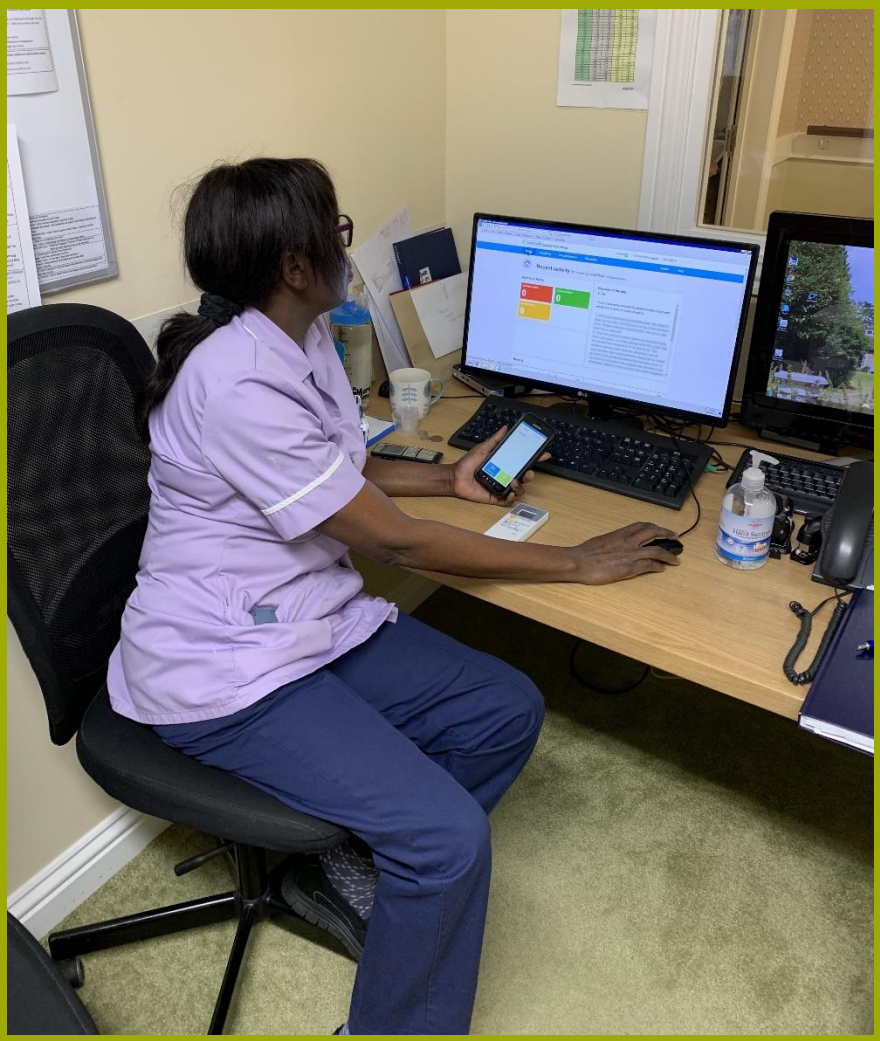
driving improvement and innovation in care

Adult Social Care Data and Cyber Security Programme 2019/20

Final Report

May 2020



Picture courtesy of Elizabeth Finn Homes

Adult Social Care Data and Cyber Security Programme 2019/20

Executive Summary

The adult social care sector is adopting technology to support care delivery. Whilst advances in technology bring benefits for the sector, and for the people the sector supports, they also present risks in how information is managed and kept secure.

To implement the outcomes of the National Cyber Security Strategy and identify the data and cyber security risks in the sector, Digital Social Care, the Local Government Association, NHS Digital and NHSX commissioned the Institute of Public Care at Oxford Brookes University (IPC) to deliver a discovery programme in 2018/19. The aim of the adult social care data and cyber security programme 2019/20 was to raise awareness of the importance of data and cyber security in the adult social care provider sector and to identify the extent to which recommendations in the 2018/19 programme report have been implemented.

Programme activity took place from July 2019 to the end of March 2020. Some activities at the end of the programme were curtailed due to the coronavirus crisis. The use of technology has changed rapidly since the lockdown. Not least that the Data Security and Protection Toolkit (DSPT) compliance requirements have been temporarily relaxed and a mass NHSmail onboarding process has begun. This report primarily reflects the activities and findings from the pre-pandemic situation. Nevertheless, the importance of data and cyber security has only increased as many digitally inexperienced care providers rapidly take up technology and criminals are using coronavirus to launch scams and cyber-attacks.

The programme supported 24 local projects and gave grants to 57 care providers, supporting many organisations to complete the DSPT as well as producing a wealth of data and cyber security guidance, training materials and other products. A key strength of the programme was the mix of organisations involved in the local projects - care providers, care associations, care provider representative bodies and councils – which allowed barriers and potential data and cyber security solutions to be explored from different perspectives.

A key conclusion of the programme is that the toolkit continues to be a “hard sell” for regulated providers and is little known by other organisations in the sector. Barriers to its use at scale include the registration process and complexity of the toolkit’s headquarters functionality, an NHS focus, and off-putting language and jargon. Most small and medium sized social care organisations will struggle to complete the DSPT in any meaningful way without support and guidance. We recommend that a social care specific assessment is developed with questions that are written in plain English so that they are more easily understood.

There are real benefits to be had from moving on-line in the ‘right way’ and making best use of the available technology. However, the data and cyber security issues and concerns that were identified in the 2018/19 programme are still very much present and there is little evidence to suggest that general risk levels across the sector have reduced

over the last year. Key risks for the sector continue to be safe use of smartphones, passwords, backups and staff training and awareness raising. In addition, publication of the toolkit does not necessarily prompt social care providers to take comprehensive cyber security measures.

The use of personal digital devices for work purposes is common across the sector, but many providers remain unaware of the risks of staff using their own devices. We advise all providers think about the implications of this and develop bring your own device (BYOD) policies and implement better security measures such as some form of mobile device management.

Digital literacy of staff in the sector is low. Making this part of the job role with an expectation of basic IT skills for all care staff is a crucial next step for the sector. Future programme support should recognise that there are a significant number of providers who struggle with even basic IT and that issues of patchy internet connectivity and digital infrastructure need to be addressed.

Culture change and skills development related to technology can be a challenge for the workforce, but digital champions and good training can make a difference. Improving the digital literacy of staff must include better awareness of data and cyber security for all types of roles working in the sector. We found that, whilst there is a wide range of data and cyber security training materials available for use (some free and some at a cost), there is nothing specifically targeted at the social care sector. Developing and promoting better, social care specific awareness raising and training materials is a priority.

We encourage councils and health commissioners to support local care providers with data and cyber security. We developed guidance that makes suggestions as to how commissioners of adult social care might support providers to adopt appropriate safeguards. This includes the recommendation that commissioners consider building into contracts with providers the requirement to complete the DSPT.

The introduction of Digital Social Care since the 2018/19 programme is a welcome development. The social care specific resources and support available from the website were well thought of and valued by all involved in the programme. However, there is low awareness of the website across the sector and we recommend that it is promoted more widely. Digital Social Care has set up a helpline to support the adult social care sector with harnessing technology during the coronavirus crisis. This, it seems to us, is a model that could be replicated to support the sector to complete the DSPT, use NHSmail or other digital tools, and improve data and cyber security post-pandemic.

Adult Social Care Data and Cyber Security Programme 2019/20

Contents

Adult Social Care Data and Cyber Security Programme 2019/20

1 Introduction

The adult social care sector is adopting technology to support care delivery. Whilst advances in technology bring benefits for the sector, and for the people the sector supports, they also present risks in how information is managed and kept secure.

To implement the outcomes of the National Cyber Security Strategy and identify the data and cyber security risks in the sector, Digital Social Care, the Local Government Association, NHS Digital and NHSX commissioned the Institute of Public Care at Oxford Brookes University (IPC) to deliver a discovery programme in 2018/19. The 2018/19 programme report made recommendations for national bodies, the NHS, local commissioners and service providers about how the sector can be supported in this area in the future.

The 2019/20 programme focused on the recommendations for local commissioners and service providers and aimed to raise awareness across councils and adult social care providers of the importance of data and cyber security – and of what they can do to adopt appropriate safeguards. It encompassed four strands of work:

- Local projects were grant funded (between £20,000 and £50,000) to work with a group of local providers to implement one or more of the recommendations and/or complete or otherwise engage with the Data Security and Protection Toolkit.
- A programme of small grants, each of up to £2,000, was made available to individual providers. The aim of this was to learn from the experience of grant recipients so as to be able to better support and advise services across the sector: recipients were required to write a report summarising their activities and learning.
- Small grant applicants and care providers engaged with local projects that had published the toolkit to 'Standards Met' or 'Standards Exceeded' were offered a supported data and cyber security risk assessment by IPC.
- IPC were asked to develop guidance for social care providers and commissioners on elements of data and cyber security where gaps existed.

Programme activity took place from July 2019 to the end of March 2020. Some activities at the end of the programme were curtailed due to the coronavirus crisis. The use of technology has changed rapidly since the lockdown. This report summarises the activities and findings primarily from the pre-pandemic situation. Nevertheless, the importance of data and cyber security has only increased as many digitally inexperienced care providers rapidly take up technology and criminals are using coronavirus to launch scams and cyber-attacks.

1.1 What is the Data Security and Protection Toolkit?

The Data Security and Protection Toolkit (DSPT) is a free, online self-assessment tool that enables organisations to demonstrate their compliance with data protection law and the ten health and social care data security standards. It is an annual assessment:

organisations review and submit or 'publish' their DSPT assessment each financial year i.e. before the 31st March each year. All organisations that have access to NHS patient data and systems must use the toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

The requirements for the DSPT are tailored to organisation type. Organisations such as NHS Trusts complete a more extensive assessment than a smaller organisation such as a social care provider. The toolkit has different levels at which it can be completed and published:

- Entry Level: this is a slimmed down version of the toolkit containing only the most critical requirements. It is only available to certain types of organisations, including to social care providers. Completing and publishing an 'entry level' DSPT assessment is a prerequisite for access to NHSmail.
- Standards Met: this includes all mandatory requirements expected of the organisational type. It allows access to NHSmail and other secure national digital solutions such as summary care records.
- Standards Exceeded: all requirements expected of the organisational type are met and the organisation has external cyber security accreditation.

For social care providers that operate under an NHS contract – that is have clients who receive NHS continuing healthcare funding or NHS-funded nursing care – then it is an NHS contractual requirement to complete the toolkit to at least Entry Level. It is recommended that other providers complete the toolkit, but it is not mandatory to do so unless the provider has access to any NHS systems such as NHSmail.

To register on the toolkit, organisations need an Organisation Data Service (ODS) code, which is a unique code that the NHS issues to all health and care providers. It is linked to organisations' CQC registration(s), although non-registered care providers can get an ODS code. If an organisation is made up of multiple sites or branches, which all follow the same policies and exist as a single legal entity, then it may choose to publish a single assessment at headquarters (HQ) level. The assessment can then be applied to all the sites linked to the HQ. Social care providers will have both a headquarters social care provider ODS code (usually A or C followed by 3 digits i.e. A*** or C***) and one social care site ODS code (usually V followed by 4 digits i.e. V****) or multiple site codes if they have more than one site or branch.

DSPT compliance requirements have been temporarily relaxed during the coronavirus pandemic. Care providers do not currently need to complete the toolkit to access NHSmail or do video calling, and the deadline for completing the toolkit this year has been extended to 30 September 2020. In addition, a new quick process to give all adult social care providers free access to NHSmail and Microsoft Teams has been set up.

Digital Social Care is a dedicated space to provide advice and support to the social care sector on technology and data protection. Specific social care DSPT guides are available to download from there as well as detailed guidance on registering and publishing assessments for social care organisations. In addition, Digital Social Care has set up a helpline to support the adult social care sector with harnessing technology during the coronavirus crisis, including support to set-up and use NHSmail or other digital tools.

2 Programme Activity

2.1 Local projects

The funding for local projects was distributed in two phases. The application window for the first phase of grants ran from 10 June to 12 July 2019. Thirty-seven applications were received in the first phase, of which eight were successful. IPC support to these eight started in September 2019. Twenty-two applications were received for the second phase of funding, which closed on 11 October 2019. Fourteen local projects were successful in this round. IPC support to these projects started with an initial training day for local project managers on 14 November 2019. Two additional projects that focused on data and cyber security from the perspective of services for adults of working age were also agreed, with support to these projects starting in December 2019. A report giving brief details of all these projects can be found here.

IPC supported local project managers to refine their project proposals and plans and delivered local support sessions to participating groups of providers as well as facilitating an event on 26 February 2020 for all local project managers to share learning. We supported each project manager, and providers in each local group where appropriate, with project work and with the Data Security and Protection Toolkit. A list of all the products developed by local projects is given at Appendix One. Local project activity can be grouped into five themes:

1. DSPT and NHSmail: London Borough of Barnet, Central Bedfordshire Council, Durham County Council, Shropshire Partners in Care, Staffordshire County Council, West Midlands Care Association.
2. The safer use of smart phones and other mobile devices: Manor Community, North Yorkshire County Council, Peterborough and Cambridgeshire Care Association.
3. Staff training and awareness: Blackburn with Darwen Council, Care England, East Midlands Care Limited, Nottingham City Council.
4. Adopting new technology: Dorset Partners in Care, Hampshire Care Association, North Tyneside Council, Stonewater and First City Nursing, Wiltshire Care Partnership.
5. Implementing safe data and cyber security practices: Lincolnshire Care Association, National Care Forum, Nottinghamshire County Council, Voluntary Organisations Disability Group and Association of Mental Health Providers.

