Digital Maturity in the Social Care Sector – Quantitative Research

Digital Social Care and Skills for Care

February 2021

Contents

Digital Social Care & Skills for Care

Published by Digital Social Care

2021

This work was researched and compiled by QA Research. This research has been carried out in compliance with the International standard ISO 20252, (the International Standard for Market and Social research), The Market Research Society's Code of Conduct and UK Data Protection law

1. Executive Summary

This research forms part of the Digital Readiness Research undertaken as part of the Digital Social Care contract.

1.1 Aims and objectives

- Explore the current appetite for digital within the social care sector
- Understand the varying degrees of digital maturity amongst social care providers and to delve into how digital is being used at present
- Investigate the impact technology has had across the social care sector to date
- Identify the ways in which COVID-19 has impacted social care providers in their use of digital technology
- Uncover any support needed by the sector in further embedding digital technology

1.2 Methodology

- Wave 2 of telephone survey (Wave 1 conducted October 2019)
- 418 telephone (CATI) surveys with social care organisations in England
- Survey developed in context of COVID-19 pandemic and a series of depth interviews undertaken by Qa in November 2020
- Fieldwork ran from 20th January to 13th February 2021
- Analysis conducted in-house at Qa Research, data was weighted in order to represent the social care sector using ASC-WDS data provided by Skills for Care
- Q1 and Q2 of 2019 survey were also weighted in order to compare responses
- Sub-group analysis by organisation type (residential/non-residential), size and location – differences only highlighted where there is a significant difference

1.3 Findings

Current use of digital

Digital readiness improving as number of ‘expert’ organisations increased over past year

- Positive movement over time, a fifth (20%) of care organisations now consider themselves digitally ‘expert’
- Organisations classing themselves as ‘novice’ dropped from a quarter (24%) in 2019 to only 14% in 2021
- No significant differences based on region, organisation size, or residential vs non-residential, so no one type of care organisation is leading the way or falling behind in terms of digital readiness
- This shows improvement from 2019 where residential and ‘micro’/’small’ organisations were more likely to be ‘novices’

Almost all have access to basic technologies, but only a fifth have 5G access

- Almost all care organisations continue to have access to basic digital technologies (internet access, hardware e.g. computers, software e.g MS Office), but 1-2% of organisations still do not have access to these
- Access to 5G introduced in 2021 survey, a fifth now have access
- 5G access regionally varied as expected, with most common 5G use in: Eastern England (34%), North West (25%), Yorkshire & Humber (25%)

COVID-19 means video meeting platforms have become ubiquitous and essential

- Small increases in the uptake of most digital systems during COVID, with a seismic shift in use of video meeting platforms (+65%)
- Indeed, nearly half (46%) 'couldn't live without' video meeting platforms
- Notable increases in: Online training (+14%) and Secure email (+12%)
- 'Medium' and 'large' organisations more likely than 'small' and 'micro' organisations to have access to the range of digital systems, with the exception of video platforms and online training which were used across the board
- Online training and secure email more likely used by residential, whilst social media, digital care planning software and digital medication management more likely used by non-residential

Data Security and Protection Toolkit (DSPT) not widely known or undertaken

- Awareness of the DSPT relatively low, half had not heard of it (52%)[1]
- Only a small proportion (16%) were working towards or achieved a level of DSPT
- In terms of support for the DSPT:
    - 22% accessed IPC webinars on the DSPT
    - 19% had accessed DSPT guidance on the DSC website
    - 19% had accessed an 'other' form of support, e.g. Local Council, CQC, NHS CCG, external IT company, Government website

Cyber security and data protection

IT security generally 'up to date' but device-specific security measures varied

- Vast majority of social care organisations described their IT security as 'up to date' (over 90%) for firewalls, antivirus and operating system & the majority (85%) of care providers have a named person responsible for data protection or a 'Data Protection Champion' or someone with named responsibility for data protection

[1] The research only spoke to one contact in the organisation and it may be the case that someone else in the organisation was aware of the DSPT

- However, the security measures in place for company devices and 'bring your own devices' were varied, both for laptops/tablets and smartphones
- Most had basic security measures like passwords/PINs, but far fewer took steps such as encryption and authentication

<u>Most covered by data protection and data breach policy, but BYOD policies less common</u>

- Most social care organisations are covered by a data security or protection policy (85%) as well as data breach and records management. However, 15-19% of organisations are not covered by these policies
- Fewest social care providers have a 'BYOD' policy:
    - 49% of organisations have employees BYOD to some extent (Q3 in survey) but only 29% of all organisations have a BYOD policy
    - Therefore there is a gap in policy for some organisations who encourage BYOD
    - 14% only started BYOD since COVID-19 (Q3) which could explain delay in policy
    - Non-residential more likely to BYOD therefore there may be work to do among non-residential organisations to encourage BYOD policy

<u>Over half of care organisations have not tested their restore process</u>

- Around half (48%) of social care providers backed up their data daily
- Large organisations were more likely to back up daily while smaller ones had more varied backup frequency
- For organisations who backed up data, 53% backed up on a 'cloud-based server' and 24% used an external hard drive to back up
- Over half (55%) of organisations had never tested the restore process

<u>1 in 10 social care providers experienced a cyber attack or data protection breach</u>

- 90% of organisations had not experienced any of these, but 8% had experienced a cyber attack and 4% a data breach
- Non-residential care organisations more likely to come into contact with a 'data protection breach' (5% vs 1% of residential)
- Micro sized care providers were significantly more likely than small sized organisations to experience a 'cyber attack' (9% vs 3%)

Current and future support

<u>Most would prefer cyber security & data protection support to be available on demand</u>

- Social care organisations preferred cyber security/data protection support to be accessible any time

- Written info (64%), pre-recorded webinars (62%) and online learning (60%) were clear favourites
- No requests for social media learning but some noted busy schedules – possibility for bitesize learning?
- Three-quarters (78%) felt that 'greater awareness of offers' would make them use more support
- Vast majority (90%) said 'email offers' were the best way to communicate, but 'RM networks' and 'membership bodies' also useful

1.4 Conclusions

Positive development in digital maturity since October 2019, which now does not vary by size of organisation. This shows improvement in the residential care sector as well as 'micro' and 'small' organisations, who in 2019 were more likely to be digital 'novices'.

Mix of company devices and 'bring your own device', with the COVID-19 pandemic instigating BYOD in some organisations. This could help explain why the number of social care providers who have a BYOD policy is less than the number who use BYOD.

COVID-19 has driven small increases in the uptake of most digital software or systems available to social care providers, but there has been a seismic shift in the use of video meeting platforms, with online training and secure email also popular.

Half of organisations had not heard of the DSPT, which suggests there is significant awareness raising to do if the goal is to expand uptake. Better Security, Better Care has been established to address this issue.

Vast majority of care organisations described their IT security as 'up to date' and had a named person responsible for data protection or a 'Data Protection Champion'. However, the security measures in place for company devices and 'bring your own devices' were varied and often single-factor.

Care organisations appeared to prefer cyber security and data protection support to be available on demand, at a time that suited them, e.g. written information, pre-recorded webinars or online learning, to match their unpredictable schedules.

Overall, 'medium' and 'large' organisations generally more likely to have policies in place for various aspects of digital such as data protection, cyber security. Also more likely to back up data daily, and have access to the full range of digital systems.

However, this is not to say that 'small' and 'micro' organisations are falling behind, as there is no reduction in their digital maturity rating.

Residential and non-residential organisations are consistent in digital maturity, but use of digital sometimes manifested differently, e.g. non-residential more likely to 'bring your own device' or use digital care planning and medication systems, while residential more likely to use secure email and online training. Non-residential also more likely to have experienced a data protection breach, an interesting finding to monitor going forward.

2. Introduction

This research was undertaken by Qa Research on behalf of Skills for Care and Digital Social Care as part of an ongoing package of work to understand digital maturity within the social care sector. This phase of quantitative research consisted of 418 telephone surveys and was undertaken as a follow up wave to an initial wave of surveys completed in 2019.

Due to the COVID-19 pandemic, it was decided that this second wave survey would not replicate the 2019 survey and instead reflect the changing context of the pandemic. A wave of qualitative depth interviews were conducted in November 2020 to inform this survey, particularly with a view to reflecting COVID-specific changes. As such, only two questions are compared between the two waves.

3. Aims and objectives

The aims of the current research were to:

- Explore the current appetite for digital within the social care sector;
- Understand the varying degrees of digital maturity amongst social care providers and to delve into how digital is being used at present;
- Investigate the impact technology has had across the social care sector to date;
- Identify the ways in which COVID-19 has impacted social care providers in their use of digital technology; and
- Uncover any support needed by the sector in further embedding digital technology.

4. Methodology

4.1 Method

This research consisted of 418 surveys with care organisations in England, administered by Computer Aided Telephone Interviewing (CATI) using Qa Research's in-house (remote working) contact centre. Fieldwork ran from 20th January to 13th February 2021.

The questionnaire for this research was designed by adapting the wave 1 questionnaire (from October 2019), and considering the COVID-19 pandemic context and findings from a programme of qualitative depth interviews conducted by Qa Research in November 2020. Note it was not possible to ask detailed questions on all topics. For example, the questionnaire covers WiFi access, but not quality of connectivity, as there was limited space in the questionnaire.

Analysis was conducted in-house at Qa Research, where the data was weighted by organisation type (residential vs non-residential), size (Micro, Small, Medium, Large), and region in order to represent the social care sector breakdown, using ASC-WDS data provided by Skills for Care. Similarly, Q1 and Q2 of the 2019 survey was also weighted to represent the same population, therefore the two survey waves can be compared.

