks associated with BYOD can vary significantly - case studies

High awareness example

- Provider was a large care charity (>3,000 employees) with a dedicated IT team
- BYOD policy developed specifically for the organisation based on collating other organisations' policies
- Policy exists as a live document
- Development of specific BYOD training module to educate staff
- Election of "staff champions" to highlight risks and best practices amongst staff
- Regular circulation of material relating to BYOD security

Low awareness example

- Provider was a medium sized domiciliary care organisation
- Policy taken from a basic template; only changes are the necessary operating system updates
- Staff sign policy at the start of their employment, but there are no processes of continuing education
- Business as usual involved insecure practices such as the use of large WhatsApp groups for company comms
- Risks of BYOD downplayed and service user data described as "boring"

Evaluation of risks

Staff demonstrated a limited understanding of the risks associated with certain practices

73% of staff report having **no concerns** about the security of using their personal device for work, however significant percentages reported:

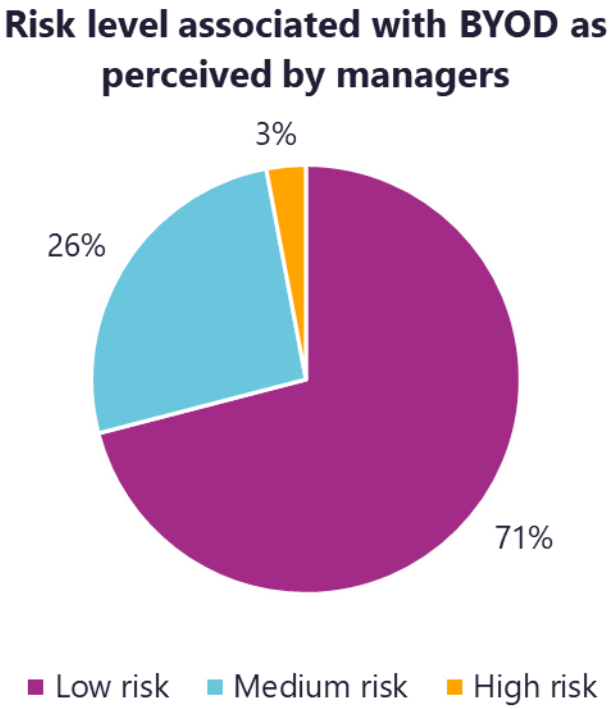
- The use of generic communications applications e.g. WhatsApp and Outlook which – without adequate MDM measures (73%) – create risks through blended usage (e.g. sending service user data to the wrong recipient)
- Connecting to insecure wifi networks – generating risks of data being decrypted and information such as service user addresses and lockbox codes being breached

Staff described the key issue relating to photos taken at work being that they occupied phone storage **– not recognising that having these images on personal devices constituted a data breach**

One staff interviewee described how their organisation used an application that did not have an effective offline mode, and due to bad mobile data coverage, **staff frequented the local supermarket to make use of the public wifi there.** This behaviour was framed by the interviewee as a solution rather than a risk

Evaluation of risks

BYOD was however perceived to be low risk by most managers



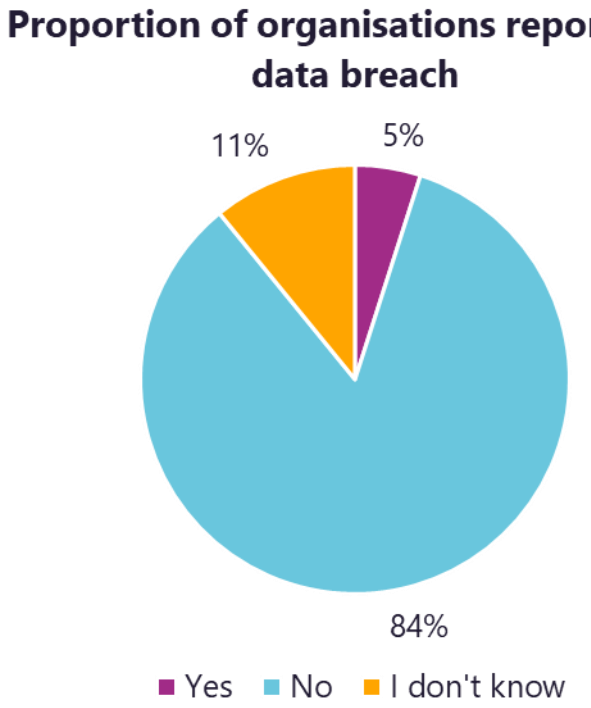
The majority of managers (71%) understood BYOD to pose a low risk to their organisation, whilst only 3% considered it to pose a high-level of risk

Many respondents reported that secure BYOD implementation and data protection were always secondary to other concerns and pressures – particularly cost and maintaining the service