IPC undertook an online survey with participating providers. The aim of the survey was to help inform sector learning and to influence next year's programme, including how best to engage providers with this subject. Providers were asked about their experiences of taking part in the programme and their ideas for improvements. A summary of the feedback gathered through the survey is given in Appendix Two.

2.2 Small grants

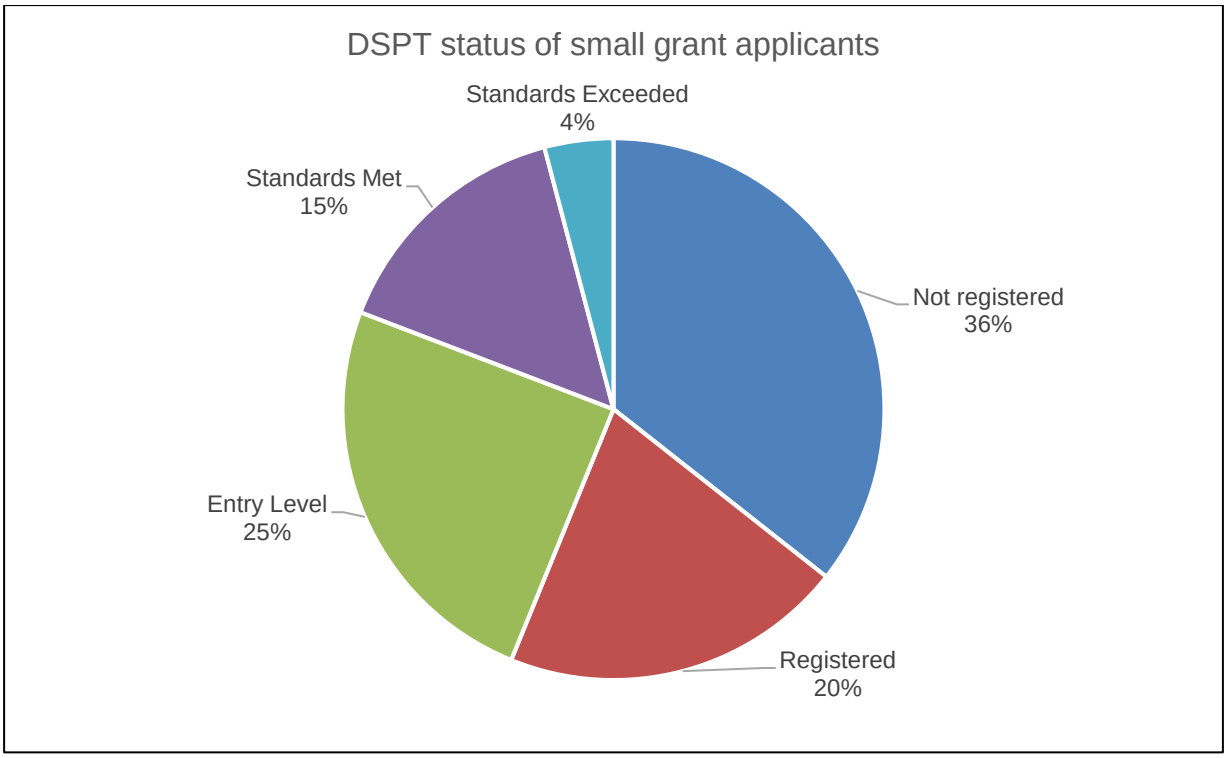
Grants of up to £2,000 each were available to help social care providers assess and manage digital risks. Seventy-three applications were received, including one that was from Scotland and hence out of scope. Four were from organisations that provide services on a national basis, with the rest split between the regions.

Over half of applications were from organisations that provide services mainly for older people (39) followed by 20 applications from organisations that support a range of different groups. Nine services provide support to people with learning disabilities and five to people with mental health issues. There were no applications from services that mainly support people with physical disabilities or sensory impairments.

Most applications were from care homes or services that mainly provide homecare – 56 applications in total from this type of provider – whilst 8 organisations described themselves as providing a range of services. The breakdown of applications by type of service mainly provided is shown in the table below:

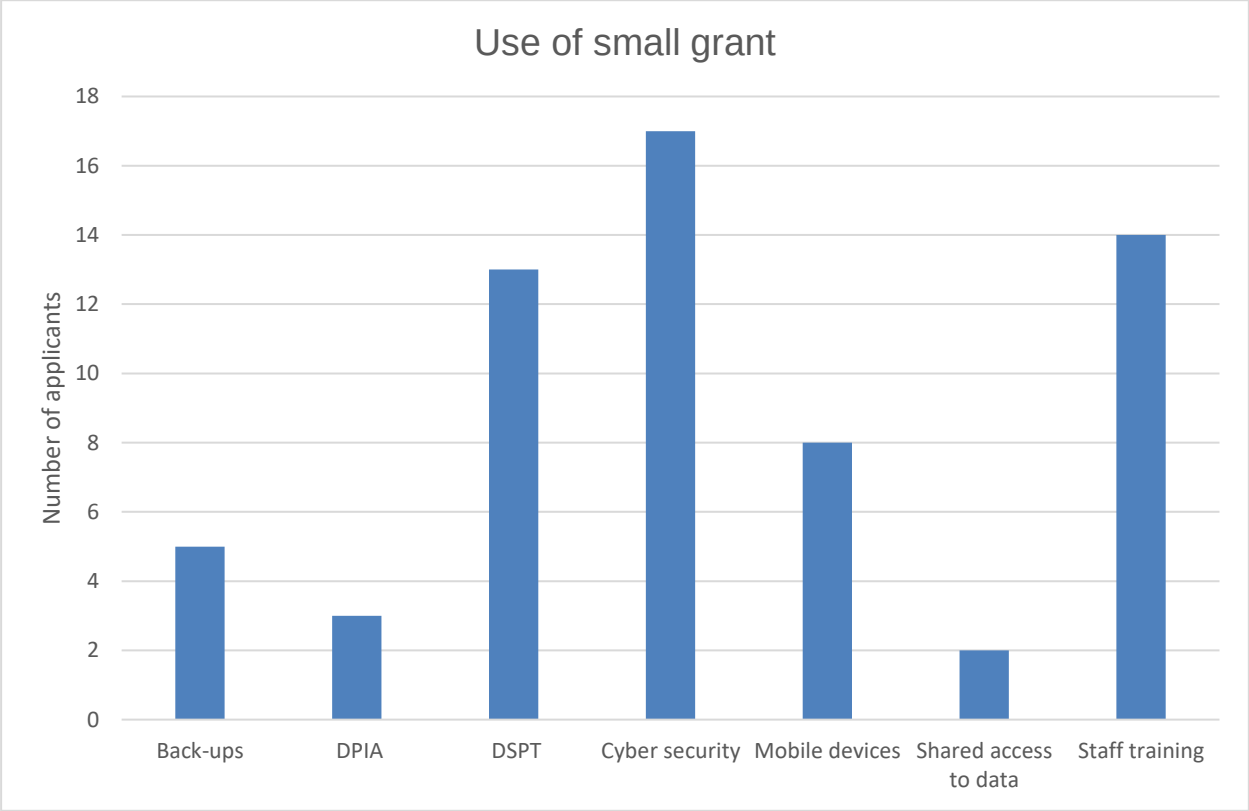
Type of service	Number of applications
Nursing or residential home	29
Homecare	27
Supported living	2
Informal support	1
Day service	2
Range of services	12
Total	**73**

From the self-declarations of providers on the application form, just over a third of applicants (26) had not registered on the DSPT, whilst a fifth (15) had registered but no level has been reached. A quarter of applicants (18) had published the toolkit to Entry Level and nearly a fifth had published to Standards Met (11) or Standards Exceeded (3), as shown in the graph below.



In total, 57 applications were accepted by the Programme Board, 14 were rejected as not meeting the criteria and 2 providers declined the grant. Most applicants who were not accepted were asking for grant support to move from paper care recording systems to digital / electronic systems or for the purchase of computer equipment or software (e.g. updating from Windows 7).

What successful applicants applied for support to do can be grouped into seven overarching areas as shown in the graph below. The most common reason for providers applying for a small grant was to review their cyber security (17), followed by staff training (14) and then staff time for or advice to enable completion of the DSPT (13), improving mobile device security (8) improving backup arrangements (5), completing a data protection impact assessment (DPIA) (3) and appropriate access to shared data (2). Note that some providers planned to spend the small grant on more than one of these areas.



All successful applicants were contacted by IPC and, if they had not published the toolkit to Standards Met or Standards Exceeded, were signposted to guidance on Digital Social Care and offered telephone support to help them complete the toolkit. Those that had published the toolkit to Standards Met or Exceeded were contacted by IPC and offered a supported data and cyber security risk assessment – see section 2.3.

2.2.1 Small grant funded activities

In terms of how the monies were spent, most were spent funding activities by staff within the provider organisation, but almost a third involved some degree of external expenditure on buying in specialist IT expertise or an application of some description. For small and medium size organisations the use of third party support and suppliers clearly makes sense. Two providers described how their work on the project had led them into longer-term IT partnerships with specialist IT companies. In contrast, one

provider invested in training up their in-house trainers (along with the Finance Manager) rather than developing a partnership approach.

A number of providers commented upon the effectiveness of some generic systems in terms of cyber security, particularly if care is taken in setting them up correctly at the outset. Sharepoint and Microsoft 365 were examples given in this regard.

A key theme running through many of providers' reports was the need to carry out activity in more than one area of data and cyber security in order to achieve the desired outcome. Achieving Standards Met on the DSPT, for example, often involved the need to up-grade systems, train staff and to develop or review policies and procedures. Similarly, the introduction of new systems or applications also required staff training and developing new, or revising existing, policies. Providers found that improvements in one area could well be negated if there was not similar improvement elsewhere in their organisation.

A further key theme running through the reports is that getting it right in terms of data and cyber security can take time and resources, particularly where improvement in one area flags up the need for improvement in other areas. However, it was generally found to be valuable and worthwhile. As one provider put it:

"Updating your policies, practices and procedures will cost little financially, however, having the correct systems in place is priceless for giving your clients, visitors and employees confidence that their data is secure."

Whilst confidentiality of data was seen as an important issue, many of the providers emphasised the potential that improved electronic systems can have for greater efficiency and effectiveness within the service.

The experiences recorded by those organisations that used the grant to focus upon implementing a mobile device management (MDM) solution are instructive and provide some noticeable contrasts. All looked at third party solutions, but one went with a software provider whose products they already used, one went for a provider delivering a simple single platform approach whilst a third went for one that enables access to a range of other programmes. A fourth trialled a system for six weeks before concluding that they did not have the necessary skills in-house to use the solution. They offered the following advice:

"Concentrate on simple measures first, ensuring that when the phone is issued it has all the correct settings, two stage passwords are in place and careful monitoring from the centre when compliance is not being met. Making sure that the care worker is confident on how to use the phone and stress not to alter any of the settings."

These findings suggest that MDM may be too complex for small providers to buy and operate their own system because of a lack of specialist IT knowledge and capacity. The North Yorkshire local project concluded that it is often simpler for providers to buy this service in from an outside source (see section 3.2 below) and most providers 'buy-in' a complete MDM solution from a supplier.

A number of providers had projects that focused on more secure arrangements for electronic file access or moving towards a 'paperless office'. One provider looked to up-

date their filesharing software to a new platform that operated more simply and straightforwardly and which they hope will allow them to maintain it over time without requiring further input from outside specialists. Moving to a similar approach, another provider took the opportunity to review and refine their filing structure as well as securely deleting a lot of old material. A third provider identified a range of advantages that accrued from implementing a new electronic HR system, including reduced travel costs and flexibility of access to records. A fourth provider focused their project around the introduction of an electronic care planning system, identifying that it provides staff with all the information they need and allows them to focus upon providing care, rather than doing paperwork.

In terms of security, one provider introduced two factor authentication (with hardware tokens) for all their mobile device users. They found that this added an extra layer of security and allowed staff to use other computers when out of the office. They also felt that whilst there was an initial outlay for the tokens the ongoing costs were limited. Individual's user tokens provide a code to access the system (alongside the username and password). Because the code varies each time the token is used, no access can be gained without having the right token for that specific username. Such systems are widely used elsewhere, including within the NHS.

The other side of security is access, and two providers in particular focused upon widening access to information within their system. One introduced an app that let people using services and their families see their care planning information, as they put it:

"…in a manner whereby we were confident in sharing the data, without fear of reprisal. This included creating a sig-off form for people to complete to give access to families"

They undertook a data protection impact assessment, which initially felt daunting to do but proved to be quite straightforward and provided them with the assurance to go ahead. Another provider looked to re-design their webpage with enhanced encryption layers and a more user-friendly approach. They also developed their social media presence by creating a Facebook page for themselves.