Where there are significant differences between type, size or region, these are noted in the analysis.

4.2 Sample

The below table illustrates the achieved sample. The sample was constructed using stratified random sampling techniques, and interlocking quota targets were imposed on the CATI system to ensure the sample was as representative of the social care sector as possible. However, there will be an element of self-selection based on willingness to engage with the research and therefore some quotas were not completely met. In order to ensure representation, the sample was weighted to reflect sector make up, therefore the impact of the sample make up on survey responses was limited as far as possible. The table below sets out the unweighted sample and weighted sample. It is broken down by the three factors that the sample was weighted by; organisation size, type, and region.

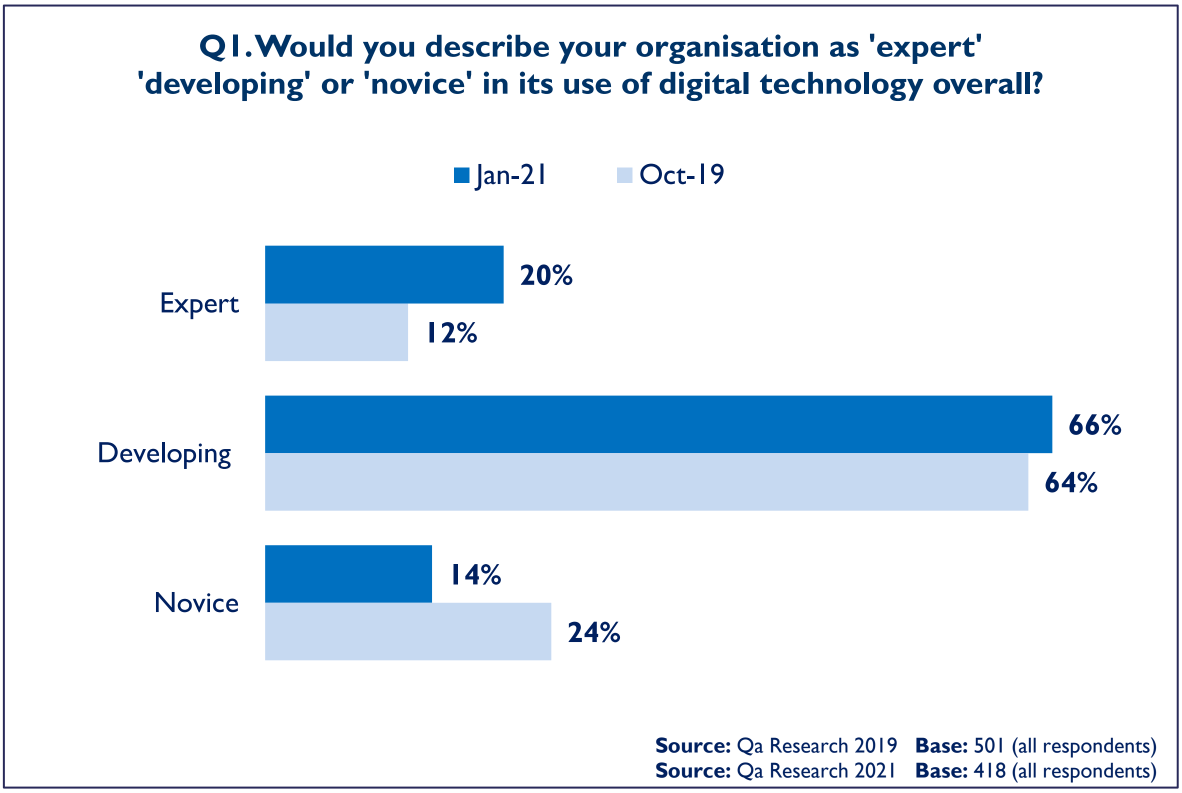
For a full discussion of sampling see Appendix 7.1.

Sample Breakdown	Unweighted sample		Weighted sample	
	Count	Percentage	Count	Percentage
Organisation type				
Residential	150	36%	179	43%
Non-residential	268	64%	239	57%
Organisation size				
Micro (1-9 employees)	178	43%	217	52%
Small (10-49 employees)	160	38%	138	33%
Medium (50-249 employees)	73	17%	54	13%
Large (250+ employees)	7	2%	10	2%
Region				
East Midlands	37	9%	35	8%
Eastern	29	7%	44	10%
London	53	13%	77	18%
North East	31	7%	15	4%
North West	47	11%	48	11%
South East	67	16%	71	17%
South West	47	11%	49	12%
West Midlands	52	12%	43	10%
Yorkshire & Humberside	55	13%	36	9%
Total	**418**	**100%**	**418**	**100%**

5. Key findings

5.1 Current use of digital technology

In this programme of work, a key metric of the social care sector's use of digital technology is whether organisations describe themselves as 'expert', 'developing' or 'novice' in their use of digital. Survey respondents were asked this question in the October 2019 survey, and again in January 2021. The below chart compares results from the two waves.



Source: Qa Research 2019 **Base:** 501 (all respondents)
Source: Qa Research 2021 **Base:** 418 (all respondents)

The above chart illustrates that there has been some positive movement, notably a fifth (20%) of care organisations now consider themselves 'expert' in their use of digital technology, up from 12% in 2019. In line with this, the amount of organisations classing themselves as 'novice' has dropped from a quarter (24%) in 2019 to only 14% in 2021.

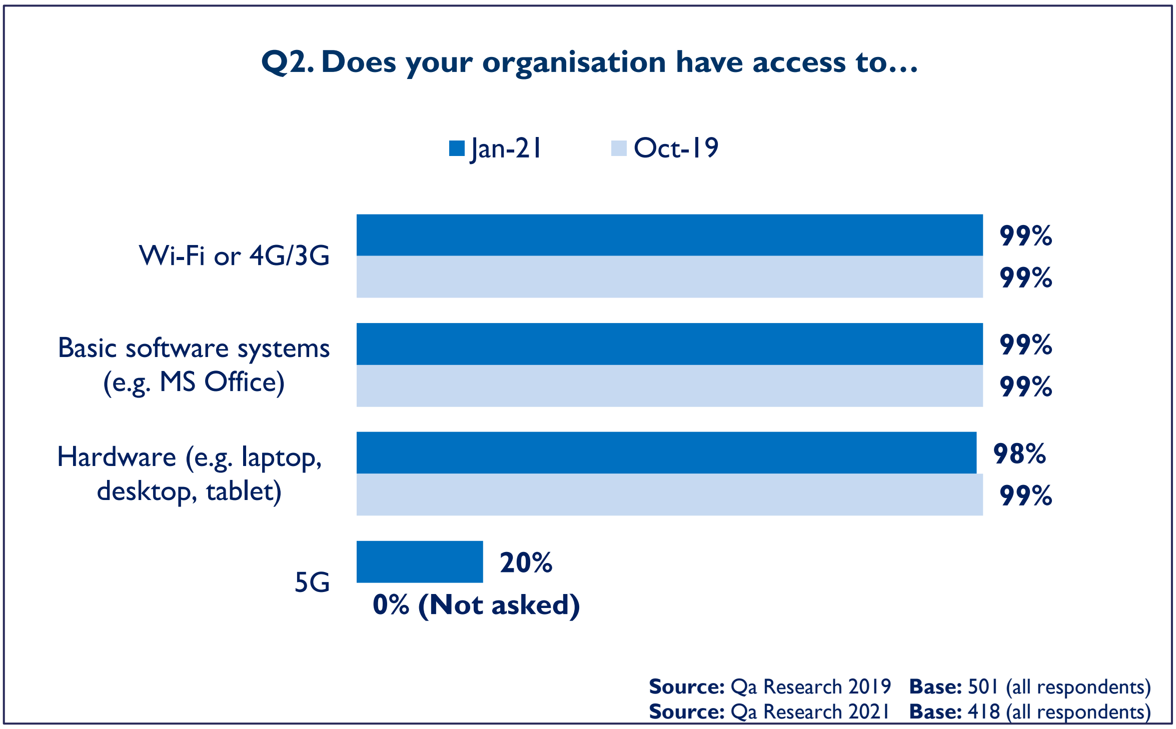
The proportion of respondents who are 'developing' digitally remains consistent as the majority category, at around two-thirds (66% in 2021, 64% in 2019), suggesting there is still room for progression in digital maturity.

Breaking this down by sub-group, there were no significant differences based on region, organisation size, or residential vs non-residential in 2021. This suggests that no one type of care organisation is leading the way or falling behind in terms of digital readiness.

This shows particular progress for the residential care sector who were significantly more likely to be 'novices' in 2019 (34% vs 20% non-res). Small and micro organisations were also more likely to be 'novices' in 2019, suggesting the smaller care organisations have developed in the past year.

In 2021, 'medium' sized organisations were most likely to define themselves at 'expert' level (29%), while 'small' organisations were least likely at 16%; however these differences are not statistically significant, merely indicative.

Respondents of the 2019 and 2021 surveys were also asked whether they had access to a number of basic digital technologies. In 2021 the list was updated to include access to 5G network. The results are shown below.



Source: Qa Research 2019 **Base:** 501 (all respondents)
Source: Qa Research 2021 **Base:** 418 (all respondents)

The above chart shows that there is relatively little change between the survey waves in terms of access to 'Wi-Fi or 4G/3G', 'basic software systems' and 'hardware', largely because these were already present in almost all organisations in 2019. While access was indicated, this survey did not probe further into reliability of the connection or quality of software/hardware systems.

In 2021 there remained a very small minority (1-2%) of care organisations that do not have access to these basic digital technologies.