In larger organisations with specific IT teams or data protection officers, the risks of BYOD appeared better understood and weighted. One provider we engaged with was interested in the idea of BYOD but assessed that the risks were too high and they did not at present have sufficient capacity to manage them

Evaluation of risks

The number of data breaches due to BYOD reported was low, a figure which our interviews lead us to question

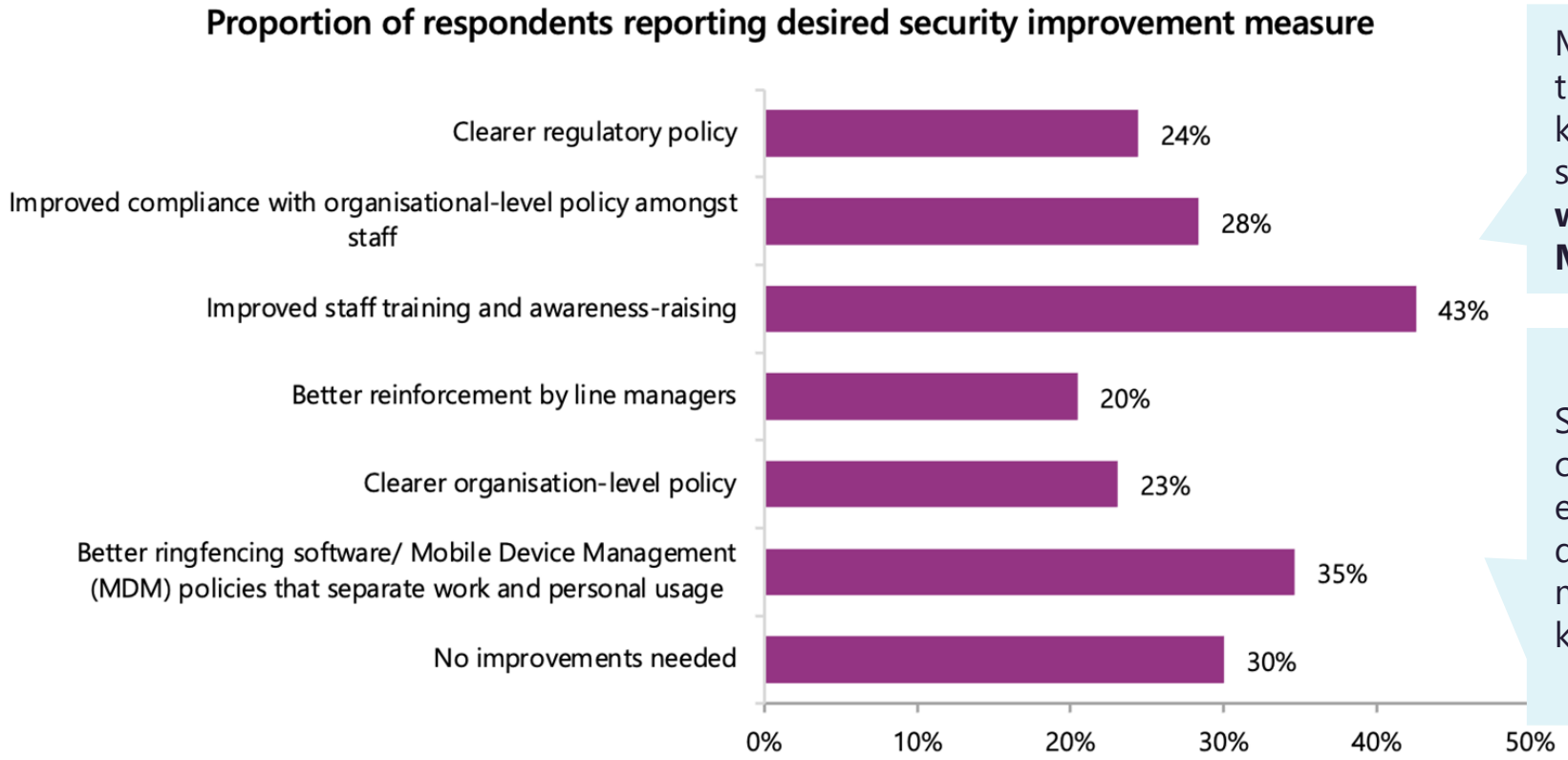


- **5%** of managers reported having experienced a data breach
- **11%** said they did not know
- **84%** said there had not been a data breach

Our interviews with providers and staff did however make us question these numbers. Data breaches were often described in these interviews, however not recognised as such. For example, staff's personal phone numbers were shared by providers with other healthcare professionals or service user family members. While staff did not like this happening, they did not see it as a data breach

Evaluation of risks

Managers looked to regulating staff behaviour as the key means of improving security



Managers identified staff training and awareness as the key means of improving BYOD security; **only 35% reported wanting to use a form of MDM**

Such findings prompt us to consider how providers evaluate the viability of different improvement measures, with cost being a key limiting factor

Evaluation of risks

BYOD risks can be minimised through appropriate technical controls

The National Cyber Security Centre highlights that BYOD **should not carry additional risks beyond using organisation owned devices, provided that the management of these devices are effective.**

This section explores **three technical management approaches** (mobile device management, mobile application management, and high-quality care applications) currently used in ASC, describing what these approaches enable in regards to increasing security.