Staff development, whether general awareness of cyber security or linked to other specific developments, featured in many of the small grant activities, often as an adjunct to the implementation of new systems or policies and procedures but also in some, as the main focus.

One project focused on sourcing awareness training for staff. They found very little that they felt they could use but did identify that, as a social care provider, they had free access to the eLearning for Healthcare Data Security Awareness training module. However, they felt that they needed something in addition to that because training needs to be consistent and not just on an annual basis - and it needs to be more engaging. They explored developing their own training video but had not started this within the programme timescale.

Another provider also researched the market for cyber security training for their organisation. They followed a structured process that saw them undertake desktop research that identified 87 potential providers followed by a selection of on-line demonstrations, and from this reduced it down to three potential providers. They

convened a focus group of staff from across the organisation that further reduced this choice to two, with whom they were negotiating to ensure best value for money. As part of this consideration they looked at both the style and length of the available on-line packages and concluded that they preferred focused, short and punchy videos over the longer variety that cover more topics in a single episode. They considered the need to test the effectiveness of the training being delivered and the possibility of supporting training with, for example, simulated phishing attacks.

Other providers focused their staff development upon specific groups of staff within their organisation. One looked at how to ensure that staff and volunteers with a learning disability are able to comply with cyber security requirements. They started to develop differentiated induction courses and assessment sheets for young people between 18 and 25 who have a disability or barrier to learning and are training to work with other young people, to ensure they know and understand what should and shouldn't be shared.

Another provider focused upon ensuring that key staff have undertaken GDPR training, accessing a range of external sources to do so. One provider delivered training sessions to staff in each of its homes, with an emphasis upon providing basic knowledge to older staff with little experience of using computers.

A number of providers sought to enhance their overall data and cyber security by undertaking a review. One provider used an assessor from an external certification body to complete a gap analysis against the ISO 27001 standard for information security management systems. The assessor spent time preparing, then one day on-site to understand the organisation and practices before providing a report. They found that this exercise gave them a comprehensive understanding of their current practices for securing information versus the requirements of internationally accepted best practice contained within the standard. It also provided opportunities to:

"….discuss how we are likely to design and operate a system within our organisation, to support high quality services with robust risk management, and effective controls that are demonstrable to those we support, our stakeholders and funders, and our regulators…. A firm foundation upon which to identify and prioritise the projects required to improve our practices and mitigate our risks in accordance with the standard."

Similarly, another provider engaged an external consultant to help them complete the DSPT and provide guidance on how to improve current systems and processes. For example, developing a privacy notice, which is now embedded in the Service User Terms and Conditions and Service User guide. They also obtained guidance on completing the Information Asset Register and Record of Processing Activities.

2.2.2 Small grant learning points

All participating organisations were invited to offer up learning points for other organisations. Many of them did, providing a wide range of comments, some of which were generic but others very focused upon their particular project. Some themes emerge from the general comments:

- There are real benefits to be had from moving on-line and making best use of the available technology.
- Paperless services can greatly increase efficiency.

- Data and cyber security do, though, need to be taken seriously.
- Giving it the right time and proper resources is important.
- It is important to ensure you have the right (expert) support for your systems. One provider wrote: *"Other small social care organisations could probably learn that if you can get the right people to support its implementation then it isn't as worrying".*
- One size definitely does not fit all in this area.
- Ensure you have effective risk management.
- Make sure to engage with those most affected.

2.3 Data and cyber security risk assessment

As part of the Adult Social Care Data and Cyber Security Discovery Programme 2018/19, IPC developed a risk categorisation model based upon National Cyber Security Centre guidance. Nine risk categories were RAG rated (red/amber/green/not known or not applicable) for preventative measures and by how ready and able a service would be able to cope for 48 hours without key systems if a problem did occur. Details of the risk categories are given in the 2018/19 Programme Report.

Small grant applicants and care providers engaged with local projects that had published the DSPT to Standards Met were contacted by IPC and offered a supported data and cyber security risk assessment - using the methodology of the discovery day visits from the 2018/19 programme - to provide RAG ratings for key elements of data and cyber security risks.

Twelve visits were arranged, with four care providers withdrawing from the process due to winter pressures or Covid-19. Eight visits were undertaken with the following service types: three homecare providers; three care homes for older adults; one adult learning disability care home provider; and one adult learning disability supported living provider. Of these providers, one is the local franchise of a national charity, one is a multi-regional provider, four are regional providers; and three are single site local providers.

2.4 Additional guidance

As well as supporting local projects and small grant recipients, IPC produced guidance for the sector on elements of data and cyber security that were identified as gaps. These three products are:

- Guidance to support service providers to identify their top three data and cyber security risks, which should enable providers to answer question 1.8.3 of the DSPT: What are your top three data security and protection risks?
- A review of data and cyber security training and awareness raising materials and guidance on their appropriateness for social care staff.
- Guidance for commissioners of adult social care on how they could better support local care providers with data and cyber security.

Initial drafts of these guides were developed for comment and testing by councils, care associations and care providers, which informed final versions.

3 Findings

3.1 Data Security and Protection Toolkit and NHSmail

Most of the local projects supported groups of 10 to 15 local providers to complete the Data Security and Protection Toolkit (as well as to explore other data and cyber security issues or solutions). In addition, six projects concentrated on supporting providers to complete the toolkit to either Entry Level or Standards Met and to register for NHSmail. They tested a mixture of methods of support and supported larger numbers of providers to complete the toolkit. These projects are summarised below:

- **London Borough of Barnet** built on the programme of work that was already in place to support toolkit completion to Entry Level (via webinars) and promote the take up of NHSmail to all care providers in Barnet. The council contracted Healthy London Partnership to deliver half day Entry Level workshops for about 100 providers plus one-to-one support visits for providers to achieve Standards Met.
- **Central Bedfordshire Council** built on previous work to promote the toolkit locally and to take up NHSmail. Bedfordshire Care Association and Central Bedfordshire Council co-ordinated provider engagement and Hertfordshire, Bedfordshire and Luton ICT Services delivered half-day Entry Level and Standards Met workshops.
- **Durham County Council** built on previous collaboration with NHS England North, which focussed on supporting provides to achieve Entry Level, to extend the support offer. They tested a peer support/buddying approach (facilitated by Microsoft Teams and some face to face meetings), to complement a workshop delivered by NHS England North trainers, and enable providers to publish at Standards Met. This offer was made to 12 domiciliary care providers that had previously achieved Entry Level.
- **Shropshire Partners in Care** built on earlier DSPT awareness raising training delivered locally to offer providers the opportunity to be supported to complete the toolkit. They delivered a series of four half-day Entry Level workshops for 12 providers that had no previous knowledge of the toolkit and a series of three half day workshops for six providers who were already at (or nearly at) Entry Level to enable them to reach Standards Met. They also facilitated a cyber security conference for local providers.
- **Staffordshire County Council** supported 13 providers to work towards and achieve Standards Met by contracting Midlands and Lancashire CSU to provide two workshops and interim virtual support (plus a few visits to providers that struggled). They also undertook research to identify the technological (IT knowledge, equipment, connectivity of systems) and process (policies, procedures and practice) risks and barriers that social care providers face in attaining DSPT compliance.
- The **West Midlands Care Association** (WMCA) delivered half day workshops (supported by pre-workshop phone engagement) to 163 care providers to support them to complete the toolkit to Entry Level and open their NHSmail account(s).

In addition, organisations that were part of the small grants programme were expected to complete the DSPT and publish at Entry Level or at Standards Met if they were already at Entry Level. Of the 57 successful small grant applications, 49 providers completed their grant funded activity and submitted a report. One provider published the DSPT to Standards Exceeded, 21 published at Standards Met and 22 at Entry Level whilst the rest registered on but did not publish the toolkit.

Recipients of small grants were invited to provide feedback about registering or completing the toolkit, and 28 did so. Their comments fell into four categories - support mechanisms; time required; standards and requirements; and the wider value of completing it – and are reflected in sections below. In addition, one provider queried the value of a self-assessment suggesting that there should be some further vetting of submissions, and one organisation expressed disappointment at the lack of checking of the toolkit entries: *"It is disappointing that no one actually checks that the toolkit has been completed correctly."*

3.1.1 Performance monitoring data

Local projects struggled to find performance data for both the DSPT and NHSmail i.e. which local providers had registered or published the DSPT and which care sites had access to a generic shared NHSmail account. Without this they do not know their baseline position and it is hard to judge the effectiveness of wider council, NHS or care association support in the area.

Improvements to the public Organisation Search function of the toolkit were made in autumn 2019 so that you can now download the latest toolkit status of organisations in a spreadsheet. This is widely welcomed as it allows you to search for providers' current DSPT status. However, this functionality does not allow you to search by location (search by provider type and commissioner is possible but usually the commissioner is not recorded). So, councils or care associations cannot extract a list of all social care providers' DSPT status in their area. This is a missed opportunity. It is possible to download care provider information from the CQC website and then copy and paste that data into a spreadsheet and, using the vLookup function in Excel, to marry up the two data sets and be able to work out the location of providers. This seems unnecessarily complicated, beyond the technical ability of some users, and it would be much more user-friendly if the location (by council and/or CCG) was available in the DSPT organisational search.

We are not aware of an equivalent public mechanism that would allow councils or care associations (who themselves do not have NHSmail accounts) to know which care sites – not individuals - have access to NHSmail accounts. Being able to see live tracking data of which social care providers have signed up to NHSmail in their local authority (or CCG) area would be enormously helpful.

3.1.2 Issues with toolkit registration

A key issue for providers completing the DSPT was the difficulties they had appropriately registering their organisation on the toolkit or knowing whether the toolkit is applicable to them. Non-regulated services, or services that are not care homes or domiciliary care organisations, in particular feel that the toolkit is not suitable for them and don't know how to register and, if they do so, how their ODS code(s) reflect their organisational structure.

Entry Level is only available for social care providers, and organisations have to register as either a care home or a domiciliary care organisation to be classed as a social care provider (in the toolkit). Many organisations register as a charity (or other organisational type that they feel is more appropriate to them) and hence are not able to publish at Entry Level. Neither the DSPT Entry Level Workbook nor Entry Level Guide mention this facet of the toolkit. We recommend that this functionality changes i.e. a 'social care

provider' organisational type is created that replaces care home and domiciliary care and gives access to Entry Level. Until then this should be identified in the guidance and the helpdesk standard response amended. Currently, if organisations contact the helpdesk to say that they can't publish at Entry Level – even if they have identified themselves as a social care provider - they are not advised that the 'organisation type' registered in the toolkit affects Entry Level publication. Notwithstanding the glitch in HQ functionality that persisted in early 2020, the helpdesk response to Entry Level queries about this issue does not solve the problem. An example (redacted) helpdesk query and response and follow up IPC response to this provider (who received a small grant), is shown in Appendix Three.

The complicated nature of how the toolkit can be completed for single-site and multi-site organisations and how ODS codes are used is causing great difficulty in the sector. This is an issue not just for large organisations but even for many small and medium sized ones due to the nature of ownership in the sector and the fact that even single-site organisations have a headquarters A code. The new guidance Registering for and completing the Data Security and Protection Toolkit for Social Care Providers is very welcome and no doubt reflects the functionality of the toolkit. However, it is technical in nature – mirroring the complications of the toolkit – and many providers struggle to follow it. For example, the following is a quotation from the guidance which we think would be difficult for many people to follow:

*"Some organisations, particularly those that provide a wide range of services may also have additional ODS codes such as those for non NHS organisations, e.g. 8***** etc. However, for the purposes of Care Home or Domiciliary Care provision such codes will not cover your sites on the Data Security and Protection Toolkit.*
*It may be that you still need a Data Security and Protection Toolkit submission in respect of the separate services covered under such codes. If that is the case you should publish against that code and then use the relevant option described in section 3 to extend coverage to the appropriate A***/C*** codes, followed by publishing on behalf of the sites as described in section 2"*

This guidance does not explore the internal governance issues related to multi-site companies. This includes, for example, what role registered managers of sites that are covered by their organisation's headquarters toolkit publication should have – so should they be able to and expected to view their headquarters publication and sign off that their site meets this standard for instance? An effective tactic for many local projects is having individual meetings with medium-sized local or regional organisations to discuss organisational structure and an appropriate approach to the DSPT. The headquarters functionality, whilst practical and welcome, may lead to discord in the sector if 'big players' are seen to circumnavigate effective data and cyber security self-assessment at a local level. It will be important to any further roll out of support to the sector, that support organisations planning to give advice to providers about the DSPT help them to register and supply ODS codes. In addition, we recommend that there is a single channel of communication with large national providers and that this is clearly communicated to local and regional support organisations.