Since its phased introduction in May 2019, a fifth (20%) of care organisations now have access to 5G. Unsurprisingly, given that 5G is not yet available country-wide, certain regions were more likely to have access. Eastern England (34%), North West (25%) and Yorkshire & Humber (25%) were most commonly using 5G.

Non-residential organisations were significantly more likely to have 5G access than residential (24% vs 16%). Also, 'expert' (32%) and 'developing' (20%) rated organisations were significantly more likely to have 5G access than 'novice' (6%) rated social care providers. There were no differences based on size of organisation.

The remaining questions only cover the 2021 survey questions, due to changes in the survey between waves.

Respondents were asked whether their organisation provided company devices, if staff were required to use their own devices, or a mix of the two. Results are shown in the below table.

Q3. Does your organisation...?		
	Count	**Percentage**
Provide company devices only	212	51%
Mix of company devices and staff using own devices for work (pre COVID-19)	123	29%
Mix of company devices and staff using their own devices for work (since COVID-19)	57	14%
Require staff to use their own devices for work purposes	20	5%
Base 418 (all respondents)		

The table shows the most popular option was for care organisations to 'provide company devices only', with just over half operating in this way (51%).

Overall, 43% used a mix of company devices and staff personal devices, however only 29% were doing this before Covid-19, while 14% brought this is due to the pandemic. A minority (5%) only used staff's own devices.

Breaking this down by subgroup, residential care organisations were significantly more likely to 'provide company devices only' compared to non-residential (60% vs 44%).

Conversely, non-residential providers were significantly more likely to have had a mix of company and staff devices as an ongoing policy before Covid-19 (36% vs 20% of residential). This suggests that using a mix of company and personal devices is a more 'business as usual' approach for non-residential care organisations.

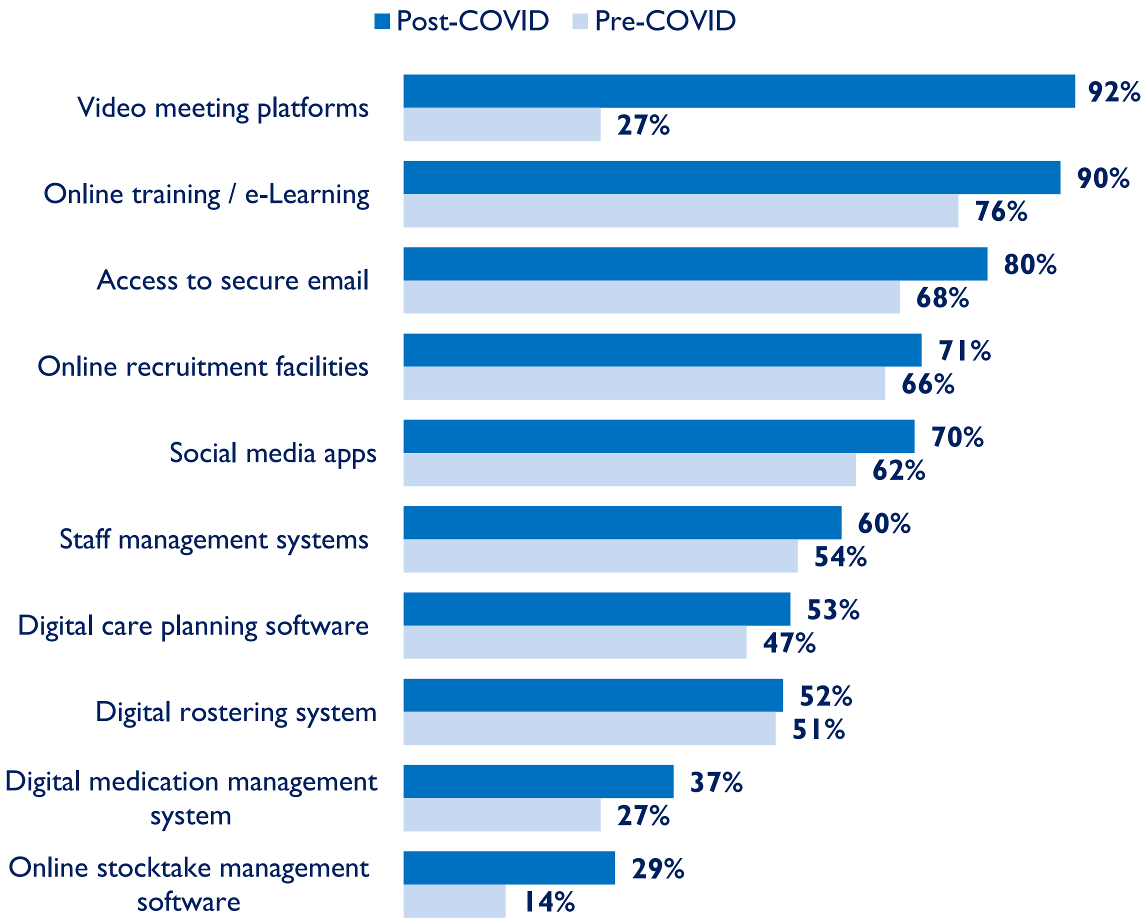
By region, London-based organisations were significantly more likely to 'provide company devices only', at 66% compared to smaller proportions in the East of England (30%), South East (45%) and West Midlands (46%).

Care organisations were asked to identify whether they used a range of digital software packages and systems and how well these were used, both before COVID-19 and now.

Respondents could answer: ‘We didn’t have any’, ‘We had some but we didn’t use them well’, ‘We had some in place and it was OK’ or ‘We couldn’t live without them’.

This question was designed to show how prevalent the use of different systems are in the social care sector, and whether the COVID-19 pandemic has driven uptake of and increased dependence on these. Results are displayed in the chart below and table overleaf, comparing pre- and post-COVID usage, in descending order of post-COVID use.

Q4a/b. Pre/post Covid-19, did/does your organisation have…



Source: Qa Research 2021 **Base:** 418 (all respondents)

The above chart clearly shows a substantial step-change in use of ‘video meeting platforms’, which increased by 65% during the COVID-19 to become the most commonly used digital software. We can reasonably assume this has been driven by the pandemic and social distancing measures.

‘Online training’ was the most commonly used platform before the pandemic, at 76%, which rose to 90% post-COVID. Similarly, ‘secure email’ was already fairly prevalent, in 68% of care organisations, but this increased by 12% during the pandemic.

Usage all of the listed software types increased during the pandemic, with smallest being ‘digital rostering systems’ by only 1%, meaning only a handful of organisations chose to implement a digital rostering system during COVID.

On the less prevalent end of scale, ‘digital medication management systems’ and ‘online stocktake management software’ both increased in usage during the pandemic, they remained the least frequently used of all the software at 37% and 29% respectively.

Interestingly, this research suggests that approximately 50% of the sector is using electronic care planning solutions which is an increase from the oft quoted 30% figure from previous research.[2] In wave 1 of our research we found that 30% had an electronic care planning system which they couldn’t live without and 15% had a system which they made some use of.

Thinking about how useful these different platforms are, the table below breaks down the software/systems that care organisations ‘couldn’t live without’, in post-COVID descending order.

Q4a/b. Pre/post Covid-19, did/does your organisation have…

	Have - couldn't live without		
	Pre-COVID	**Post-COVID**	**% increase**
Video meeting platforms	4%	46%	42%
Online training / e-Learning	22%	39%	17%
Access to secure email	21%	28%	7%
Social media apps	12%	23%	11%
Online recruitment facilities	15%	23%	8%
Digital rostering system	20%	23%	3%
Staff management systems	17%	21%	4%
Digital care planning software	17%	20%	3%
Digital medication management system	11%	15%	4%
Online stocktake management software	3%	8%	5%

Base 418 (all respondents)

[2] https://ipc.brookes.ac.uk/publications/adult-social-care-data-and-cyber-security-programme-report (May, 2019). Note that this report did not state that 1/3rd of care providers used electronic care planning solutions. It supposed 3 personas – completely paper based, mix of digital and paper, completely digital – and stated that roughly a third of providers fell in each category.

The above table shows that 'video meeting platforms' (46%), 'online training' (39%) and 'secure email' (28%) were the top 3 essential systems for care organisations post-COVID, which mirrors the chart on the previous page showing uptake.

'Social media apps', 'online recruitment facilities' and 'digital rostering systems' were all essential to around a quarter (23%) of care organisations. However, if we look at the % increase column, it shows that the proportion of care providers who couldn't live without social media apps increased by 11% during the pandemic. Those who couldn't live without online recruitment increased by 8% while digital rostering only increased by 3%.

Breaking down by sub-group, in almost all areas (with the exception of 'video meeting platforms' and 'online training', the most prevalent platforms) 'expert' rated organisations were significantly more likely to have access to the different software, than 'novice' rated organisations.

For systems such as 'digital care planning', 'digital rostering', 'digital medication management', 'staff management' and 'online recruitment', the size of the organisation came into play, with 'micro' and 'small' sized organisations significantly less likely to have these than 'medium' and 'large'.

Non-residential organisations were significantly more likely to have a 'digital care planning software', 'digital medication management system' and 'social media apps' compared to residential. On the other hand, residential care providers were significantly more likely to have 'access to secure email' and 'online training' than non-residential. During COVID-19, a number of offers were made available to care organisations in order to assist the sector in such a challenging time. Respondents were asked whether they took advantage of any of the following offers. Results are shown in the below table.

Q5. Did your organisation take advantage of any of the offers that were available during COVID-19 for social care?	**Count**	**Percentage**
Free iPad	122	29%
Digital Social Care Website	63	15%
Fast track application to NHSmail	62	15%
National Care Forum (NCF) Hubble	23	5%
Wi-Fi discounts from NHSX and NHS Digital	20	5%
Base 418 (all respondents)		

The table shows that take-up of these offers was fairly low overall, with a 'free iPad' the most commonly used at 29%. We cannot know from these responses whether this was the NHSX offer aimed at care homes, or other regionally based offers from local councils or CCGs.