The section concludes with discussion of other technical approaches identified as options for reducing particular risks.

Although technical controls are widely offered by the market, our research highlighted that only a small portion of the provider market has them in place (as above)

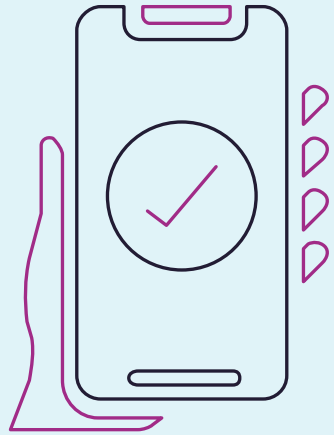
Existing technical controls

Mobile device management provides the highest level of security for organisations

Mobile Device Management (MDM) is a more secure alternative to BYOD. Organisations provide users with devices (typically phones) and then dependent on the capabilities within the organisation either run the device management internally or outsource it to a supplier.

MDM allows organisations to control the applications on the device, prevent downloads of malware, mark devices as lost, wipe all data on the device, and set additional security measures such as requiring long passwords or locking the phone if inactive.

While MDM approaches are more expensive, care providers can rent managed devices complete with data plans for around £7.50 per month. Given some organisations contribute £5 per month to covering data costs, this would go much of the way to also getting a managed device.



Existing technical controls

Mobile application management protects both work and personal data on employee devices

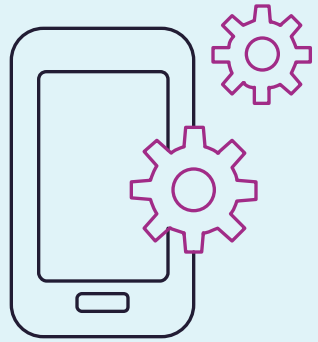
Mobile Application Management (MAM) describes a popular BYOD management approach that allows employers to manage the applications employees use for work on their personal devices.

Typically, MAM approaches create two "containers" within a personal device that are both secure and separate. This means:

- Personal data is inaccessible to employers
- Employers can remotely manage the applications their employees use and the associated data

The advantages of MAM are that employers can push the updates work applications might need, better guarantee the security of the data, and allow employees their privacy.

Many personal devices are now set up to easily facilitate MAM through features such as Android Enterprise or Apple Business Manager.

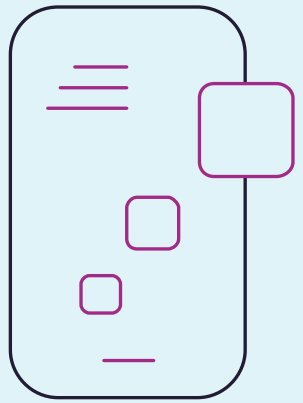


Existing technical controls

In the absence of management software the best care applications provide a number of security controls

The best quality applications will have the following features:

- Biometric login (*quick to use and unique*)
- Offline mode (*removing need for public wifi networks*)
- Remote application logout (*allowing managers to secure data*)
- Unable to upload photos (*forcing photos to be taken through the app*)
- Regular penetration testing (*checking security*)
- Internal messaging function (*stops blended use of WhatsApp and sharing of staff numbers*)
- Rapid logout (*protecting data in case of loss*)
- Data only generated within app (*no service user data stored locally before upload*)
- Data stored remotely (*protecting data in case of loss*)
- Only working on secure wifi networks (*no public wifi access*)

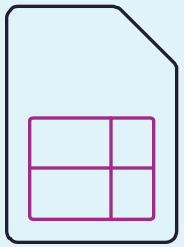


Existing technical controls

Additional technical controls can supplement security

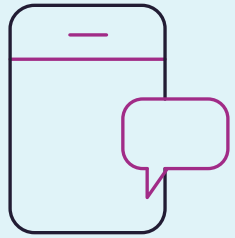
eSIMS:

- From staff, we heard concerns about the costs of covering their mobile data used at work and their personal phone numbers being shared with other staff or healthcare professionals.
- Organisation provided eSIMS would ensure staff always had data (reducing use of insecure wifi networks), they didn't have to bear the cost of this, and their personal phone numbers could be protected.



Secure messaging applications designed for social care:

- Currently, generic platforms such as WhatsApp are used for communication which creates risks from blended personal/ work use, non-employees remaining in group chats, and photos being downloaded onto devices.
- More secure messaging applications are available such as Pando, which separates personal communications from work ones, stores all images within the app, and allows notifications to be muted outside of working hours.