At the beginning of the programme, the HQ functionality built-in to the toolkit was not automatically turned on i.e. providers needed to contact the exeter.helpdesk@nhs.net and ask for HQ functionality to be turned on for their headquarters site. This added another barrier to social care provider take up of the DSPT. We understand that this

may now have been rectified but we have not tested this and the Digital Social Care guidance still advises providers to contact the helpdesk "and ask for HQ functionality to be turned on for you [*sic*] headquarters site". We recommend that HQ functionality is automatically turned on for A code registration and/or that the DSPT registration guidance is amended.

3.1.3 Issues with toolkit functionality and questions

Providers found the toolkit "time consuming" to complete. Overwhelmingly, care providers found the language used within the toolkit to be difficult due to use of jargon, overuse of acronyms, the complex 'information governance' language used which was not familiar to care providers, and NHS rather than social care focus. Some examples of the many comments are reproduced below:

- *"The jargon of the DSPT needs to be adjusted to match language used in care organisations- it is all very 'NHSy'"*
- *"I found it so unwieldy and not really applicable to a fairly small voluntary organisation like ours"*
- *"A sledgehammer to crack a nut"*
- *"Improve ease of access for those not already familiar with IT/jargon by providing laymen terms"*
- *"Less jargon and greater use of layman's terms"*
- *"Too long, too complex and insufficiently relevant to social care"*

Recipients of small grants felt that the toolkit was designed for the NHS and was not suitable for use by the social care sector - and some of the questions were actually not relevant outside of the NHS. One queried the completion rate required for staff training, citing the large size of their organisation and the high turnover amongst their staff.

VODG and AMHP (see section 3.5) reported that smaller organisations struggled with understanding toolkit terminology and responsibilities especially around issues such as the Caldicott Guardian and Senior Information Risk Officer roles and acronyms. In general, they reported that the DSPT was widely seen as a regulatory burden rather than a springboard for better use of digital opportunities and it is unlikely as things stand to be undertaken by large numbers of providers that do not contract with the NHS.

We strongly recommend that the questions in the toolkit are reviewed so that it is more easily understood – written in plain English - being mindful of the general low level of digital maturity within the care sector and poor standard of literacy in the UK. This is in addition to the recommendations for specific questions outlined below.

An example of terminology that is likely to confuse social care providers is assertion 6.2: "All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway." Many people might be unclear about what a 'corporate gateway' is in this example.

The specific wording of the assertions or evidence items is very important as they may have implications or unintended consequences for care providers. For example, assertion 3.2 states that "Staff pass the data security and protection mandatory test." And evidence item 3.2.1. is "Have at least 95% of all staff, completed their annual Data Security awareness training in the period 1 April to 31 March?" The phrasing of these

implies that there is one mandatory test that social care provider staff have to take. This is a key barrier as many organisations think that all their staff have to pass the national Data Security Awareness eLearning. This is compounded by the fact that the eLearning for Healthcare portal is difficult to access. Rephrasing the assertion and evidence item to be “Staff have annual data security and protection training” and “Have at least 95% of all staff completed data security and protection awareness training in the period 1 April to 31 March?” would help as would developing better, social care specific training modules and examples of awareness raising that are appropriate to the different types of roles working in the sector.

A further consideration is that this is a self-assessment and the questions should be designed to make respondents ask themselves (or external support) the right question. An example of this is section 6.2: evidence item 6.2.1 asks for “Name of the anti-virus product” and 6.2.2 “Number of alerts recorded by the AV tool in the last three months”. 6.2.2 is a key stumbling block for most small social care providers as they don’t know this information and, if they continue with the toolkit at this point, and many don't, the vast majority will ask their (usually external) IT support for the answer.

What question they ask their IT support will depend on the wording of the evidence item. Currently, evidence items 6.2 push providers to ask ‘what anti-virus software do we use’ and ‘how many AV alerts do we have’ to which they would get a numerical answer (say 14). Most providers will not know whether this is good or bad and enter the answer 14 into the toolkit without understanding what it means. How does that help in a self-assessment? A more useful question to prompt care providers to ask of their IT support is ‘Have we installed up-to-date anti-virus software on all our devices and do we keep it up to date?’. This would ensure that their IT support confirms, in layman's terms, that they have followed recommended guidance for malware.

A number of organisations that received small grants reported that they accessed support in completing the toolkit from either their local CCG, from guidance published on Digital Social Care or from IPC, and those that fed back were very positive about the support received from all sources. Others commended the quality of the guidance documents available (we signposted providers to Digital Social Care guidance).

Recommendations for changes to specific questions asked in the toolkit standard for 2019/20 and advice contained in the DSPT guides and workbook available to download from Digital Social Care are given in Appendix Four.

We recommend that a new level should be available to be published on the toolkit – Improvement Required or Standards Nearly Met (or similar wording) – that allows providers to publish an action plan rather than an assertion that the standard has been fully met. Currently, Standards Not Met covers providers that have answered none or only a handful of assertions through to those that have completed 55 out of 56 assertions. Many providers get so far with the toolkit and then cannot progress until they have carried out planned activity such as training a group of staff or developing a new procedure. Being able to publish the toolkit in a way that highlights their outstanding actions would be helpful. Currently, there is functionality in the DSPT dashboard for users to download a spreadsheet that lists the remaining evidence items which they must provide in order to meet Standards Met. If this could be linked to actions required or comments input in the assertions it might motivate providers who are nearly at Standards Met and give a more detailed picture of progress for the sector.

3.1.4 Issues with National Administration Service NHSmail registration process

There are three NHSmail registration routes for social care providers:

- The national administration service (NAS) process through the registration portal. A generic shared site account and individual accounts linked to the shared mailbox can be opened through the NAS portal for each site that provides social care. For providers with over 25 care sites wishing to join NHSmail in bulk via NAS a different process is available by application.
- The self-management process, which is for care providers who have the technical capability to carry out the administration activities for their own NHSmail accounts. This route is usually only considered by larger care providers with good internal IT support.
- The local registration process i.e. being sponsored by a CCG or CSU, which was used in the past but we believe has been discouraged in favour of NAS.

In addition, there is a separate registration route for non-social care providers i.e. other organisations supporting publicly funded health and social care can apply to join NHSmail via the third party process and these are reviewed on a case by case basis. The West Midlands Care Association (WMCA) registered for an NHSmail account using the third party process and reported that it is much easier than the NAS process used by social care providers.

A new quick process to give all adult social care providers free access to NHSmail was set up as a response to the coronavirus crisis – replacing the previous NAS process. Quick access to NHSmail enables each provider to have a shared mailbox and two individual user accounts if they complete a form that is available to download from Digital Social Care. Digital Social Care is currently operating a helpline to support the adult social care sector with harnessing technology during the coronavirus crisis, including support to set-up and use NHSmail.

The following comments (and Appendix Five) apply to the NAS registration portal process pre-pandemic. We were not able to test the effectiveness of the self-management process or NAS bulk upload facility. A generic shared site account - and up to 10 linked individual accounts - could be opened through the NAS portal for each site that provides social care if that site (or its linked Headquarters) has completed the DSPT to Entry Level or higher – although there are no technical controls to ensure that only sites that have achieved Entry Level or higher can open an NHSmail account. There is a Guide on how to complete the NHSmail social care registration portal available from the NHSmail portal as well as some guidance at Digital Social Care here. The guide lacks the detailed information needed to enable care providers to easily open their own accounts and no videos are available explaining how to do it. There are no training materials (e.g. slides) available to use in workshops or other sessions supporting providers to open accounts. It is very difficult for local project managers to produce them without access to test accounts to produce screenshots.

Although 95% of providers that attended the WMCA Entry Level workshops completed the DSPT to Entry Level or higher only 65% successfully opened their NHSmail accounts and this was despite considerable time spent trying as well as dedicated help and follow up support. Anecdotally, we understand that the national conversion rate of

social care providers who have published at Entry Level and have then opened NHSmail accounts through the NAS is low. It would be interesting to obtain these figures.

The WMCA experience was that the NAS verification procedure was not fit for purpose and throws up barriers for social care providers to be able to register for NHSmail. To open the shared site account, providers need the site postcode where they are registered, their CQC location ID (which is on their registration certificate) and the CQC Contact ID. Despite providers having this information, less than half were successfully able to register during the workshops. To compound this, providers are only able to attempt to register three times before the portal locks them out (and they cannot continue at a later date unless their account is reset by the NAS administrator). Other problems were caused by the unclear time constraint and requirement for personal communication details to be provided for all staff registering for individual NHSmail accounts, which happens at the same time as opening the shared site account, and the login instructions received. These issues were experienced consistently across all the WMCA workshops and are listed below and explained in more detail in Appendix Five. The latter three issues are still relevant to the fast track roll out of NHSmail:

- Provider not being identified on the system from postcode
- CQC location ID not accepted
- CQC Contact ID not known or accepted
- Individuals' personal data
- Login instructions received in initial email from the system
- No local mailbox admin function

Because of the first three issues WMCA partially circumvented the NAS verification process for their latter workshops by applying, one week in advance of the workshops, for one-time passcodes to be sent by post to all services who had signed up to attend (and notified providers to look out for these letters and bring them with them).

These issues, initially identified by WMCA, were confirmed by all the other local projects that supported providers to complete the toolkit and access NHSmail. For example, Barnet did not originally plan to cover NHSmail application in their Entry Level workshops, but signposted providers to the NHSmail portal to register through the NAS. However, they found that few providers then went on the register for NHSmail and in later workshops registering for NHSmail was included in the session and those who had previously published to Entry Level were invited back to the workshops to sign up for NHSmail. This improved the success rate with registration, but providers still struggled to use NHSmail e.g. to be able to send an email from their generic shared site account rather than their individual email address or add their NHSmail account to Microsoft Outlook. Without support at this early stage many providers do not go on to use their NHSmail accounts even if they do successfully register. NHSmail support was outside the scope of this programme and some of the training and support providers did not have access to an (actual or test) NHSmail account. Ideally, these sessions would demonstrate how to use the portal and Outlook, changing the password, updating providers' profile, and what to do when employees with an NHSmail account leave your employ or new employees start, as well as other benefits of an NHSmail account like the NHS directory, and access to Skype plus or MS Teams.

We recommend that, if sign up to and use of NHSmail is wanted, then support for care providers to register and start to use their NHSmail account is continued (through the Digital Social Care helpline for instance) and/or included in future DSPT training and support programmes.

There is a low level of knowledge in the sector about the need for secure email and the options available for social care providers to obtain it. In particular there is a lack of knowledge as to why NHSmail is important and needed and confusion with existing secure email systems required by local authorities such as Egress. We recommend that further promotion of the benefits of secure email for social care providers is undertaken including the need for it, how to obtain it, advice on how to check if your system is secure and/or examples of common systems that are not secure. This should include alternative support for social care providers to obtain secure email if wide roll out of NHSmail is not continued.

In Staffordshire, in a deviation from the original project plan due to the impending deadline for removal of faxes and the urgent need to scale up the solution, the project trialled the secure NHS cloud-based integrated Office 365 email platform as an alternative to NHSmail. This email platform allows one cloud-based (web browser) account to be set up per care organisation, which will communicate securely with NHSmail. This may be an alternative to using the NAS registration process. If so, there are three points to consider:

- The Office 365 cloud-based email account can be set up without providers needing to publish the toolkit to Entry Level. Organisations wishing to use the downloadable version must complete and publish the DSPT to ensure compliance with an appropriate level of cyber security. Wide scale availability of the cloud-based account could further weaken the incentive for providers to complete the toolkit.
- The Office 365 email platform would not give social care providers an NHSmail email address per se and would use either a standard or bespoke email naming convention, which would be approved by NHS Digital e.g. ….@staffscareprovider.nhs.uk or similar. One consequence of this that local NHS providers may not recognise that this is an nhs.net compatible email. One of the advantages of the NAS route is that care providers are perceived as being 'in the NHS tent' as they have a NHSmail email address.
- Accounts are not free to social care providers (unlike the NAS). We understand that one licence per organisation was purchased for participating providers in Staffordshire from programme funds.

3.1.5 Effectiveness of toolkit training and support

Six projects tested a mixture of support methods and provider engagement for both Entry Level and/or Standards Met. The impacts of these projects are summarised in the table below:

Local project	No. of providers invited to participate	No. of providers agreeing to participate	No. achieving Entry level	No. achieving Standards Met level	Support cost per provider
Barnet	159	139	104	1	£178 for EL £500 for SM
Bedfordshire		43	22	16	
Durham	N/A	12	N/A	11	
Shropshire	228	15	2	4	£491 for EL
Staffordshire	471	13	6	7	£1,012 plus VAT
WMCA	1324	244*	150	14	£547 for EL £1785 for SM

*This figure is the total number of providers who registered to attend a WMCA workshop, however, of that 244, 81 either cancelled at the last minute or didn't show up and hence 163 providers participated

Local project managers reported that there is a notable lack of knowledge amongst providers about the DSPT and NHSmail and the reasons why they should have it (unless significant engagement activity had already been undertaken). DSPT was a "*hard sell*". It is perceived as complicated to register and time consuming to complete, if providers are aware of it at all, and the benefits for care providers of completing it (or in having NHSmail) have not been communicated well. The WMCA, for instance, contacted over 1,300 providers to offer support with toolkit completion with only 244 taking up the offer and 163 attending workshops (a dropout rate of 33%).