The DSC website and fast track NHSmail both reached 15% of care organisations, while the Wi-Fi discounts from the NHS were least prevalent, only taken up by 5%. The NCF Hubble Project also reached 5% of providers however a direct comparison between this and the National schemes is not possible. The Hubble project was a first of type, digital platform which demonstrated the range of technologies available to the sector. Given these facts, and that the launch was in the middle of a pandemic, it might not be helpful to compare to the free iPad offer for example. Given that care providers were clear that they would like the kind of support offered by Hubble in this research, further work to promote the Hubble as part of the support for the sector would be helpful.

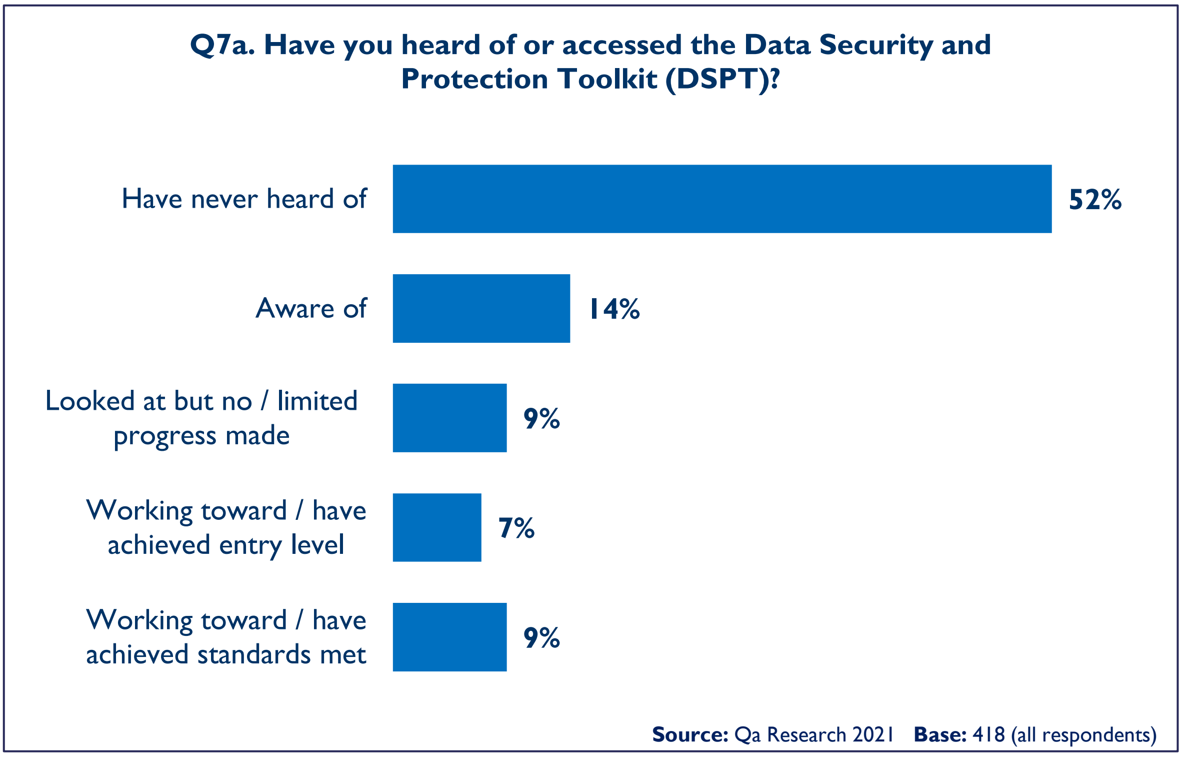
Breaking down by size, 'micro' sized care providers were the least likely to have taken up any offers, with 58% having used no offers.

The 204 respondents who had taken up at least one of the offers, were asked where they heard about them in an open response question. Results were coded and are shown in the below table.

Q6. Where did you hear about the offer(s)?	Count	Percentage
Email	81	40%
Local Council or Care Association	57	28%
NHS	27	13%
CCG	16	8%
Head office or senior staff	7	3%
Digital Social Care Website	4	2%
Skills for Care	1	1%
Other	26	13%
Do not know	12	6%
Base 204 (all who took up an offer in Covid-19 pandemic)		

The most common place where organisations heard about offers was on 'email', with two-fifths (40%) of respondents hearing about them this way. Next most popular was 'local council or care association', with just over a quarter (28%). The next most common sources were from the 'NHS' (13%) in general or their local 'CCG' (8%).

Respondents were next asked about their knowledge and experience with the Data Security and Protection Toolkit (DSPT). First care organisations were asked if they had heard of the DSPT and if so, how far they had progressed with it. Results are shown in the chart overleaf.



The chart illustrates that there is some way to go in terms of awareness of the DSPT, with over half (52%) of care organisations reporting to 'have never heard of' it.

There could be a number of reasons why half are unaware of the DSPT; each telephone interview was undertaken with the person 'best placed to answer our questions about cyber security and data protection', however we know from the previous qualitative work that one person may be best placed to answer some questions but not others. Therefore it is possible that some interviewees did not know of the DSPT but another in their organisation would have.

14% were aware of the DSPT but not looked into it any further, while nearly 1 in 10 had looked at it but not made any progress (9%). A total of 16% were working towards or have achieved a level of the DSPT.

Following this, respondents were asked whether they had heard of or accessed support for the DSPT. The results were:

- 22% had accessed IPC webinars on the DSPT, while 55% had never heard of this
- 19% had accessed DSPT guidance on the DSC website, while 57% had not heard of this
- 19% had accessed an 'other' form of support, examples of which included Local Council, CQC, NHS CCG, external IT company, Government website

5.2 Cyber security and data protection

The next block of questions relate to topics surrounding cyber security and data protection. Care organisations were asked to describe their IT security for firewalls, antivirus software and operating systems as ‘non-existent’, ‘needs updating’ or ‘up to date’. Results are shown in the table below.

Q8. How would you describe your IT security for office based devices?

	Non-existent	Needs updating	Up to date	Don't know
Firewalls	2%	2%	92%	5%
Antivirus software	2%	1%	93%	4%
Operating system	1%	3%	91%	4%

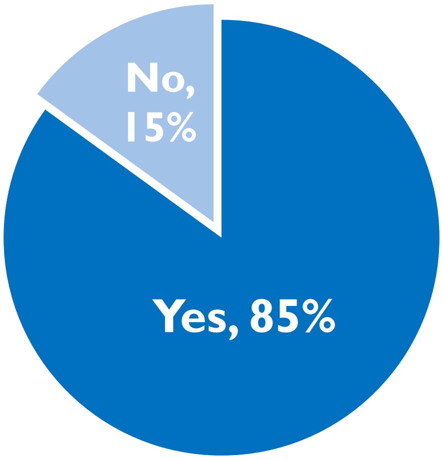
Base 418 (all respondents)

The table shows that, positively, the vast majority of care organisations would describe their IT security of all three aspects as ‘up to date’, over 90% in each.

A minority of social care providers felt their IT security needed updating, and only 1-2% of organisations described their IT security as ‘non-existent’.

Next, respondents were asked whether or not they had a designated person in their organisation responsible for data protection. The below chart shows that the majority (85%) of social care providers did have a named person responsible for data protection, or a ‘data protection champion’. While this seems a high proportion, we cannot know from this question the range of responsibilities undertaken by this role in each organisation.

Q9. Does your organisation have a named person with responsibility for ensuring the protection of confidential data (sometimes called a Data Protection Champion)?



Source: Qa Research 2021 **Base:** 418 (all respondents)

In terms of subgroups, digital 'novices' were significantly more likely to have nobody in place as a data protection champion (26% said 'No'). However, there were no significant differences by size of organisation or residential vs non-residential, which suggests there is no one size or type of social care provider leading or lagging on data protection, aside from digital maturity.

Respondents were asked a series of questions about the security measures in place for various mobile hardware devices. The below table shows the prevalence of security measures in place for mobile devices such as laptops or tablets.

Q10. What best describes mobile device security (i.e. laptop or tablet) for company provided devices and/or bring your own device in your organisation?	Count	Percentage
System password	358	86%
Encrypted device	177	42%
Up to date authentication verification app	122	29%
Two factor authentication	112	27%
Virtual desktop	90	21%
Bring your own device policy	85	20%
Don't have mobile devices	24	6%
Base 418 (all respondents)		

The table shows that the most commonly used security measure by far was a 'system password' (86%), over double the next most popular which is an 'encrypted device' (42%). Just over a quarter use an additional authentication feature, such as a 'verification app' (29%) or 'two factor authentication' (27%).

In a similar question, care organisations were asked which of the following security measures they have in place for company and personal smartphones. Results are shown in the below table.

Q11a/b. Which of the following does your organisation have to ensure security of company / bring your own device smartphones?	Count	Percentage
Company smartphones - PIN	259	62%
Company smartphones - Up to date systems	179	43%
Personal smartphones - Bring your own device policy	157	37%
Company smartphones - Mobile device management	125	30%
Company smartphones - None, don't have any	124	30%
Base 418 (all respondents)		

Almost two-thirds (62%) of care providers used a PIN code to secure company smartphones. This does not mean to say that the reverse (38%) are using company smartphones without

PINs, as the last row of the table shows that 30% responded 'none, don't have any company smartphones'. From this we can deduce that approximately 8% do not have PIN codes on their company smartphones – although this was not asked explicitly.