Existing technical controls

7. Detailing the risks

With a clear view of the landscape, we turn to collating and evaluating the risks of BYOD

We will ask the following questions to uncover and understand the risks:

- What are the risks?
- Why do these risks arise?
- How frequently do they occur?
- Who do they affect?
- How do they consolidate to create particular patterns of vulnerability?

From collating all of our primary and secondary data, **we established a comprehensive list of risks that emerge from insecure BYOD usage.**

We were then able to divide these risks in terms of 'why they arise', describing four contexts (detailed on the next slide) which structures this section

With each outlined risk, we reflected on the frequency of occurrence (often, sometimes, rarely) and who they affected

Finally, we considered how many of the identified risks became compounded, with some organisations and settings looking to be particularly vulnerable

Four contexts were identified as the settings through which BYOD risks arise

Through analysing our comprehensive list of risks developed through the compilation of our primary and secondary research; we were able to identify **four key contextual reasons as to why BYOD risks arise**:

- Limited understanding of risks amongst providers & staff
- Minimal knowledge of secure practice amongst providers & staff
- Tight budgets leading to insecure compromises
- Software solutions not facilitating security

These contexts provide a structure for detailing the full list of risks. The following four slides capture the risks we observed, as well as measures of their frequency, and reflections on who they affect

We saw limited understanding of risks amongst providers and staff

Risk	Freq.	Who is affected?
Data breaches not being perceived as such, for example photos of service users being stored on personal devices	Often	Service users
Sometimes, core organisational practices (such as staff communications) were conducted through insecure networks	Sometimes	Service users, staff
In some organisations, efforts were made to protect service user data in BYOD approaches but not staff data, for example staff members' personal phone numbers were given out by management and used for conversations with other healthcare professionals	Often	Staff

"The risks of a data breach because of staff using their own phones is very low"

"It's not like it's interesting data we collect on service users... It's mostly just whether they've eaten or how much water they've had... I guess we do also have the codes to their lock-boxes"

Minimal knowledge of secure practice amongst providers & staff leads to a risky BAU

Risk	Freq.	Who is affected?
Providers not knowing a policy needs to be in place for best practice	Sometimes	Service users, staff
Providers not having the knowledge or resources to develop an effective policy resulting in using boilerplate policies	Often	Service users, staff
Not tailoring staff training to include BYOD specific components	Often	Service users
Providers having insufficient knowledge of what they might need from technical solutions	Often	Service users, staff
Best practice security controls often not considered as necessary	Often	Service users

"It was hard to develop a policy. Most of the big organisations' policies I tried to copy just weren't relevant for us"

"We're told off when we done something wrong, but we're never taught how to do it right"

Tight budgets result in insecure compromises

Risk	Freq.	Who is affected?
Staff are not recompensed for data encouraging use of insecure public wifi networks	Often	Service users, staff
Providers purchase cheaper applications without built-in security features (e.g. only taking photos in the app)	Often	Service users
Reliance on free generic communications apps e.g. whatsapp/ telegram for managing internal comms	Sometimes	Service users, staff
Additional security features such as MAM/ VPNs / MFA are not invested in	Often	Service users, staff
Tight budgets can also bring about BYOD by default e.g. where procured devices do not have data plans	Sometimes	Service users

"We chose this app because it's what I used before. I'm not sure if it's the best but it's cheap"

"Why would I pay for a separate app when WhatsApp is encrypted?"

"There's no point taking a device without data out - I need to be online!"

Software solutions often do not facilitate security

Risk	Freq.	Who is affected?
Not requiring strong passwords, MFA or biometric login	Sometimes	Service users, providers
Not having good offline functionality, preventing staff from working normally outside of mobile data coverage and encouraging connection to public wifi	Sometimes	Service users, staff, providers
Staying logged in for extended periods (thus increasing risk of data breach if phone is stolen)	Sometimes	Service users, providers
Prioritising developing new features rather than security updates	Often	Service users, staff, providers
Encouraging the use of external communications apps through not providing in-app functionality	Often	Service users, staff

"I use the same pin code to log into the app as I do for my phone"

"My manager will message me if I haven't submitted my notes, but I can't do that unless I can connect to the internet"