It was reported by local project managers that the incentive for providers to complete the DSPT was undermined by the number of NHSmail accounts that had been set up for providers by CCGs or CSUs without them completing the DSPT to Entry Level (through the local registration process rather than the NAS). We speculated whether the local registration process had been used on a wide scale as a workaround to enable social care providers to access NHSmail because registration though NAS was so difficult. There were also issues in many areas that local take up of DSPT and/or NHSmail was undermined by other organisations, such as GPs, not being prepared to use NHSmail accounts to communicate with care providers.

The issue of incentive is critical. Local projects used the 'carrot' of being able to access NHSmail to persuade providers to complete DSPT to Entry Level. We found the NHSmail sign up process difficult, and many providers struggled to register and use NHSmail. This is doubly worrying as 'axe the fax' approaches and some CCGs are making having NHSmail a prerequisite of contracting with care providers. Longer-term, and in a wide scale roll out, access to NHSmail therefore is not a good incentive for providers to undertake the toolkit unless NHSmail registration functionality and guidance materials are improved. Without the link to NHSmail, the value of having an Entry Level is debatable as Entry Level assertions do not cover cyber security. Some local projects argue that Entry Level dissuades providers from completing Standards Met, but if Entry Level is removed then fewer social care providers are likely to undertake the toolkit.

The benefits of completing the toolkit will not be realised unless providers publish at Standards Met. This is partly because Entry Level does not cover cyber security, but also because of the need for providers to thoroughly understand the requirements and check how these are being implemented in their organisations. Local project managers reported that some providers had discovered that their organisation had previously completed the DSPT (or previous IG Toolkit) but that there was no corporate knowledge of the answers. There is a danger that an individual will complete the toolkit as a stand-alone project or tick-box exercise without data and cyber security good practice being implemented throughout the organisation.

For wider scale roll out, it will be important to sell the benefits of completing the toolkit, i.e. assurance that you are data and cyber security compliant as well as a gateway to other digital tools, and, crucially, that councils and CCGs are bought into the toolkit being the single mechanism for use by adult social care providers to give assurance of their data and cyber security. CQC have recently promoted the DSPT in their monthly newsletter so further promotion of this and the ability to support and review both digital practices and DSPT completion at inspection would enhance uptake in both areas. There is still a variety of data and cyber security contractual or tendering requirements asked of service providers, and little support available from commissioners, which gives the programme few levers to encourage toolkit take up. A key step for the programme will be awareness raising with councils and CCGs and CQC.

In addition, for wider scale roll out, we believe that there is a risk of a bottleneck in the supply of organisations that can provide expert DSPT input, particularly those that can deliver training. Currently, the toolkit is not intuitive and issues with its functionality and terminology (see sections 3.1.2 and 3.1.3 above) mean that it needs interpreting for care provider organisations. There are a limited number of support organisations that have detailed knowledge of the DSPT and, to ensure sustainability, it is important to embed that knowledge at a local level and/or overhaul and simplify the toolkit.

A key finding was that having a variety of engagement and support methods maximised both the participation of care providers and success rates. Some providers are able to complete the toolkit after being signposted to the Digital Social Care support materials, and others need just a bit of support to understand what the assertion is asking (see section 3.1.3 about the language and jargon used in the toolkit). A DSPT champion for local areas is recommended as a cost-effective solution for these providers. Other providers benefited from more intensive support such as workshops and one to one support via telephone/email or face to face visits. For these methods to work, considerable effort was needed by local organisations – frequent phone calls as well as emails - to maximise attendance/minimise dropout and get the right people to consistently attend and complete the necessary preparation activities. The key lessons learnt from local projects delivering DSPT support are summarised as:

- We estimate that 5 – 10% of small care providers are not ICO registered. Local or regional support programmes should include checking ICO registration.
- One size doesn't fit all – have a range of support and activities available. We recommend a mixture of signposting, awareness raising and training plus having a DSPT champion. A DSPT champion understands the requirements of the toolkit and can provide ad hoc support and answer questions such as through a 'live chat' facility or by appointment.

- There are a significant number of providers who struggle with even basic IT, support needs to address this as part of any approach to wider scale DSPT roll out.
- Joint support and a shared vision for data and cyber security from local organisations is more powerful than one-off expert input from other organisations. Good relationships with local providers is needed to sell the benefits of the toolkit and encourage continued participation.
- Toolkit registration is complicated and the assertions cover a range of areas. Awareness raising sessions that help local providers understand their registration options and who, within their organisations, need to be involved are recommended. Providing ODS codes and ICO registration numbers kick starts the process.
- Involve the right people from each provider. Busy managers or owners are likely to delegate workshop attendance to admin staff or others who may not have the knowledge or oversight needed to ensure compliance.
- Access to the DSPT test site helps trainers or DSPT champions/support people to be familiar with the toolkit and can demonstrate it. The test site should have an HQ view available as well as the Entry Level V**** code site view.
- Facilitated peer support, complemented by virtual communication tools such as Microsoft Teams, can be a good method of encouraging toolkit completion.
- Offer care providers protected time to complete the toolkit, away from the distraction of a busy service, and with access to technology to work on it 'live'. This format, extensively trialled by WMCA, is suited to providers who are already comfortable with GDPR policies and – through extensive preparatory support - are happy that they are reasonably compliant.
- Breaking down the work - with homework/action planning between sessions – over a period of time will reduce the risk of it becoming a tick box exercise that participants complete in one session without understanding the assertions or embedding good practice in their organisations. Time is needed for providers to thoroughly understand the requirements and iteratively check how these are being implemented in their organisations.
- If promoting NHSmail, offer support to sign up to and start using NHSmail at same time as completing the toolkit.
- Digital Social Care, and the very helpful materials available there, are not well known in the sector: further national promotion and local signposting is important as providers are unlikely to find them of their own accord. These DSPT support materials were extensively used by local projects. A variety of new training and support materials, to complement what is already available, was developed and tested as part of the programme.

3.2 The safer use of smart phones and other mobile devices

Local projects developed guidance, policies, tools and templates to support the use of mobile devices by care providers. These projects are summarised below:

- **Manor Community** developed a guide to help providers decide between purchasing mobile devices or asking staff to bring their own device, including potential costs of purchase.
- **North Yorkshire Council** developed a guide for how to implement either a bring your own device (BYOD) or a purchase model. As part of this, the development of a costed service offer to provide mobile device management (MDM); this service to

include forcing software updates onto devices and extra security including location tracking and a facility which wipes a phone if it is lost or stolen.

- **Peterborough and Cambridgeshire Care Association** (PCCA) developed policy for use of mobile devices by care workers. PCCA also developed a template for a contract of employment section covering use of mobile devices by care workers.

The guide to help providers make the choice between 'bring' or 'buy' is aimed at those who may be very new to smartphones and cyber security. Similar to a 'Which?' guide and developed collaboratively with small and medium sized care providers, the content takes the reader through the key concerns and technical details of safely installing any device into care services. It looks at three main levels of use: using devices for simple communication; using devices to access paperless intranet systems and finally; smartphones for full care processes and senior management. Providers should consider how to balance value for money with security of data. At 'lower levels' of use it is easier to safeguard information (with less control over the devices) but as you move towards more extensive use of devices it is more difficult to ensure safety without paying for fully managed and protected company phones. Whilst the care planning/rostering software may itself be secure (due diligence will be key here), this may not be the only source of confidential information on a phone and so security for the whole device will be needed.

There is a school of thought that, as providers in general can sustain investment in company phones, BYOD therefore is not worth the risk. However, in practice this is rarely a binary choice: almost all organisations will have some people using their own phones for work purposes, plus typically there are at least one or two company phones, so inevitably there will be a mix. Therefore, we advise all providers to think about the implications of bring your own device.

North Yorkshire's work on mobile device management solutions (MDMs) has shown that this is a good practice approach for providers who are buying more than two or three phones. For most organisations a web-based service that is run and maintained by the vendor will be the best approach. North Yorkshire Council provides such a service locally for example, and in their product 'An Introduction to Mobile Device Management' set out considerations for providers when looking into this. Even with a commissioned service, there may be technical challenges. For example, not everyone is aware that the phone operating system is vital for MDM – all phones need to have the same system – and that the infrastructure for MDM (e.g. adequate wifi) is not always in place.

Of the providers receiving a small grant, five focussed on mobile phones. One provider found that trying to operate their own MDM system was too onerous for them, and it may be too complex for small providers to run this sort of system themselves. The others managed it more effectively, although one in the end only added anti-virus software to their existing devices. One provider implemented new software that required all their 500 plus phone users to use passwords and to have encryption on their phones. Another established a comprehensive MDM system (Microsoft Intuit) that they were confident was going to allow greater control of their mobile devices and greater security (through limiting the apps that can be used, enabling remote wiping of lost devices and allowing a 'one touch' setup for new devices). The fifth provider placed (unspecified) MDM software on all their mobile devices and identified that this had allowed them to safely add a further suite of applications for use by staff and increase the security of devices by: enforcing password policies; group policies that restrict access to specified

areas of the device; and remote control of devices if needed. Key learning for implementing either buying or bringing approaches for phones include:

- The need to engage all staff from the start. As with any new technology much of the implementation task is about securing staff sign up. Piloting approaches is essential but wider engagement is needed to ensure take up is successful.
- Staff will need ongoing encouragement (and monitoring) – implementation is not a one-off training exercise and staff can be under confident; reminders such as to update phone software (if no MDM in place) will be important.
- Having a champion at frontline worker level is helpful and good practice.
- Even at 'intranet-level' (e.g. sharing view-only policies) phone use encourages the use of technology and paperless approaches.
- The importance of engaging the people who use your services. Clients will need reassuring that staff are not tapping away on their phones for personal use, and that the absence of an official-looking paper file is not a cause for concern.
- The importance of sharing experiences with other providers in order to promote best practice, in particular through peer groups such as care associations.

Peterborough and Cambridgeshire Care Association, in developing clauses for employment contracts and policies for frontline care workers using ICO guidance as a basis, found the following challenges:

- That photographs are a key concern when thinking about policy: easy to create, the storage, sharing and deletion of images then needs to be considered.
- Once policy and contracts have been developed, how best to get staff to comply, and that accessible social care-specific training is a key gap. And should a member of staff break the clause in their contract, this should be classed as a disciplinary offence i.e. that there can be serious consequences.
- Companies who sell care policies to providers have not yet all recognised the need for policies to cover this area. This represents a further risk to the sector in using mobile devices securely.

Use of company phones is a relatively new and developing area in the sector. BYOD, whilst an approach used extensively, currently remains a key area of concern as many providers remain unaware of the risks of staff using their own devices.

3.3 Staff training and awareness

Five local projects focused on staff training and awareness around data and cyber security and a number of the organisations receiving small grants also had projects that focused upon staff development or included it as part of their activity. The local area projects are summarised below:

- **East Midlands Care Limited** (EMCARE) aimed to explore, test and evaluate staff training and awareness around cyber security in care homes to establish relevance, accessibility and affordability of methods used. They also wanted to develop materials to assist in the identification and analysis of cyber security training needs and to identify strengths and weaknesses in local approaches and to seek to improve these where possible.

- **Nottingham City Council** investigated existing cyber-security knowledge of local providers and identified short comings to enable them to author a bespoke cyber-security training course based on the findings. They also carried out further site visits to assist with implementation of new learning, to deliver cyber-security training and assist with DSP Toolkit completion.
- **Blackburn with Darwen Council** explored the most effective way for the council to support providers in the area of cyber security. It produced training materials specifically for care providers, and it developed an offer of hands on support and advice which care providers could access in the future.
- **Care England** evaluated the best methods to educate people on their responsibility to help protect the confidentiality, availability and integrity of the information of a personal and sensitive nature held by the organisation and to stress that information security is everyone's responsibility, not just the IT department. They also evaluated the effectiveness of a standardised training course carried out in each organisation through targeted and monitored phishing attacks.
- **Care England** also worked specifically with providers of learning disability services to identify the training gaps in registered services and implement training plans in each.

Several issues and themes emerged from the staff development projects. There is variable awareness of cyber security and limited understanding of the benefits of ongoing training and awareness raising or completing the DSPT. Each of the projects experienced providers dropping out after initially signing up for the project. This perhaps reflects the position of data and cyber security as an area seen as important by many providers but is overtaken by other more pressing operational issues. It also may reflect the tight timescales for the programme and the additional pressures experienced by providers over the winter and Christmas period.

The projects explored different ways of identifying the training needs of provider organisations and the best means of meeting them. All the projects met with providers to identify their training needs and the Care England projects utilised a proprietary survey and questionnaire to do so. Nottingham City also utilised an on-line survey and EMCARE deployed the Skills for Care digital readiness tool in their meetings with providers.

After identifying training needs, most projects then delivered training to providers and sought to evaluate the impact of it. Care England drew upon a training provider for their material whilst Nottingham and Blackburn with Darwen developed their own materials. However, EMCARE researched, identified and tried out free guidance, support, products and training available and held a workshop with providers to test and evaluate those of most relevance, effectiveness and appropriateness.