Care organisations describing themselves as 'expert' (74%) or 'developing' (62%) were significantly more likely to use PIN codes on company smartphones compared to 'novice' rated organisations (45%).

Care organisations were asked how they manage login and passwords for devices that access the internet; respondents could select multiple options from a pre-coded list. Results are shown in the table below in order of the most frequent practices.

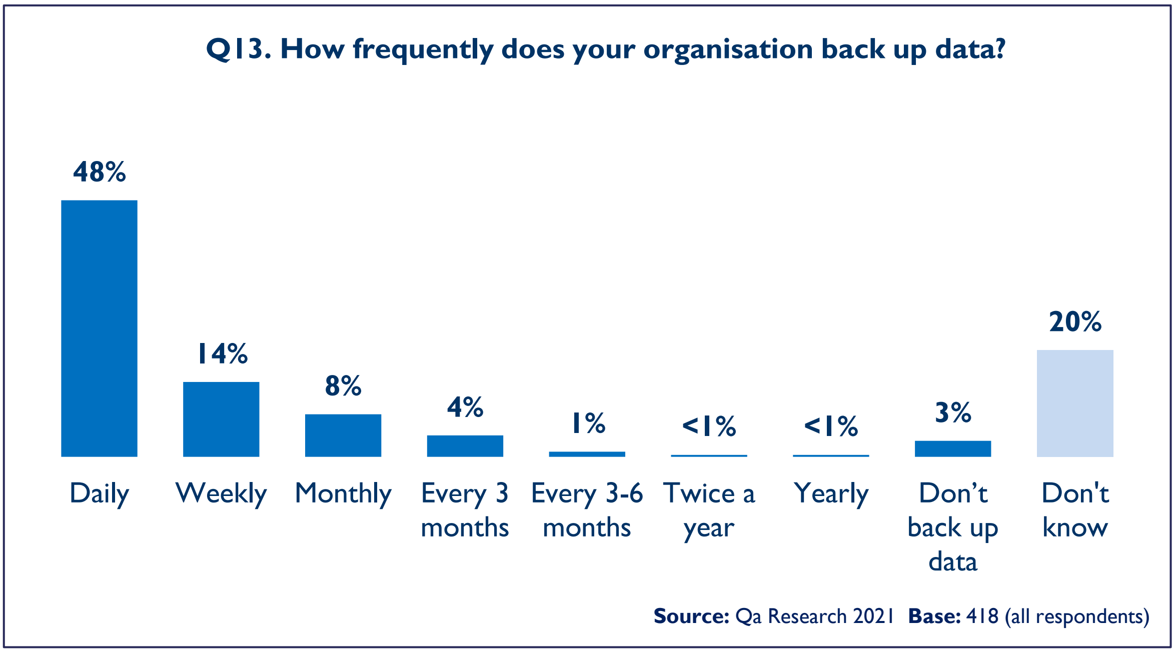
Q12. Can you describe how your organisation manages login and passwords in the organisation for devices that access the internet?	Count	Percentage
Passwords are deleted for staff who have left	343	82%
Password changed from original	325	78%
No password sharing between staff	291	70%
Password rules in place	272	65%
Other	64	15%
Base 418 (all respondents)		

The table shows the measures were fairly well used, with around 4 in 5 care organisations 'deleting passwords for staff who have left' (82%) and 'changing passwords from original' (78%).

70% had a policy of no sharing passwords between staff, while 65% had password rules in place. In terms of these two policy-related measures, 100% of 'large' sized organisations (250+ employees) had both of these policies in place, significantly more than smaller care providers.

In line with the findings so far, 'expert' organisations were most likely to have all four measures in place for password protection, while 'novices' were least likely across the board to have these.

Next, respondents were asked about their data back up systems. The chart overleaf shows responses to how frequently care organisations back up their data.



Q13. How frequently does your organisation back up data?

Source: Qa Research 2021 **Base:** 418 (all respondents)

The chart shows that almost half of care organisations (48%) back up their data ‘daily’, by far the most common frequency of backup. 14% back up ‘weekly’, while 8% back up ‘monthly’. However, it is worth noting that a fifth of respondents ‘didn’t know’ (20%) how often their data was backed up. As a general pattern, larger organisations claimed to back up their data more frequently, whereas smaller care providers were more varied in their back up frequency.

The 318 respondents who backed up data at Q13 (also excluding those who didn’t know) were asked how their organisation managed their back ups. Results are shown in the table below.

Q14a. How does your organisation manage your data back ups?	Count	Percentage
Cloud based back up on single server	112	35%
External hard drive	78	24%
Cloud based back up on multiple servers	55	17%
Back ups stored on site	34	11%
Other	39	12%
Base 318 (all who back up data)		

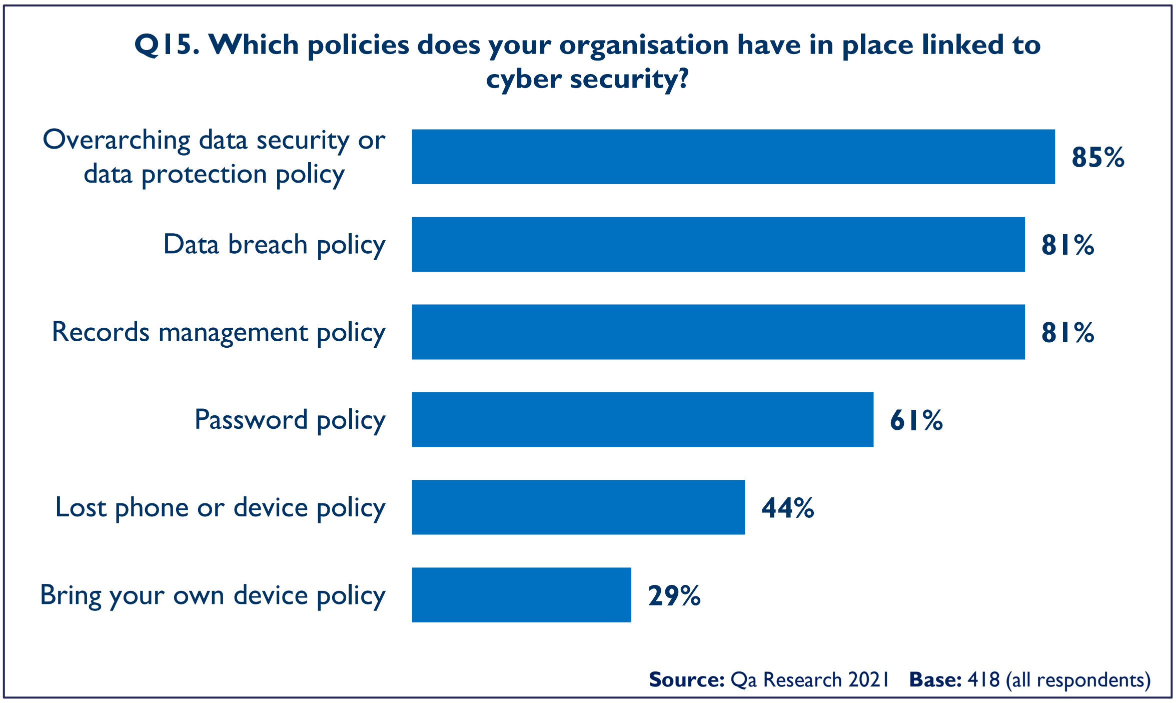
The table shows that cloud based backups on a single server were most common at 35%, with a quarter backing up on an external hard drive (24%).

Around half of all who back up data used cloud based backups in total (53%), be that on a single or multiple servers.

Respondents who backed up data were also asked ‘have you ever tested the restore process?’, the results of which were:

- 55% had not tested the restore process
- 44% had tested the restore process successfully
- 2% had tested the restore process and it failed

All respondents were next asked about which cyber security policies they have in place, results are shown in the chart below in descending order of usage.



Source: Qa Research 2021 **Base:** 418 (all respondents)

The chart shows that the most common cyber security policies were ‘overarching data security or data protection’ (85%), ‘data breach’ (81%) and ‘records management’ (81%).

‘Password policies’ (61%) and ‘lost phone or device policies’ (44%) were less well used, and a ‘bring your own device policy’ was only present in 29% of care organisations.

If we put this figure in the context of Q3, where 51% of organisations used ‘company devices only’, this means 49% of organisations have staff use their own devices to some extent. We know from this question (Q15) that 29% have a BYOD policy therefore this suggests that approximately 20% of care organisations encourage staff to bring their own devices but do not have a BYOD policy in place.

Non-residential care organisations were significantly more likely than residential providers to have a ‘lost phone or device policy’ (50% vs 35%) and a ‘BYOD policy’ (35% vs 22%).

'Medium' sized residential organisations were the most likely group to have an 'overarching data security or protection policy' in place, with 98% of organisations. This is significantly more likely than 'micro' (83%) or 'small' (79%) residential care providers.

'Expert' rated organisations were significantly more likely to have all of the listed policies in place (aside from 'overarching data security / protection') than 'developing' and 'novice' rated social care providers. Using 'password policy' as an example, 75% of 'expert' organisations had one in place, compared to only 60% of 'developing' and 46% of 'novices'.

This suggests a link between digital maturity and implementation of digital-related policies.

Respondents were asked how their policies are communicated throughout their organisation, and could select multiple options from a pre-coded list. Results are shown in the table below.

Q16. How are the policies communicated through the organisation?	Count	Percentage
Induction sessions	306	73%
Written communications	207	50%
Supervision sessions	193	46%
Via email	176	42%
Workshops	64	15%
Other	121	29%
Base 418 (all respondents)		

The most common way of communicating policies is through 'induction sessions', in nearly three-quarters (73%) of care organisations. Half (50%) of respondents communicate policies through 'written communications', closely followed by 'supervision sessions' (46%) and 'via email' (42%).