The risks in adult social care tend to cluster together

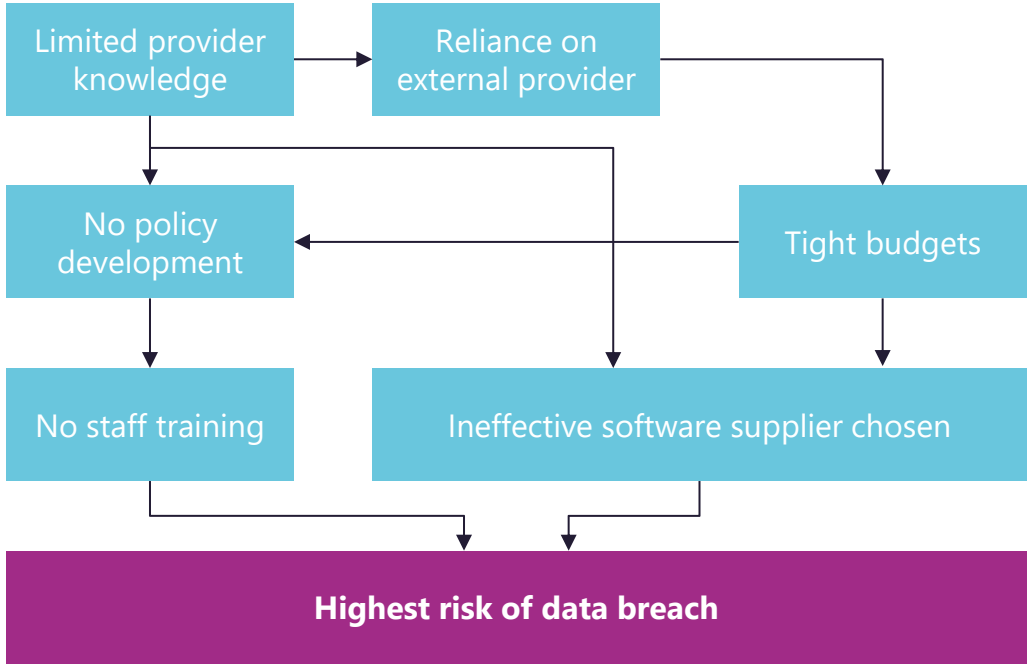
Many of the clusters of risk in the Adult Social Care landscape overlap to become consolidated, for instance:

Limited provider knowledge may lead directly to the lack of a policy being developed, or as mediated through reliance on external providers and budgetary constraints

Without a policy, staff may not receive specific training, and with tight budgets, they also might be using insecure software

All these factors result in a higher risk of a data breach for some organisations. We found the risks were most clustered amongst small providers with limited financial resource, digital development, and technical knowledge

Our research has however highlighted a high degree of diversity in BYOD security across the sector; with some providers well protected and others highly vulnerable



At present, service users and staff bear the day-to-day risks of insecure BYOD practices

Our analysis of risks highlights that in many cases, service users and staff face the greatest risks from insecure BYOD practices. **It is the data of these individuals that is frequently breached; with at present, little means of redress**

For service users particularly, the data collected about them is highly sensitive and the lack of protection around it sees new risks introduced for an already vulnerable group

From considering how risks consolidate in certain organisations where knowledge of both risks and secure practice is low, budgets impact the security of solutions, and effective technical controls are not in place, there are particular vulnerabilities

Into the future, we anticipate that if data protection and BYOD security become greater components of regulation in Adult Social Care, providers will start to see more implications of risky practices.

Negative CQC reviews, fines, and reputational damage could start to affect providers.

8. Outlining improvement measures



The PSC

8.1. The ASC context: Scope for solutions

A number of challenges need to be overcome to enact large scale change in ASC

Regulatory challenges

- Currently, limited potential for regulatory action
- The CQC is the main enforcer within social care and BYOD is not yet a specific part of their assessment
- The ICO tend to avoid handing out fines to organisations that cannot afford them - as of yet no ASC providers have been fined despite 200+ recorded data breaches
- While guidance exists around how to run BYOD securely, there's little specific policy or law that requires compliance

Market-based challenges

- Care providers operate under very tight budgets, with an increase in spending on more secure technologies not viable for all
- Recent increases in required NI contributions look to tighten budgets further
- Care providers are also specialists in care, rather than in cyber security or digital, resulting in dependence on more expensive external providers

As a result of these challenges, our suggested improvement measures focus on educating and encouraging providers and staff towards good practice; with more expensive measures or those needing regulatory enforcement noted, but marked for the future

8.2. Prioritised improvement measures

We've grouped our improvement measures around four key themes

Improvement measure groupings
1. Increased awareness of risk
2. Enabling secure practice
3. Incentivising secure behaviour
4. Regulating non-compliance

We've divided our long-list of improvement measures into four different thematic buckets

The first two groupings map to the risks outlined in the previous section and are designed to increase awareness of risks and better offer providers the resources they need to mitigate the risks

The second two groupings reflect more on the mechanisms to bring about change, both through positive reinforcement of secure behaviour and through creating consequences of non-compliance

We've also tested our solutions with providers and technical experts

Our providers told us:

- Policy guidance would be very helpful but we need this in layman's terms so it's interpretable to everyone who might need to read it
- An outline of everything that needs to be considered as part of BYOD would make policy writing easier
- A bronze/ silver/ gold roadmap would allow us to know what we need to be doing as a minimum and to plan how we invest our resources into the future
- Adept providers told us they had their own screening criteria for suppliers, but think less digitally developed organisations could benefit from this

The technical experts we engaged with told us:

- Policies need to outline precisely what an employer can and cannot access on employee devices
- MDM solutions are not expensive, can be managed externally for providers without an IT team, and dramatically increase BYOD security
- Providers are looking for new features rather than security updates; improvement measures need to address this view
- In an ideal scenario, having good BYOD security would be a requirement of receiving LA commissioned work

Our top 4 improvement measures for now

Measure group	Methods	Effort	Impact
BYOD education piece	"Have you thought about this risk as part of BYOD" guide cataloguing risks across all elements of BYOD usage	Low	High
Custom policy-building tool	BYOD guidance product including a specific policy development tool that can be tailored to your organisation + developed for care setting e.g. domiciliary versus care home. A sensible next step may be a prototype or "alpha" stage to prove the logic and demand.	Low	High
Recommended tech solutions tool	A "what technical solutions does my organisation need?" interactive tool, plus advice on the security features they might want for each of their technical solutions e.g. biometric login, good offline mode, not connecting to insecure wifi networks etc. Again, this would be tractable for prototyping.	Low	High
Risk awareness comms	Educational piece illustrating bad practice and highlighting consequences of reputational damage and financial losses during recovery	Low	Med

Of our long-list of improvement measures, we evaluate these to be the priorities for the short-term due to their relatively low effort and higher impact, a full list of measures is in the appendix

In order to take forward our top-4 improvement measures, we propose the following next steps:

1

Agree on how many top improvements you can practically take forward

We believe that those top 4 improvements should be worked on in parallel to target providers at different points of their secure BYOD journey, but your resource/budget will determine the final improvement ideas to take forward

2

Mobilise internal or external resources to deliver chosen solutions

Once you've decided on the measures to take forward, teams with expertise need to be mobilised/ commissioned to ensure smooth implementation. Working with your local support networks as needed

3

Digital Care Hub to regularly revisit the long list of improvement ideas

We recommend that the Digital Care Hub revisits the long list of improvement ideas as policy and provider market change, which may warrant some ideas to be taken forward

9. Conclusion

Current BYOD practices pose significant threats to the ability of organisation to deliver secure care

Current state:

- Our research - the most extensive conducted into BYOD usage in ASC - allows us to draw a series of conclusions about the current state
- We find that BYOD approaches are popular in the ASC sector:
  - They are drawn upon by half of care providers surveyed
  - BYOD is particularly popular amongst small organisations and within domiciliary care settings
- We found the key driver of BYOD adoption to be cost, aligning with its popularity in small and domiciliary care organisations where budgets are tighter
- We present data illustrative of insecure practices, including only around half of BYOD organisations following policies, and few organisations making use of technical controls to ensure security
  - Questions put to staff both in interviews and the survey highlight how insecure practices often operate as standard, for example through:
    - The use of large WhatsApp chats for communicating service user information
    - Connecting to public wifi networks in order to complete care notes
- While many managers perceived BYOD to be “low risk” and few reported data breaches in the survey, interviews made it apparent that data breaches are not always understood as such, leading us to reflect that perceptions of risk and the numbers reported do not reflect actual conditions

The ‘insecure as usual’ practices within many care organisations create significant risks

Risks:

- Through analysing the data, we find risks associated with BYOD can be understood to arise from four main areas:
  - Limited understanding of risk
  - Limited knowledge of best/ secure practices
  - Cost leading to insecure compromises, and
  - Software solutions not facilitating security.
- Risks also coalesce, with some providers affected across all four areas. Anecdotally, these risks seem to consolidate in small providers, where budgets are tightest and the lack of a specific IT team or data protection lead results in limited knowledge both of risks and secure practices
- Both service user and staff data is vulnerable as a result of these risks. Into the future, we imagine providers will also begin to experience consequences of data breaches if the CQC’s remit on enforcing data protection compliance increases

Improvement measures need to begin with increasing education and awareness

Improvement measures:

- Due to regulatory and market-based limitations, BYOD security improvement measures need to be targeted around education and increasing awareness
- Through prioritising improvement measures by effort involved and magnitude of impact, we propose 4 ‘measures for now’ which we anticipate will assist providers in improving their BYOD practices. These improvement measures aim to:
  - Increase provider awareness of risks associated with different components of BYOD
  - Empower providers to develop tailored policies through a new tool
  - Assist providers in choosing technical solutions and appropriate security measures
  - Develop awareness of risks and consequences through writing an educational piece to be shared on social media
- In addition to these four prioritised improvement measures, a full list of suggested options is detailed in the report appendix