The Care England project sought to evaluate their training by carrying out phishing attacks on a sample of staff from each provider, including those who had done the training. The results showed that 39% of untrained staff who were sent a phishing email opened it and clicked on it so were in effect ‘caught’ by the simulated phishing attack. Staff who had received the training were less likely to respond unsafely to the phishing email. Further points arising out of the training undertaken were:

- Generally, it was found that staff often have a short attention for training in this area and that shorter more concise materials worked better.
- There is a vast range of 'help' available on the internet, but no means of differentiating the good from the bad. There is an appetite for a singular product in the marketplace that answers all cyber-threat questions clearly and concisely.
- The eLearning for healthcare Data Security Awareness programme is difficult to access by social care providers and the instructions need updating.
- A good portion of 'generic' cyber security training used terminology which wasn't suited to the target audience.
- Training can be difficult for staff who have English as a second language.
- Those who are responsible for cyber security, such as managers, have different training needs over and above those of other staff.
- Provider staff often use a range of devices, sometimes in a very ad hoc fashion.
- Staff were expected to operate safely, but sometimes with old kit and programmes.
- Often, care providers do not make best use of available resources. Safety features in Microsoft 365 are under used and there is a requirement for dedicated training on the benefits and advantages of using cloud-based systems such as Microsoft 365.
- Providers do not know what they do not know, leading to a lack of knowledge regarding areas of risk.
- The effectiveness of training can be tested through staff and organisational feedback, but there may also be benefit from 'site testing' such as simulated phishing attacks.

It is also worth noting that VODG and AMHP (see section 3.5) said that several providers reported difficulties in delivering training to staff who have infrequent contact with head office. A significant majority of staff in the sector do not have regular access to company devices, do not work out of offices and rarely use IT, especially in supported living services.

Overall, the findings were that providers do need some guidance on how to make systems safe as well as how to identify the training needs of their staff. Whilst there is a wide range of training materials available for use, some free and some at a cost, there is nothing specifically targeted at the social care sector. The specific training modules developed through this part of the programme will be especially helpful to social care providers. Effective testing of the impact of training is also a key component and there is a need for greater awareness in relation to phishing attacks throughout the sector.

3.4 Adopting new technology

Local projects supported some care providers to test specific digital innovations and, through completion of a Data Protection Impact Assessment (DPIA), to prepare to adopt new processes or use more digital solutions. These projects are summarised below:

- **Dorset Partners in Care** used the Skills for Care digital readiness tool to identify barriers to developing digital maturity for providers who have little or no prior knowledge of digital applications. One of the unexpected successes of this project was having a slight mixture of digital maturity amongst the reference group. By having a small number of providers who were just a 'step ahead', allowed those who were just beginning to see how digital technology could be implemented and

used successfully within their setting. The reference group sparked peer support and learning with reciprocal visits being made between providers which allowed some participants to fully utilise digital technology they already had within their service but was not being used to its full capacity due to both a lack of knowledge and hesitancy in relying on digital. Similarly, the opportunity to utilise existing networks such as Registered Managers Networks and Care Associations to encourage buddying/mentoring relationships worked well for providers to learn from one another.

- **Hampshire Care Association** (HCA) used the Information Commissioner's Office DPIA template to support 12 care homes complete a DPIA in readiness for the safe implementation of a new care home telehealth support service commissioned by the West Hampshire CCG. This followed supporting the 12 care homes to achieve DSPT Standards Met and leading four provider events across West Hampshire attended by 35 care providers and the CCG to promote the telehealth support service and explain the readiness requirements.
- The **North Tyneside Council** (NTC) project focused on the use of assistive technologies and considered the replacement of medication visits with digital solutions i.e. the use of medication dispensing equipment and remote monitoring cameras in the citizen's home. Through the design and completion of a specific camera based DPIA template NTC explored questions such as who owns the data collected by assistive technologies; how is it stored and shared; how service users can be assured that their data is safe; and how the answers to these may vary between different technical solutions.
- **Stonewater** and First City Nursing explored the risks, issues and benefits of gaining evidence of consent using digital tools (rather than by hard copy signature) within social care, housing and voluntary sector organisations working within Swindon. They carried out research into digital consent solutions, including analysis of the regulatory requirements relating to digital signatures, the accessibility and functionality of products currently available within the marketplace. Participating providers tested a range of possible digital solutions.
- **Wiltshire Care Partnership** tested the secure use in care services of the Amazon Echo voice-activated home speaker powered by Alexa software. They identified potential benefits and challenges in the use of the technology and the information flows involved and developed guidance for implementation and use as well as a specification for the work to establish a comprehensive ethical and legal framework suitable for such technology's wider use.

Care providers would benefit from more criteria and guidance on the selection of software. This could range from a small provider selecting their computer operating system(s), office productivity software and back-office systems (such as HR, payroll and accounts), to organisations selecting rostering systems and frontline care systems. The Partners in Care reference group reported that basic knowledge was often assumed and therefore omitted from user guides which left them feeling further removed from digital developments. Partners in Care developed a series of basic guides to address gaps in knowledge, for instance 'What is the cloud?'

It was noted that the learning, products, tools and resources that come out of this programme need to be produced and made available in bite-sized and logical sets so the most appropriate resource can be readily identified and used. Otherwise there is the danger of care providers being overloaded and confused by the resources.

Workforce considerations are very significant and not to be underestimated. Providers cited 'seasoned workforce' as a barrier to embracing technology (it is worth noting that they do not want to lose these staff as they are reliable and do an excellent job) as they are nervous around technology and require support to confidently embrace this - more training than had been anticipated. Embedding 'workplace digital champions' within organisations could be a good way to ensure providers embrace the challenges of a digital age. A feasible way to achieve learning at scale is to use a 'champion' approach to embed and cascade skills which has the added benefit of bringing your staff group with you and providing a possible solution to resistance of adopting technology.

Linked to the above, the general culture change work that needs to be undertaken with staff is also not to be underestimated. In addition to the adoption of technology there are apprehensions of the impact on the individual's role. Culture change with the people who use services was also underestimated on some projects, with people not embracing the technology as readily as had been assumed, even if they were enthusiastic when the opportunity to trial the technology was initially discussed. Vulnerable people and their families can be suspicious of digital records of them and so assurance of the security of this data and for what it will be used and by whom need to be clearly communicated.

Wiltshire Care Partnership concluded that, although they can be very beneficial, digital assistant devices were not always suitable for everyone receiving care, they need to be used selectively with people who are keen and interested in using the technology and where there are potential benefits to them. Safe use requires responsive staff who are able to notice any changes in the mood or behaviour of individuals. In residential care where the devices are all on the same premises they recommend that the devices are all registered to the providers Amazon account and that voice purchasing is disabled. In domiciliary care and supported living they recommend that the devices are registered to the individual's Amazon account and that the provider has a conversation with the individual and/or their family about the benefits or otherwise of voice activated purchasing.

Partners in Care organised a Grow Digital conference that featured a workshop on cyber security from Dorset Police Cyber Crime Unit that received excellent feedback from delegates. The police are seen as a trusted, independent source of information. It is likely that there are similar units in all police forces and national or regional approaches to the police could be made and local connections utilised for adoption by other areas in future programmes or wider roll out.

The various public bodies/agencies (e.g. local authorities, CCGs, NHS Trusts, GPs) are all at different levels of digital maturity and leadership themselves, both in the local partner context and across the nation. This results in different vision, leadership, expectations and views on priorities between the parties, which in turn is difficult for care providers to respond to.

VODG and AMHP (see section 3.5) reported that respondents to their survey with social care services for working age adults identified a wide range of barriers to greater use of IT in their organisations. These can be broadly grouped under the headings of:

- Skills: staff, culture, IT team.

- Money: hardware, software, implementation.
- Accessibility: connectivity, disparate systems, data security.
- Time for: policy development, organisational change, testing and embedding.

The skills of front-line staff, basic familiarity with computers and computer safety and confidence were the most frequent barriers and some respondents observed the problem of staff turnover creating a recurring problem. Cultural issues were more about a reluctance or lack of confidence among front line staff to engage with IT than active resistance. There was also mention of a shortage of specialist posts and specialist applicants and a lack of expertise in procuring IT systems. Funding issues referred to the cost of IT systems and hardware and training. Barriers around access to hardware were principally around the sufficiency of hardware and the problems of interfacing between systems for different parts of the business, disparate requirements of commissioners and other agencies or regulators and the challenge of internet connectivity and speed, especially in rural areas.

Local projects commented that centrally driven digital initiatives such as this tend to assume robust internet access is had by all. However, one of the challenges for projects involving rural areas is lack of broadband/ 3 or 4G coverage, speed of the connections, basic mobile phone coverage, and that many older citizens do not have broadband connections in their home. Therefore, central programmes need to take due consideration of this and maybe even support some projects that seek to address this.

3.4.1 Gaining digital consent

Stonewater reported that providers involved in the digital consent project incur large costs associated with the printing of documents required for the delivery of safe and effective services. First City Nursing identified that they spend approximately £60,000 on printing and paper per annum. Furthermore, there is considerable time and expense required to obtain consent in a traditional format. Whilst initial investment costs would need to be considered, the opportunities associated with reducing the use of paper across the social and housing sectors are significant. However, there were barriers to using digital consent. It was identified that many of the people whom participating organisations support do not have the technical capabilities or, in many cases, internet access to give consent via digital communications. Where possible, some provision must be made to mitigate this. In addition, the providers themselves did not always have the hardware to store digital documents. Providers identified a number of areas where barriers were not so prevalent: recruitment, staff development, and contracts.

One of the participating organisations experienced a unique challenge. They provide support for people who have or are experiencing domestic abuse. This organisation did not want any trace of the digital consent stored on the individual's personal mobile device. Many of the solutions save a copy for both parties and while this is a benefit in most instances this posed a potential risk to the people who use such a service. Although there was option of the organisation instructing their clients to delete all correspondence and clear browsing history, this was deemed too high risk to proceed.

Information governance and security also presented challenges throughout the digital consent project with questions raised relating to where personal data obtained via the digital solutions was stored. Increasingly commissioners require data stored within EU or UK based servers. Many of the solutions identified utilise AWS and office 365 servers some of which use US servers to store personal data. To overcome this, providers

developed processes whereby personal data was uploaded directly to company servers and deleted from the digital consent solutions.

Stonewater recommended that any scaling up of digital consent solutions should be considered at a system level as compatibility and information governance across various systems can prevent challenges. Scaling up a digital consent project could involve encouraging collaborative purchasing for digital consent solutions to achieve standardisation and best value. For instance, by procuring a single electronic consent platform that all partners delivering care on behalf of a council are able to buy into.

3.4.2 Data protection impact assessments (DPIA)

The Hampshire Care Association digital champion developed a comprehensive resource pack which includes an NHSmail presentation and templates and guidance for: information asset register; DPIA template and screening tool; Privacy Notice; FAQs including sustainability guidance; and IT screening tool. The IT screening tool allowed care and nursing home IT equipment, cyber security, internet bandwidth/speed and wifi connectivity around the building to be considered at a basic level to ensure video conferencing would be possible, effective and safe. A further valuable product of the project is an example DPIA for video conferencing with care home residents that can be made available for use by other care providers.

North Tyneside Council worked in partnership with Age UK, who had already published the DSPT to Standards Met, to recruit and support a group of extra care and domiciliary care providers (whose visits would be replaced but who needed to support the citizens in understanding the medication dispensing and monitoring) to gain at least DSPT Entry Level and involve them in the piloting of the digital solution and the associated DPIAs. In parallel, NTC worked with its in-house telecare team (who installed the technology and undertook the remote monitoring) and the council's experts on the use of CCTV and associated surveillance legislation to develop and undertake a relevant DPIA for each of the two different camera technologies piloted: live stream camera based technology through Alexa Show and the Ring camera which uploads recordings to a server.

These pilots took place with the extra care providers which also allowed exploration of whether there are any particular data and cyber security issues linked to the interaction between housing and care providers. However, despite several of the domiciliary care providers gaining DSPT Entry Level none chose to be involved in the pilots. This appeared to be related to the potential for their service (chargeable carer visits) being replaced by a remote monitoring service provided by the council and therefore a loss of revenue for them. In this context, the DPIA was also that of the council's telecare service and not the domiciliary care provider and so the domiciliary care providers saw no ownership of the DPIA process and output. Though the technology provider and user does need to ensure anyone working in the home (i.e. domiciliary or extra care provider) has been made aware of the technology and issue a privacy notice, NTC commissioners believe they need to undertake more market shaping and explore links to outcomes-based commissioning to generate more engagement with domiciliary care providers. The extra care providers participated from both a proactive engagement in understanding the benefits of assistive technology perspective and from appreciating that it had the potential to improve the productivity and focus of their care staff at the extra care locations. NTC also noted the need to ensure relevant data sharing agreement are in place between participating providers in an extra care setting e.g. between housing providers and care providers.

The NTC project has developed a draft resource pack for 'Introducing Digital Camera Based Technology', which includes a toolkit for care managers and assistive technology care services to use to work through when introducing digital technology into someone's home and an example DPIA for considering digital technology for medication management. NTC feel that in the near term the main adopters of this technology, and therefore users of the resource pack, are likely to be telecare services and not care providers, depending how particular markets are commissioned.