Digitally 'expert' organisations were significantly more likely to communicate policies through 'workshops' (24%), compared to 'developing' (14%) or 'novice' (11%) organisations.

29% used an 'other' method of communicating policies, these responses included:

- Employee portal / staff intranet
- Hard copy communal file
- Shared drive digital file
- Staff meetings
- Via an app
- Verbally

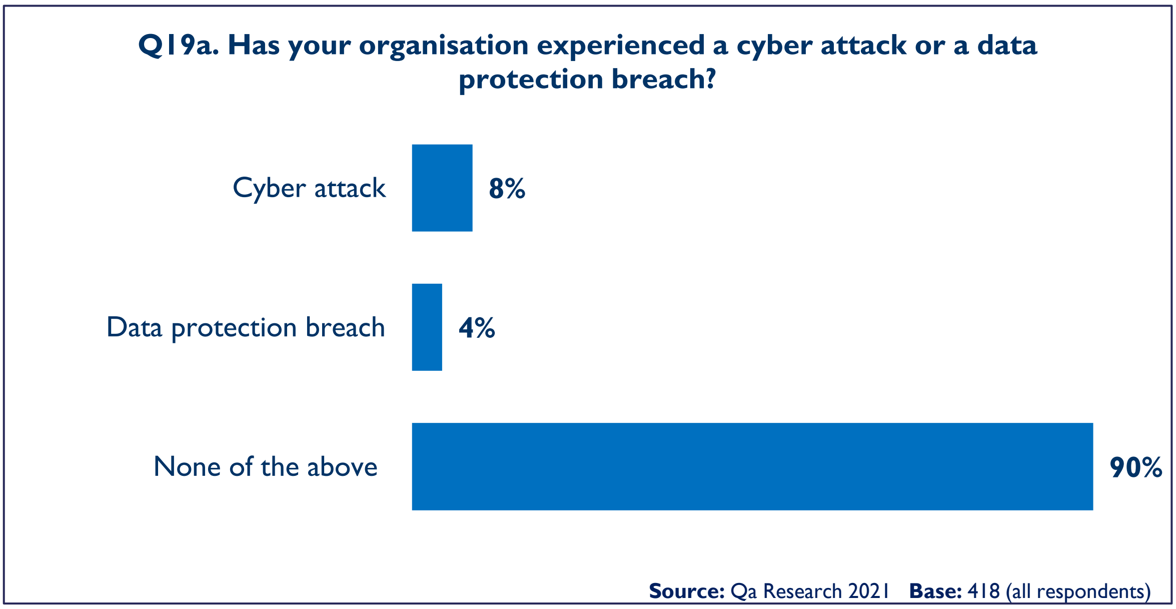
Respondents were next asked to describe the training and awareness of cyber security and data protection, selecting multiple options from a pre-coded list. Results are shown in the table below.

Q18. Describe the training and awareness raising that staff are expected to access around cyber security and data protection?	Count	Percentage
Mandatory part of induction	349	84%
Mandatory training and awareness raising on a regular basis	307	73%
Voluntary training and awareness raising on a regular basis	46	11%
No training and awareness raising training is available for staff	18	4%
Base 418 (all respondents)		

Most commonly, cyber security and data protection training formed a ‘mandatory part of induction’ (84%), closely followed by ‘mandatory training on a regular basis’ (73%).

A minority of 4% of care organisations do not have any training available on cyber security and data protection.

Care organisations were asked whether they had experienced a cyber attack or data breach, shown in the chart below.



Source: Qa Research 2021 **Base:** 418 (all respondents)

Fortunately, 90% of care providers had not experienced either cyber attack or data protection breach that they know of, however this means 1 in 10 had been through one of these. 8% of organisations experienced a known ‘cyber attack’ and 4% a known ‘data protection breach’.

Non-residential care organisations were significantly more likely to come into contact with a ‘data protection breach’ (5% vs 1% of residential). Further work could explore why this is the case.

‘Micro’ sized care providers were significantly more likely than ‘small’ sized organisations to experience a ‘cyber attack’ (9% vs 3%).

5.3 Current and future support

The following questions detail the support care organisations are currently accessing for digital and assess possibilities for future support.

Respondents were asked whether they currently access any support for cyber security and data protection, and if they did were asked to specify from where in an open response question. Comments were coded and are shown in the below table.

Q20a. Do you currently access any support for cyber security and / or data protection for your organisation? Please specify	Count	Percentage
Yes - External company	127	30%
Yes - Internal advisor	40	10%
Yes - Head office	29	7%
Yes - Independent advisor	10	2%
Yes - Local company	5	1%
Yes - External software	5	1%
No - do not access support for cyber security / data protection	189	45%
Base 418 (all respondents)		

Most commonly an ‘external company’ (55%) was used for cyber security and data protection support. Less common was an ‘internal advisor’ (18%) and ‘head office’ (13%).

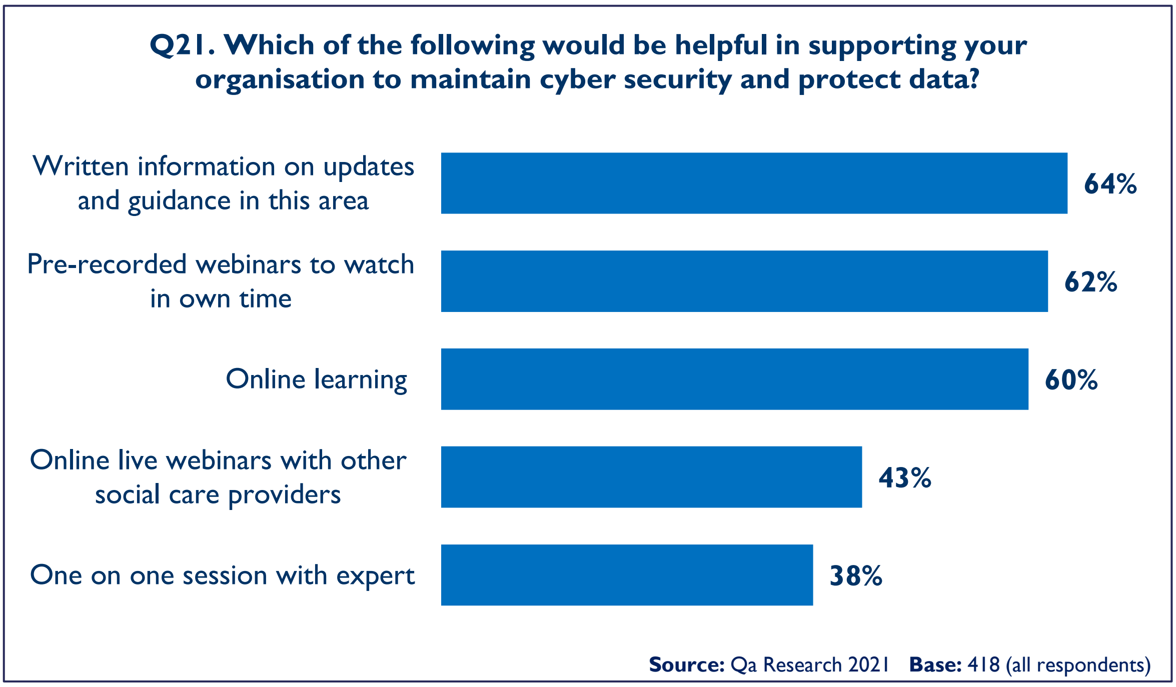
Care organisations who did not access support for cyber security were asked why they did not access this, in an open comment question which was coded. Results are shown in the below table.

Q20b. Why don't you currently access any support for help with cyber security and / or data protection for your organisation?	Count	Percentage
Dealt with internally	51	27%
No need to or no issues	40	21%
Dealt with externally	23	12%
Small company	20	11%
Experienced in field	13	7%
No specific reason	8	4%
Cost	7	4%
Base 189 (all who don't access support for cyber security)		

A quarter of care providers who don’t currently access cyber security/data protection support said this was because it was ‘dealt with internally’ (27%), while 21% said it was because there was ‘no need or no issues’.

A smaller proportion said this was 'dealt with externally' 12%, which largely meant they have an external organisation such as a local authority or freelancer if needed but they do not require their support currently.

Care organisations were next asked to think about their cyber security and data protection support needs, selecting from a list or writing in 'other'. Results are shown in the chart below.



The above chart shows the most helpful support measures were 'written information on updates' (64%), 'pre-recorded webinars' (62%) and 'online learning' (60%). Support that can be accessed at any time appears to be more widely helpful than support at a dedicated time, as 'online live webinars' only appealed to 43% of organisations.

Requests for social media based support did not appear in the 'other' comments, although some commented on their busy schedules which could suggest an appetite for bitesize learning.

Respondents were then asked what would help them make more use of the support that is currently available, from a pre-coded list. Results are shown in the chart overleaf.