Appendix

Full list of research methods

Our desk-based research highlighted existing gaps in the knowledge base of BYOD usage

The following sources have been invaluable in informing our initial understanding, however we struggled to find up-to-date and specific information on BYOD usage in social care:

- NHSX Technology and Digital Skills Review 2021 developed by IPSOS MORI, The Institute of Public Care, and Skills for Care
- Adult Social Care Cata and Cyber Security Programme Report 2019-20 developed by the Institute of Public Care
- The currently unpublished Adult Social Care Cyber Security Report 2024 developed again by the IPC
- 2023-24 Workforce Data from Skills for Care
- Research into specific BYOD technologies and security practices in an Australian healthcare context by Ahmad Wani et. al. (2022)

As we turned to look at best practices to inform our improvement measures, we've drawn on information from:

- National Cyber Security Centre's 2021 BYOD guidance
- BYOD security guidance from the ICO

775 individuals working in social care responded to our survey

We circulated a survey designed for both managers who can comment on BYOD usage in their organisation as a whole and staff who can comment on their own experiences

775
Individuals completed the survey in total

606
Managers

169
Staff

303
With BYOD

303
Without BYOD

79
With BYOD

90
Without BYOD

Workshops and 1-1s added detail to our growing understanding of practices and risks

First, we hosted a manager workshop - attended by **7 senior staff** from different care providers - then supplemented our learnings from this exercise with an additional **7 manager 1-1s**

Next, we facilitated 1-1s with **11 staff members** who worked across a variety of care settings but who all used personal devices in their work

From managers we wanted to learn:

1. How policies were arrived at (tasks, devices, operating systems)
2. Perceived risks
3. Security controls and decisions around these
4. Who does the security management?
5. How are policies enforced?
6. Managing employee privacy

From staff we wanted to learn

1. Sentiment surrounding personal phone use
2. Choice in using personal device and preferences
3. Who covers the costs?
4. How staff follow the company BYOD policies/ guidelines
5. Perceived risks associated with personal device usage

Expert interviews guided us towards improvement measures which we then tested with providers

We conducted **7 interviews with experts** across policy and technical remits who helped us develop, iterate, and validate our long-list of prioritised improvement measures.

We then tested these improvement measures with **2 providers** to evaluate the viability of measures proposed.

In our expert interviews we covered:

1. Tailoring effective BYOD policy
2. The minimum acceptable standard for BYOD through to examples of best practice
3. Specific software solutions for BYOD best-practice at a range of price points
4. The features care applications need to be secure
5. More secure alternative to BYOD in the form of managed devices

In our provider testing sessions, we asked:

1. Do these proposed improvement measures align with your needs?
2. Do they seem viable?
3. Where might some of the challenges come with implementation?
4. What is the appetite for change and how might this be increased?

Policy solutions

What does a good BYOD policy look like?

- **Live:** Rather than as part of a contract signed once, the BYOD policy is a live document that is updated regularly and staff have the ability for staff to engage with it
- **Specific:** It reflects the unique organisational context rather than being a boilerplate policy
- **Considered:** It correctly accounts for the whole variety of different BYOD use cases and comprehensively covers secure practices across each
- **Feasible:** Staff can reasonably enact the contents of the policy and it can be effectively practically applied
- **Has clear ownership:** Ownership of the policy is held by the care provider who utilises it to ensure safe practice
- **Defines responsibility:** Obligations of suppliers, managers, and staff are clearly identified

Full list of improvement measures

Increasing provider awareness of risks

Improvement measure	Methods	Effort	Impact
Raising awareness of risks associated with BYOD	Writing an educational piece illustrating bad practice and highlighting the consequences of reputational damage and financial losses during recovery	Low	Med
	Developing a "Have you thought about this risk as part of BYOD" guide cataloguing risks across all elements of BYOD usage	Low	High
Increasing provider knowledge of risks	Annual provider training	Med	High
	Provider guide book (with options for different orgs / stages of development)	Low	Med
	BYOD/ BYOD policy mentioned explicitly in CQC guidance	High	High
	Fun challenges to test BYOD security knowledge	Low	Med
Increasing staff awareness of risks	Staff BYOD security modules as part of mandatory training	Med	High
	Providers sharing pre-developed reminder resources to remind staff of risks	Med	Med

Enabling secure practice (1/2)

Improvement measure	Methods	Effort	Impact
Empowering providers	BYOD guidance product including a specific policy development tool that can be tailored to your organisation + developed for care setting e.g. domiciliary versus care home	Low	High
	Bronze / Silver / Gold BYOD policy + practice examples	Low	Med
	Targeted support for organisations highlighted to be facing the biggest BYOD security risks	Med	High
	Local team support or provider hotline / helpdesk for BYOD inquiries	Med	High
	Software supplier assessment criteria to help choose secure suppliers	High	High
Making BYOD security affordable	Grants / subsidised MDM packages or tax breaks for suppliers	High	High
	Salary sacrifice schemes for supplied managed devices	High	Med
	Develop a Social Care contract with Microsoft and Google similar to those in the Education sector	High	High
	Encouraging providers to make use of pre-existing technical controls they may have access too such as Android Enterprise through Google Suite	Med	Med