The NTC pilots and DPIA work identified that the live stream camera-based technology, such as Alexa Show, is much less intrusive than technology that uploads recordings to a server, such as Ring cameras. They therefore propose that live stream camera-based technology is the default technology, with recording-based technology reserved for when the specific requirements and circumstances demand it. NTC also identified that people on direct payments are likely to realise the benefits of this type of technology for communicating with their PAs and as they, as individuals, are not subject to GDPR it will be very flexible. Consequently, there is the opportunity to develop support tools to help citizens and their families ensure they adopt this technology in a safe way.

Both DPIA related projects have produced completed DPIAs that can act as good practice examples for other organisations considering the same or similar circumstances. These should be added to the resources available on the DCS website, and we note that the DCS website has the potential to act as a repository of further example DPIAs and for sharing these across the sector. The projects have also produced guidance for care providers in undertaking a DPIA which can accompany the example DPIAs.

The example DPIAs and associated guidance will be valuable resources as there is low awareness of the need to undertake a DPIA in the sector, and therefore low use of them, where digital solutions are intended to be applied and will capture and store personal and sensitive information.

Both DPIA projects identified that suitable internet connectivity and appropriate IT and cyber security arrangement could not be assumed and had to be reviewed as part of the project, as these issues were not fully covered by either DSPT or the DPIA. The projects also demonstrated some contrasting points. Hampshire with an established care association was able to engage and mobilise care providers. Conversely, in North Tyneside where there is not an equivalent care association that effectively represents the domiciliary care providers the engagement with the care providers proved more problematic. In Hampshire the care provider was clearly the party that needed to undertake the DPIA whereas in North Tyneside the care provider needed to be aware of the technology, support and assure citizens in its use, and its staff be provided with a privacy notice, but it was the telecare service as the actual provider and user of the digital solution who needed to undertake the DPIA.

3.5 Implementing safe data and cyber security practices

Some local projects undertook a variety of activities to test how data and cyber security has been implemented in practice and how it could be improved. These projects are summarised below:

- **Lincolnshire Care Association** explored sustainable, affordable external IT support and advice for care providers, including the potential for a viable support contract with the CSU. They organised a conference with a cyber security support organisation.
- **National Care Forum** (NCF) worked with care providers who had already completed the toolkit to Entry Level or Standards Met to understand whether or how the providers' approaches to cyber security have been influenced through toolkit completion; what they learnt from the process and whether it had made the organisation more resilient.
- **Nottinghamshire County Council** undertook system resilience testing with providers to help them plan for system failure and test contingency arrangements and backup plans. They devised some social care-specific scenarios to mimic disasters and cyber-attacks.
- **Voluntary Organisations Disability Group** (VODG) and the **Association of Mental Health Providers** (AMHP) worked with providers of social care services for working age adults to ascertain the preparedness, issues and obstacles they faced in relation to data and cyber security and to raise the profile of the DSPT. They undertook an online survey with members supported by individual and group discussions.

VODG and AMHP reported a low response rate (20% or 33 responses) from their members to the survey, lower than usual for similar activity, which reinforced the experience of other local projects that this is a difficult area to engage the sector with. Half of these respondents had not published the toolkit at any level. Larger organisations were more likely to have engaged with the DSPT and mental health organisations were less likely to have registered than learning disability organisations. This appears to be a consequence of the nature of their activity i.e. where an organisation is more engaged with the NHS they are more likely to be registered whilst housing organisations or those with substantial other charitable or non-regulated services were less likely to see the DSPT as relevant. For instance, one provider was concerned that Ofsted propose to make ISO27001 a requirement for specialist educational colleges. Completion of the toolkit was seen as particularly challenging in organisations whose work crossed geographical and regulatory boundaries (Wales, NI, children's services, housing etc.). As such it may be seen as more of a burden for voluntary sector organisations who will be involved in directly commissioned and regulated activity as well as delivering wider community services. The main driver for DSPT engagement is when it is a contractual requirement. The experience of a cyber-attack, especially in smaller organisations, has tended to lead such organisations to Cyber Essentials rather than the DSPT.

In terms of cyber security, the risks for providers of social care services for working age adults reflected the findings from the data and cyber security discovery programme in 2018/19, namely that many providers are reliant on paper records, some organisations have some devices using windows 7, and the secure use of smartphones was an issue as was access to and understanding of secure email. An additional finding is that third party systems, especially WhatsApp, are in widespread informal and sometimes formal use (even where prohibited). One provider had upgraded mobile phones because WhatsApp ceased to be available on Windows phones. These systems are attractive because digitally disengaged staff recognise and understand them. For the same reason, Workplace by Facebook had gathered some traction. The absence of integrated

systems and formal communication barriers was often filled by front line staff adopting unsafe but effective workarounds with such systems. We recommend that guidance is developed to advise organisations on their options for the safer use of WhatsApp and other similar, commonly used communication systems.

Nottinghamshire County Council wanted to test providers in 'real word scenarios' and developed three exercises that they conducted 'on-site' at participants' premises:

1. Power cut. A scenario of a lightning strike which disabled the care home's power and wi-fi: can the home get online to receive important information about a new resident?
2. Ransomware. A test of a provider's response to receiving a ransomware email.
3. Lost or stolen device. A scenario to test what systems were in place to safeguard the data on these machines - could they be traced or wiped remotely - including council staff posing as members of the press to ask staff on duty about this to see how they would cope under stress.

They reported considerable success in undertaking site visits to highlight the importance of business continuity planning and cyber security: "*doing it for real helps people think about the issues in a way that desk top exercises don't.*"

The three tests identified lapses in cyber security at provider services. In particular, participants clicked on the simulated malicious emails/links, even though they had signs of being malicious, because providers felt comfortable in doing so as they recognised the sender. This is a theme that is common in phishing and cyber fraud.

Local projects discovered that some care providers admitted to being the victims of cyber-attacks and/or ransomware attacks and some businesses have paid between £5,000 - £20,000 to get back online following ransomware attacks. In some cases they were unfortunately unsuccessful even after paying this ransom. We suspect that cybercrime is under reported and we know that care providers are unaware of who to or how to report this if it happens to them. We recommend that a handbook on how to recover from a cyber-attack is developed. The social care sector will not be immune to this threat and recommend more awareness raising specifically about what to do if you are attacked (linked to how to prevent one). Providers don't make the connection between cyber security and care: "it's unlikely to happen to me" mentality.

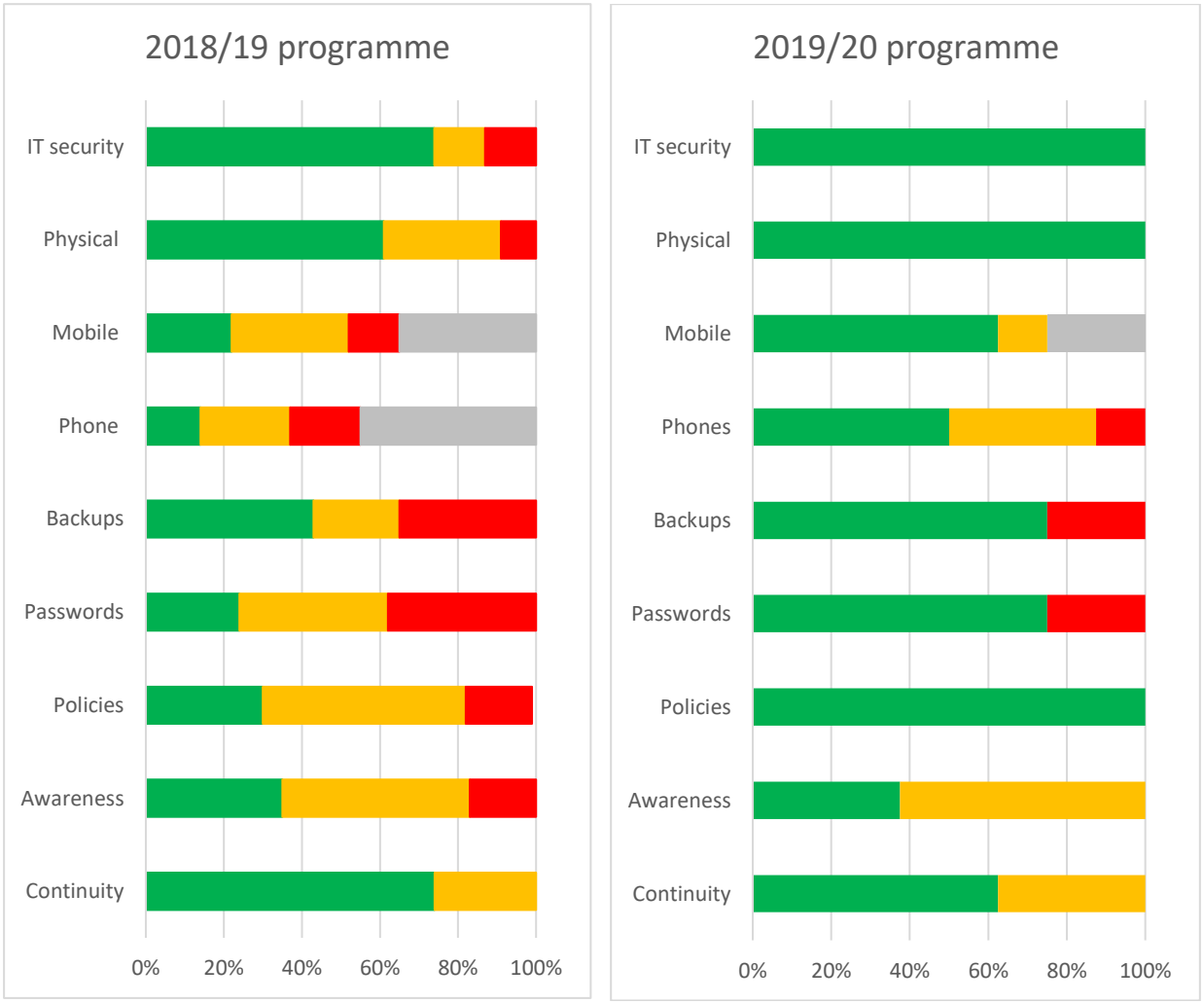
Similar to the experience of local projects trying to engage providers with the DSPT, the NCF struggled to get providers to engage with its links to cyber security. NCF reported that a significant number of providers had not heard of the toolkit and thus have little or no understanding of the potential benefit of completing it and, once completed, the DSPT can be seen as a static product that is 'shelved'. As such providers have struggled to make the connection that the contents of the DSPT actively influence how cyber security issues are/can be dealt with and it remains unclear how the DSPT tangibly influences cyber security practices for providers. In addition, a significant number of providers outsource their IT support to a third party and many assume such issues are by extension the responsibility of the IT supplier rather than their own.

Lincolnshire Care Association reported that the market for IT support for small care providers is not well developed, what exists is hard to find, and providers' collaborative

buying power has not been realised. In addition, providers are often required to sign up for several years when entering into a new agreement with support companies.

3.6 Data and cyber security risk assessment

Eight data and cyber security risk assessment visits were undertaken with providers that have published the DSPT to Standards Met. The percentage of services categorised as Red, Amber or Green (or not applicable) as a proportion of responses for each risk category for the eight participating providers in 2019/20 compared with 70 providers that had not completed the toolkit, i.e. from the 2018/19 programme visits, are illustrated below.



Details of our risk categorisation judgements for these eight care providers are given in Appendix Six. Six of these providers make use of NHSmail and the remaining two use encrypted email but don't use NHSmail. This was due to a combination of: contact with NHS still being paper based (letters to clients or hard copy prescriptions); secure communication with other parties such as local authorities being conducted through Egress and so not seeing a need for a further secure route; or difficulties with NHSmail registration.

It should be noted that this analysis is only for a limited number of care providers compared to those visited during the 2018/19 programme and care must be taken in

drawing firm conclusions from this part of the programme. Nevertheless it appears that there is a general improvement in data and cyber security risk levels for providers that have published the toolkit to Standards Met compared to those visited during the 2018/19 programme (who had not completed the toolkit) and particularly that: relevant policies are in place and understood; good physical security measures are in place; and basic IT security – firewalls, malware protection and patch management - is in place. All organisations visited had business continuity plans, but they considered data and information recovery to varying degrees. The greatest risks continue to be:

- Smartphone security - Some organisations continue to underestimate the issues related to staff using their own smartphones for work and the need to enforce a robust BYOD policy, and that this should apply equally to management as well as frontline care staff.
- Backups - Though there are still red risks in relation to some providers' data backup practices, those that were already green (before toolkit completion) have generally continued to improve their backup arrangements through greater use of cloud storage and implementation of cloud-based care systems.
- Logins and passwords - Some locations continue to have a shared password for certain computers used by care staff. These were care home locations where care plans and records are still purely paper-based.
- Staff training and awareness raising - Office staff have annual updates on data security and protection, frontline care staff updates appear to be more focused on client information confidentiality in the context of safeguarding, with less inclusion of cyber security aspects. Some care providers who use the data and cyber security related NHS e-learning modules commented that even though they use them for office staff the modules are less relevant for frontline social care staff.