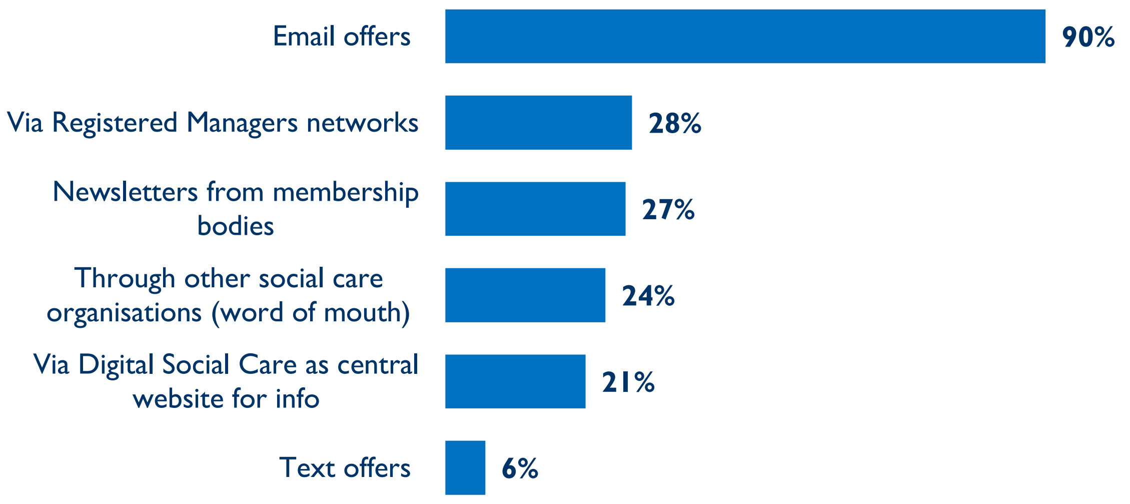
Q22a. What would help you/your organisation make more use of the support that is currently on offer around cyber security and data protection?	Count	Percentage
Greater awareness of what is on offer	326	78%
Requirement from commissioners or CQC	198	47%
Bespoke help for my organisation	159	38%
Experience of a data breach or other cybersecurity issue	147	35%
Other	71	17%
Base 418 (all respondents)		

Care providers most commonly felt that 'greater awareness of what is on offer' (78%) would help them make use of cyber security and data protection support, followed by it being a 'requirement from commissioners or CQC', which would motivate just under half (47%).

While 38% felt 'bespoke help' would encourage greater use of support, when asked, only 47% of these would be willing to pay for that bespoke support, with 53% unwilling to pay.

Finally, respondents were asked about their communication preferences, which methods of communication would be best to promote offers around cyber security and data protection. Results are shown in the chart below.

Q23. In terms of communication, what is the best way to promote offers around cyber security and data protection to your organisation?



Source: Qa Research 2021 **Base:** 418 (all respondents)

By a large margin, the chart shows that 'email offers' are the most popular way to contact care organisations, with 90% claiming this is the best way to promote offers.

Selected by about a quarter were ‘via Registered Managers networks’ (28%), ‘newsletters from membership bodies’ (27%) and ‘through other social care organisations or word of mouth’ (24%).

It appears that ‘text offers’ would not be effective as it was only selected by 6% of respondents, although ‘micro’ sized organisations were significantly more likely to select this option (9%).

Looking at subgroup breakdown, residential care organisations were significantly more likely to want to hear about offers ‘via Registered Managers networks’ compared to non-residential (36% vs 23%).

There were also a number of differences based on region. For example, London (42%) and the North East (45%) were more likely to select ‘newsletters from membership bodies’, and London (36%) were most likely to want to hear about offers through other social care organisations.

6. Conclusions

Use of digital

It appears there has been a positive development in the digital maturity of the social care sector since the wave 1 survey in October 2019, with an increase in ‘expert’ rated social care organisations and a corresponding decrease in those classing themselves as ‘novice’. Digital maturity does not vary by size of organisation, which suggests that there is not one size or type of social care provider leading the way or falling behind digitally. This shows improvement in the residential care sector, who in 2019 were more likely to be digital ‘novices’.

In terms of the hardware used in the social care sector, there is a mix of company devices and ‘bring your own device’, with the COVID-19 pandemic instigating BYOD in a number of organisations. This could go some way to explaining why the number of care providers who have a BYOD policy is far less than the number who use BYOD.

The COVID-19 pandemic has driven small increases in the uptake of most digital software or systems available to care providers, but there has been a seismic shift in the use of video meeting platforms, to the point where two-fifths ‘couldn’t live without’ them, a change experienced by most sectors. Video platforms join online training and secure email as the top 3 most used and important digital systems.

Half of organisations had not heard of the Data Security and Protection Toolkit, which suggests there is a significant amount of awareness raising to do if the goal is to expand uptake. However, there is a possibility that the survey respondent was not aware of the

DSPT but another person in the care organisation (i.e. IT, Head Office, Owner) is aware and working towards this; drawing on the qualitative interviews, oftentimes there was not a single person who could answer every question on digital and IT.

Cyber security and data protection

The majority of social care providers had a named person responsible for data protection or a 'Data Protection Champion', although the range of responsibilities of this role covers in different organisations would benefit from further investigation.

The vast majority felt their IT security was 'up to date', however the security measures in place for company devices and 'bring your own devices' were varied, both for laptops/tablets and smartphones. Most had basic security measures like passwords and PINs, but far fewer took steps such as encryption and authentication, which could be an area to draw attention to going forward.

In terms of the policies in place, most organisations had an overarching data protection, data breach and records management policy, although nearly a fifth did not have these in place. Considering the fact that all care providers must be compliant with GDPR regulations, it may be worth understanding why this minority has yet to develop a data protection policy.

Another interesting finding regarding policy was a suggested link between digital maturity and the implementation of digital policies, as 'expert' organisations were more likely to have policies in place across the board, compared to their 'developing' and 'novice' counterparts.

Around half of social care organisations back up their data daily, with larger organisations more likely to back up daily and smaller social care providers having a more varied frequency of backup. Of those who knew about their data backups, only half had tested their restore process.

Current and future support

Social care organisations appeared to prefer cyber security and data protection support to be available on demand, at a time that suited them, for example in written information, pre-recorded webinars or online learning. This marries with the qualitative research, which found that the social care sector environment was unpredictable and employees could not easily commit to specific dates and times.

Most felt that having greater awareness of the support on offer would help them to use the support that is out there, although a lesser proportion were actually willing to pay for bespoke help. Overwhelmingly, respondents said that email was the best way to let them know about offers, but a multi-media approach is usually advised, especially with busy individuals like social care sector managers who can easily miss email communications.

Therefore, other approaches like Registered Manager networks and membership body newsletters could be considered for communication purposes.

Overall patterns

As is to be expected, organisations that rated themselves as 'novices' were far less likely to have a range of software and systems in place, as well as policies to go with them, while 'experts' consistently were more developed in these areas.

In terms of size, medium and large care organisations were generally more likely to have policies in place for various aspects of digital such as data protection, cyber security, records and more. They were also more likely to back up data daily, and on the whole were more likely to have access to the full range of digital systems and software – with the exception of video meeting platforms and online training which were ubiquitously used.

However, this is not to say that smaller and micro organisations are falling behind per se, as there is no reduction in their digital maturity rating, or their likelihood of having a data protection champion. Drawing on the previous qualitative research, size may be more of a factor in terms of having available funds to invest in systems, so they may only access one or two rather than all of them.

Residential and non-residential organisations were consistent in their digital maturity, but their use of digital sometimes manifested differently, for example non-residential were more likely to bring their own devices or use digital care planning and medication systems, whereas residential were more likely to be using secure email and online training. Non-residential care providers were also more likely to have experienced a data protection breach, which is an interesting finding to monitor going forward.

Areas that would benefit from further investigation or monitoring

- While the majority (85%) of social care organisations claimed to have a named person in their organisation responsible for data protection or a 'Data Protection Champion', we cannot know what this role entails. It would be advisable to conduct some engagement with the sector to understand what responsibilities this role covers in the full spectrum of the sector (size, type and digital maturity in particular may have different understandings). There are clear roles for safeguarding leads and fire safety leads in social care, further work could explore the sector's appetite for a similarly defined role for data protection champions.
- As noted in the conclusions, it may be useful to continue to monitor known data protection breaches to understand if non-residential organisations continue to be disproportionately affected by this.
- It would be useful to monitor whether there is an improvement in the proportion of 'bring your own device' policies as organisations emerge from the pandemic, and indeed how the landscape of BYOD changes post-COVID, whether the increase in BYOD is sustained or reverts back.

Areas to support the social care sector

- Targeted support based on the systems or software that different types of organisation are more likely to use. For example, non-residential social care providers may benefit from tailored support on ‘digital care planning software’ and ‘digital medication management systems’ which they are more likely to use.
- Support and awareness raising of the Data Security and Protection Toolkit (DSPT) due to current low levels of awareness. This is already underway as part of the ‘Better Security, Better Care’ programme. It may be useful to continue to revisit this question over time to monitor progress of the DSPT (if so be sure to weight the data to the same specifications).
- The survey revealed that while many social care providers have basic security measures in place such as passwords, two-factor authentication uptake was much lower. Support on how to improve security of devices may be useful.
- Over half of organisations have not tested their restore process for data backups, which suggests this may be worth highlighting to organisations and supporting them to test this process.
- Raising awareness of the support available for cyber security and data protection, because the majority of organisations claimed that having more knowledge of what’s out there would help them use the support that is currently on offer. In addition to raising awareness, there are also some considerations regarding CQC requirements, as nearly half felt a CQC requirement would encourage them to use support for cyber security and data protection. Therefore the findings from Q22 will help inform how the sector is supported in this respect going forward.

7. Appendix

7.1 Sample breakdown and limitations

See below for a breakdown of the unweighted and weighted sample by the three factors of organisation type, size and region.