Enabling secure practice (2/2)

Improvement measure	Methods	Effort	Impact
Using the right technical solutions	eSims to protect staff phone numbers + provide staff with data plans	Med	Med
	A "what technical solutions does my organisation need?" interactive tool	Low	High
	An interactive guide which prompts providers on the security features they might want for each of their technical solutions e.g. biometric login, good offline mode, not connecting to insecure wifi networks etc.	Low	High
	Recommended software supplier list	High	High
	Pursuing containerisation options such as Android Enterprise to separate personal and work usage	High	High
Facilitating staff to use personal devices securely	Options to access secure wifi networks	High	Low
	Applications having offline modes so they can be used outside of service range	Med	Med
	Auditing process to ensure service user / staff data is not on devices but staff privacy is still respected	Med	Med

Incentivising secure behaviour

Improvement measure	Methods	Effort	Impact
Highlighting best practice	Success stories shared and naming and celebrating good practice	Low	Med
	Awards and badges for good BYOD security approaches	High	Med
Rewarding good practice	BYOD security assurance as a necessity for LA or NHS commissioned contracts	High	High
	Trusted provider' kitemark for organisations with high levels of security that then improves procurement options	High	Med

Regulating non-compliance

Improvement measure	Methods	Effort	Impact
Consequences for non-compliance	CQC to investigate / regulate BYOD usage and share examples of where it's gone wrong	High	High
	Fines for non-compliance	High	High
	Consequences for managers of care organisations	High	High

For both "incentivising good practice" and "regulating bad practice" the effort involved enacting the improvement measures is typically high. This is due both to the number of different organisations who would be responsible and the new architectures needed to implement the measures

While the impact of these measures would likely be high, in the short term, efforts to improve the security of BYOD would be better focused around raising awareness both of the risks and what good practice looks like

Checking our improvement measures match our risks (1/3)

Risk group	Risk	Addressed?	Priority?
Limited knowledge of risks	Data breaches not being perceived as such	Y – risk education piece	Y
	Sometimes, core organisational practices conducted through insecure networks	Y – risk education piece	Y
	Staff data breaches not viewed the same as service user data breaches	Y – risk education piece	Y
Minimal knowledge of secure practice	Providers not knowing a policy needs to be in place for best practice	Y – policy builder tool	Y
	Providers not having the knowledge or resources to develop an effective policy resulting in using boilerplate policies	Y – policy builder tool	Y
	Not tailoring staff training to include BYOD specific components	Y – staff training modules	N
	Providers having insufficient knowledge of what they might need from technical solutions	Y – interactive tech + security solutions tool	Y
	Best practice security controls often not considered as necessary	Y – interactive tech + security solutions tool	Y

Checking our improvement measures match our risks (2/3)

Risk group	Risk	Addressed?	Priority?
Tight budgets leading to insecure compromises	Staff are not recompensed for data encouraging use of insecure public wifi networks	Y - making BYOD security affordable	N
	Providers purchase cheaper applications without built-in security features (e.g. only taking photos in the app)	Y - making BYOD security affordable and software solutions tool highlighting appropriate measures	N
	Reliance on free generic communications apps e.g. whatsapp/ telegram for managing internal comms	Y - making BYOD security affordable and software solutions tool highlighting appropriate measures	N
	Additional security features such as MAM/ VPNs / MFA are not invested in	Y - making BYOD security affordable and software solutions tool highlighting appropriate measures	N
	Tight budgets can also bring about BYOD by default e.g. where procured devices do not have data plans	Y - making BYOD security affordable	N

Checking our improvement measures match our risks (3/3)

Risk group	Risk	Addressed?	Priority?
Software solutions often not facilitating security	Not requiring strong passwords, MFA or biometric login	Y - software and security tool highlighting necessary security	N
	Not having good offline functionality, preventing staff from working normally outside of mobile data coverage and encouraging connection to public wifi	Y - software and security tool highlighting necessary security	N
	Staying logged in for extended periods (thus increasing risk of data breach if phone is stolen)	Y - software and security tool highlighting necessary security	N
	Prioritising developing new features rather than security updates	Y - software and security tool highlighting necessary security	N
	Encouraging the use of external communications apps through not providing in-app functionality	Y - software and security tool highlighting necessary security	N

DSPT
Better Security.
Better Care.

Digital
Care Hub

The PSC

digitalcarehub.co.uk