Sample Breakdown	Unweighted sample		Weighted sample	
	Count	Percentage	Count	Percentage
Organisation type				
Residential	150	36%	179	43%
Non-residential	268	64%	239	57%
Organisation size				
Micro (1-9 employees)	178	43%	217	52%
Small (10-49 employees)	160	38%	138	33%
Medium (50-249 employees)	73	17%	54	13%
Large (250+ employees)	7	2%	10	2%
Region				
East Midlands	37	9%	35	8%
Eastern	29	7%	44	10%
London	53	13%	77	18%
North East	31	7%	15	4%
North West	47	11%	48	11%
South East	67	16%	71	17%
South West	47	11%	49	12%
West Midlands	52	12%	43	10%
Yorkshire & Humberside	55	13%	36	9%
Total	**418**	**100%**	**418**	**100%**

During the fieldwork, quotas were set to attempt to achieve a sample as close as possible to the population of the social care sector, as defined by the ASC-WDS data provided by Skills for Care. However, 'micro' sized businesses and residential care providers proved challenging to access, due to a lack of contacts available for these sectors.

As such, the data was weighted in order to replicate the makeup of the sector, and also enable comparison between the 2019 and 2021 survey data.

7.2 Questionnaire

Skills for Care Digital Maturity Survey 2021

Good morning, my name is XXX, I'm calling from Qa Research on behalf of Skills for Care. May I speak to YYY?

ONCE SPEAKING TO CONTACT: Good morning, my name is XXX, I'm calling from Qa Research on behalf of Skills for Care.

We have been commissioned by Skills for Care to conduct a survey with health and social care organisations about your usage of ICT and how "digitally ready" you consider your company to be.

The survey takes around 10-15 minutes to complete over the phone. Would you be happy to run through that with me now?

S1. Are you the person who looks after cyber security and data protection?

Singlecode

Yes

No

If no

Is it possible to speak to that person as they will be best placed to answer our questions about cyber security and data protection within your organisation?

If yes, continue

Thank you. Skills for Care have a role in helping to create a well-led, skilled and valued adult social care workforce. The purpose of this research is to help them and NHS Digital plan the further support the sector needs in the area of cyber security and data protection. Your honest replies are very much appreciated and will help us prioritise work in this area.

Just to reassure you, the interview will be carried out in accordance with the Market Research Society's code of conduct and GDPR.

Your answers will be anonymous and confidential, so nobody will know what you or your organisation has said.

The legal basis for the research is Legitimate Interest, and if you would like to see a copy of the Privacy Information Notice for this research, I can send it to you in an email.

The call will be recorded for Quality Purposes. Is that OK?

Section 1: Current use of digital technology

Q1. Would you describe your organisation as 'expert' 'developing' or 'novice' in its use of digital technology overall?

Singlecode

Expert

Developing

Novice

Q2. Does your organisation have access to…

Singlecode

Yes

No

Loop

Wifi or 4G/3G

5G

Hardware (e.g. laptop, desktop, tablet)

Basic software systems (e.g. Microsoft Office or equivalent)

Q3. Does your organisation?

Singlecode

Provide company devices only

Require staff to use their own devices for work purposes

Use a mix of company devices and staff using their own devices for work (since COVID-19)

Have had a mix of company devices and staff using own devices for work (pre COVID-19)

Other, please state

Q4a. Pre Covid-19, did your organisation have…

Singlecode

We didn't have any

We had some but we didn't use them well

We had some in place and it was OK

We couldn't live without them

Only joined during the pandemic

Don't know

Loop

A digital rostering system

Digital care planning software

A digital medication management system

Access to secure email (NHSmail/ Secure Email Accreditation with NHS Digital/ Egress, please specify)

Staff management systems e.g. HR system

Video meeting platforms (e.g. Zoom/MS Teams, health consultations)

Online training / e-Learning

Social media apps

Online recruitment facilities

Online stocktake management software (e.g. PPE stock)

Other, please state

Q4b. Now thinking about during Covid-19, does your organisation have…

Singlecode

We don't have any

We have some but we don't use them well at the minute

We have some in place and they are OK

We couldn't live without them

Don't know

Loop

A digital rostering system

Digital care planning software

A digital medication management system

Access to secure email (NHSmail/ Secure Email Accreditation with NHS Digital/ Egress, please specify)

Staff management systems e.g. HR system

Video meeting platforms (e.g. Zoom/MS Teams, health consultations)

Online training / e-Learning

Social media apps

Online recruitment facilities

Online stocktake management software (e.g. PPE stock)

Other, please state

Q5. Did your organisation take advantage of any of the offers that were available during COVID-19 for social care?

Multicode

WiFi discounts from NHSX and NHS Digital

National Care Forum (NCF) Hubble **(If needed: as part of the NHS Digital Pathfinders Programme; The NCF Hubble Project aimed to help care and housing providers to understand the benefits of technology, how to build a business case for investment, and how to successfully introduce, use and evaluate technology)**

Digital Social Care Website

Fast track application to NHSmail

Free iPad ***(Only display if respondent is from a carehome)***

Other, please state

Ask Q6, if any response selected at Q5, if none go to Q7a

Q6. Where did you hear about the offer(s)?

Codes open

Q7a. Have you heard of or accessed the Data Security and Protection Toolkit (DSPT)?

Singlecode

Have never heard of

Aware of

Have looked at but no/limited progress made

Working toward/have achieved entry level

Working toward / have achieved standards met

Don’t know

Q7b. Have you heard of/accessed any of the following:

Singlecode

Have never heard of

Have heard of

Have accessed

Have used/participated

Don’t know

Loop

IPC webinars on the DSPT

Guidance on the DSPT on Digital Social Care website

Other sources of information or support, please specify

Section 2: Cyber security and data protection

Q8. How would you describe your IT security for office based devices? (by IT security we mean firewalls, antivirus and operating systems)

Singlecode

Up to date

Needs updating

Non existent

Don’t know

Loop

Firewalls

Antivirus software

Operating system

Q9. Does your organisation have a named person with responsibility for ensuring the protection of confidential data (sometimes called a Data Protection Champion)?

Singlecode

Yes

No

Q10. What best describes mobile device security (i.e. laptop or tablet) for company provided devices and/or BYOD (bring your own device) in your organisation?

Multicode

Encrypted device

System password

Up to date authentication verification app

Two factor authentication

Virtual desktop

Bring your own device policy

Don’t know

Don’t have mobile devices

Other

Open response

Q11a. Which of the following does your organisation have to ensure security of company smartphones?

Multicode

PIN

Up to date systems

Mobile device management

Other

Please specify

Q11b. Does your organisation have a Bring your own device policy for staff using their personal phone for work?

Singlecode

Yes

No

Q12. Can you describe how your organisation manages login and passwords in the organisation for devices that access the internet (e.g. wifi router, tablet, phone etc)?

Multicode

Password changed from original

No password sharing between staff

Password rules in place

Passwords are deleted for staff who have left

Other, please specify

Q13. How frequently does your organisation back up data?

Singlecode

Daily

Weekly

Monthly

Every 3 months

Every 3-6 months

Twice a year

Yearly

We don’t do data back up

Don’t know

If ‘we don’t do back ups’ or ‘don’t know’ at Q13, go to Q15, Others go to Q14a

Q14a. How does your organisation manage your data back ups?

Singlecode

Back ups stored on site

Cloud based back up on single server

Cloud based back up on multiple servers

External hard drive

Other

Please specify

Q14b. Have you ever tested the restore process?

Singlecode

No

Yes, successfully

Yes and it failed

Q15. Which policies does your organisation have in place linked to cyber security?

Multicode

Lost phone or device policy

Overarching data security or data protection policy

Records management policy

Data breach policy

Password policy

BYOD policy

Other

Open response

Q16. How are the policies communicated through the organisation?

Multicode

Via email

Workshops

Written communications

Induction sessions

Supervision sessions

Other (please specify)

Open response

There is no Q17

Q18. Can you describe the training and awareness raising that staff are expected to access around cyber security and data protection?

Multicode

Mandatory part of induction

Mandatory training and awareness raising on a regular basis

Voluntary training and awareness raising on a regular basis

No training and awareness raising training is available for staff

Don't know

Q19a. Has your organisation experienced a cyber attack or a data protection breach?

Multicode

Cyber attack

Data protection breach

None of the above

If 'Cyber attack' or 'Data protection breach' at Q19a ask Q19b, if 'none of the above' go to Q20a

Q19b. Were the policies you had in place sufficient to deal with the attack or breach?

Codes open

Section 3: Current support

Q20a. Do you currently access any support for help with cyber security and / or data protection for your organisation?

Singlecode

Yes, please specify

No

Ask Q20b if 'no' at Q20a, if 'yes' go to Q21.

Q20b. Why not?

(Do not read out – prompt if necessary):

We are clear in this area and don't have any support needs

We have internal support and expertise

We are not really engaged with this area and don't know where to access support

Codes open

Q21. Which of the following would be helpful in supporting your organisation to maintain cyber security and protect data?

Multicode

Written information on updates and guidance in this area

Pre-recorded webinars to watch in own time

Online learning

Online live webinars with other social care providers to allow learning together

One on one session with expert

Other please specify

Q22a. What would help you/your organisation make more use of the support that is currently on offer around cyber security and data protection?

Multicode

Greater awareness of what is on offer

Bespoke help for my organisation

Experience of a data breach or other cybersecurity issue

Requirement from commissioners or CQC

Other, please specify

Ask Q22b if 'Bespoke help for my organisation' selected at Q22a, others go to Q23.

Q22b. Would you be willing to pay for this bespoke support for your organisation?

Singlecode

Yes

No

Q23. In terms of communication, what is the best way to promote offers around cyber security and data protection to your organisation?

Multicode

Email offers

Newsletters from membership bodies

Text offers

Via Digital Social Care as central website for information

Via Registered Managers networks

Through other social care organisations (word of mouth)

Other, please specify

Thank and close