There had been a range of progress across the eight participating care providers since publishing their DSPT submission. Some providers proactively updated operating systems (e.g. from Windows 7 to 10), implemented applications in support of frontline care delivery, and improved the security and resilience of data through transition to cloud-based solutions, whilst others with a low level of digital maturity made no further progress other than registering for NHSmail. The narrative from staff interviewed as part of the visit is that, where there is interest in digital maturity by the owner / senior leader of the organisation there is naturally leadership and investment in the issue, with the converse also applying where the owner / senior leader does not invest.

The knowledge of the DSPT requirements within an organisation varied from those where the Registered Manager, Quality Manager and others understood the requirement and how they were operationalised (usually the regional to larger organisations) to those where it was dependent upon an individual (usually regional to local organisations) and with limited permeation of operations. The latter situation obviously impacting upon the sustainability of the care providers' data security and protection endeavours. We continue to be concerned that toolkit completion is undertaken as a one-off or stand-alone exercise by an individual without sustainable implementation throughout the organisation. We recommend that Digital Social Care marketing and communications approaches are reviewed to ensure that they reach, engage and influence care provider owners and senior leaders.

4 Conclusions

The 2019/20 programme supported 24 local projects and gave grants to 57 care providers, supporting many organisations to complete the DSPT as well as producing a wealth of data and cyber security guidance, training materials and other products. IPC will review the materials produced, edit them if necessary, and make recommendations as to which should be made more widely available through the Digital Social Care website or other channels by July 2020. A key strength of the programme was the mix of organisations involved in the local projects - care providers, care associations, care provider representative bodies and councils – which allowed barriers and potential data and cyber security solutions to be explored from different perspectives.

A key conclusion of the programme is that the Data Security and Protection Toolkit continues to be a “hard sell” for regulated providers and is little known by other organisations in the sector. If the toolkit is to become the single mechanism for use by adult social care providers to self-assess their data and cyber security then the communication strategy, language and guidance needs to widen beyond care homes and domiciliary care organisations. Achieving uniformity across mechanisms and regulators would also help as organisations need portability or passporting through key elements of the DSPT when providers already have Cyber Essentials (not just Cyber Essential Plus) or other accreditations such as ISO27001.

The DSPT is widely seen as a regulatory burden rather than a springboard for better and safer use of digital opportunities and we continue to be concerned that toolkit completion is undertaken as a one-off or stand-alone exercise by an individual without sustainable implementation throughout the organisation. Worryingly, publication of the DSPT to Standards Met does not necessarily prompt social care providers to take comprehensive cyber security measures. It is striking, for instance, that there are no questions in the toolkit for social care providers about two of the areas of greatest risk identified in the 2018/19 programme report: backups and passwords. We recommend that a gap analysis is undertaken against Cyber Essentials and the risk assessment developed by IPC as part of this programme to highlight areas of cyber security that are not covered by the DSPT.

Barriers to the wide scale adoption of the toolkit include the registration process and complexity of the toolkit’s headquarters functionality, an NHS focus, and off-putting language and jargon. We recommend that a social care specific assessment is developed with questions that are written in plain English so that they are more easily understood. Furthermore, we have made detailed recommendations in section 3.1 as to how toolkit functionality could be improved, which are:

- make performance monitoring data (of DSPT and NHSmail progress) by council or CCG area publicly available;
- create a ‘social care provider’ organisational type that replaces care home and domiciliary care and gives access to Entry Level;
- automatically turn on HQ functionality for A*** ODS code registration and/or that the DSPT registration guidance is amended to reflect this;
- produce guidance that explores the internal governance issues related to multi-site companies and DSPT publication;
- have a single channel of communication with large national providers (about DSPT) that is clearly communicated to local and regional support organisations;

- develop a new level of toolkit publication – Improvement Required or Standards Nearly Met (or similar wording) - that allows providers to publish an action plan rather than an assertion that the standards have been fully met;
- make the changes listed in Appendix Four to questions asked in the toolkit; and
- make the changes detailed in Appendix Four to the DSPT guides that are available to download from Digital Social Care.

The toolkit is not intuitive and issues with its functionality and terminology mean that it needs interpreting for social care provider organisations. Most small and medium sized social care organisations will struggle to complete the DSPT in any meaningful way without support and guidance. This has knock on affects for any wide scale programme to support its completion, including the risk of a lack of DSPT experts. We think that programmes to support providers to complete the DSPT should focus on local sustainability and have a variety of engagement and support methods - a mixture of signposting, awareness raising and training plus having a DSPT champion – as well as a variety of organisations actively involved e.g. councils, CCGs, care associations, and local police cyber crime units. Any such programme should promote the DSPT on the basis of its benefits to providers rather than on contractual obligations or as a stepping stone to NHSmail.

We recommend that, if free social care provider use of NHSmail is continued, then support for care providers to set up and start using their NHSmail account is continued (through the Digital Social Care helpline for instance) or included in future DSPT training and support programmes. The pre-pandemic National Administration Service (NAS) NHSmail registration route for social care providers was not user friendly. The process was changed in March 2020 to enable mass NHSmail onboarding. This has made the registration process much easier, but improvements are still recommended, such as:

- There should be a local mailbox admin function that allows care providers to have responsibility for adding and removing staff without going through the help desk.
- The complexity and length of shared mailbox addresses is problematic and reduces the likelihood of providers routinely using them.
- Asking for unique email addresses and mobile numbers for the individual account opening process is causing some providers problems.
- The process should allow dual registered managers to open more than one care site's shared account.
- Helpline options should allow providers to speak directly to helpdesk staff.

We suggest that in the short term the NHSmail guidance is reviewed and refreshed and videos and training materials are made available. Longer term, we suggest that further promotion of the benefits of secure email for social care providers is undertaken including the need for it, how to obtain it, and advice on how to check if your system is secure. If wide-scale free use of NHSmail is not continued, then alternative support for social care providers to obtain secure email will be needed along with awareness raising for health services professionals that it is NHSmail compatible.

The data and cyber security issues and concerns that were identified in the 2018/19 programme are still very much present and there is little evidence to suggest that general risk levels across the sector have reduced over the last year. Key risks for the sector continue to be safe use of smartphones, passwords, backups and staff training

and awareness raising. Future programme support should focus on these elements, noting that there are a significant number of providers who struggle with even basic IT and that issues of internet connectivity and digital infrastructure need to be addressed.

The use of personal digital devices for work purposes is common across the sector, but many providers remain unaware of the risks of staff using their own devices. We advise all providers think about the implications of this and develop bring your own device (BYOD) policies and implement better security measures such as some form of mobile device management.

Digital literacy of staff in the sector is low. Making this part of the job role with an expectation of basic IT skills for all care staff is seen as a crucial next step for the sector. Discussion with Skills for Care on how to best achieve this is recommended.

Low digital literacy means that common, widely recognised communication systems such as text messages and WhatsApp are in widespread informal and sometimes formal use (even where prohibited). We recommend that guidance is developed to advise organisations on their options for the safer use of WhatsApp (and other similar, commonly used communication systems) and alternative systems that could be easily deployed.

Whilst there is a wide range of data and cyber security training materials available for use, some free and some at a cost, there is nothing specifically targeted at the social care sector. Developing and promoting better, social care specific elearning and other training modules (and an induction pack) that are appropriate to the different types of roles working in the sector still needs to be done. Effective testing of the impact of training for front line and senior staff is also to be recommended.

There is low awareness in the sector of the need to undertake a data protection impact assessment (DPIA) and therefore low use of them. The example DPIAs and associated guidance developed as part of the programme will be valuable resources that can act as good practice examples for other social care organisations. These can be added to the resources available on Digital Social Care, and the website has the potential to act as a repository of further example DPIAs and for sharing these across the sector.

We discovered that social care providers being the victims of ransomware cyber-attacks is a plausible threat to the sector. Many providers don't make the connection between cyber security and care: "it's unlikely to happen to me" mentality. The social care sector will not be immune to this threat and we recommend that a handbook on how to recover from a cyber-attack is developed - to complement the materials on how to reduce vulnerability and avoid being the victim of an attack.

To help ensure a sustainable and diverse adult social care market, we encourage councils and health commissioners to support local care providers with data and cyber security. We developed guidance that makes suggestions as to how commissioners of adult social care might support providers to adopt appropriate safeguards. This includes the recommendation that commissioners consider building into contracts with providers the requirement to complete the DSPT.

Lastly, the introduction of Digital Social Care since the 2018/19 programme is a welcome development. The social care specific resources and support available from

the website were well thought of and valued by all involved in the programme. However, there is low awareness of the website across the sector and we recommend that Digital Social Care marketing and communications approaches are reviewed to ensure that it reaches, engages and influences care provider owners and leaders more widely.

5 Appendix One: Products developed by local projects and IPC

Institute of Public Care

- Guidance for commissioners – suggestions as to how commissioners should support providers to keep systems and information safe and secure
- Risk assessment – a tool to help providers self-assess what key data and cyber security risks they might have and to prioritise those risks and think about next steps
- A review of data and cyber security training materials – a review of their suitability for social care staff
- DSPT getting started guide – one-page guide that gives basic information and signposts to the DSPT, the ODS portal and Digital Social Care guidance
- DSPT Standards Met summary of evidence items
- DSPT introductory workshop training materials – slides and handouts
- Registering for NHSmail training materials - slides

London Borough of Barnet

- DSPT workshop communications and flyers
- Example Record of Processing Activities and Information Asset Register

Central Bedfordshire Council

- Case studies on DSPT completion
- Email templates to send to providers re preparation needed for workshops
- Checklist for managers of services that are part of larger organisations which have completed the DSPT to Standards Met at an HQ level

Blackburn with Darwen Council

- A training video for care home staff that covers cyber security risks and uses less-technical language
- A training video for owners / managers of care homes who have responsibility for IT security as part of their job description

Care England

- A top ten tips to establish a cybersecurity culture in a social care setting
- A questionnaire for people to help establish the knowledge of workers
- Case studies on how a dedicated supported resource focussing people's minds on cybersecurity can bear results

Dorset Partners in Care

- Encrypted Emails – What is encrypted email and how to achieve it
- Staff guide to avoiding Cybercrime - Eight steps that you can take to protect yourself from becoming a victim of cyber fraud
- Protecting and backing up your computer – How to ensure your computer is protected and how to backup your data
- General computer operating systems – What is an operating system and how to make the right choice

- How to create a document management system – Three steps to creating a system which allows information to be created, shared, organized, and stored efficiently and appropriately
- What is digital data storage? - A guide to digital storage options and common causes of digital data loss.
- What is the cloud? - Why you need to consider cloud-based storage options and the benefits
- Bringing your files with you – What to consider when you need to take digital files to a different location and options to do this
- What are accessibility features? – A guide to common accessibility features
- Troubleshooting – Top tips for common problems with your computer

Durham County Council

- Guidance on adding NHSmail account to Microsoft Outlook
- Email template to request additional users for shared NHSmail
- A series of short videos to help providers find their ODS code, register on the DSPT and use NHSmail

East Midlands Care Limited

- Training and development toolkit:
  - Identification and nomination of a cyber security champion
  - Training of cyber security champion and cyber security champion training analysis tool
  - Digital footprint audit tool for current IT structure
  - Learning needs analysis
  - Training plan
  - Training tool to deliver improved and supplementary appropriate staff training and awareness around cyber security to ensure the safe use of digital technology
  - Learning needs analysis gap planning tool
  - Future training plan
- An introduction to cyber security: staff training presentation

Hampshire Care Association

- DSPT and NHSmail training materials – slides
- DSPT and NHSmail certificate
- DPIA policy, template and example completed DPIA for telemedicine
- Frequently Asked Questions about the DSPT, NHSmail and DPIA
- Telemedicine care home scoping exercise
- DSPT common policy examples and templates: IAR, ROPA, privacy notice etc

Lincolnshire Care Association

- A guide for SME care providers on understanding their IT support provider needs and what to consider when selecting an IT support provider (work in progress)

Manor Community
- A guide to help senior managers in small care providers decide between purchasing smartphones or asking staff to bring their own device

National Care Forum
- A cyber security readiness/strength matrix tool
- A top tips document including recommendations for enhancing cyber security
- Case studies

North Tyneside Council
- Resource pack for 'Introducing Digital Camera Based Technology' including:
  - Decision tree to guide people through the overarching process
  - DPIA Stage 1 client specific questions and Technology Care Plan
  - DPIA Stage 2 template for approving digital camera-based technology solutions
  - Guided conversation template to support a 'needs led' conversation with clients focusing on where digital technology might be an enabler so that the right technology can be found to meet specific needs

North Yorkshire County Council
- A bring your own device (BYOD) to work policy
- A company device policy
- An introduction to mobile device management (MDM)
- Privileged user access statement of compliance

Nottingham City Council
- Cyber audit checklist and review report
- Training needs analysis
- New to market checklist
- Cyber security staff training materials

Nottinghamshire County Council
- Cyber security attack exercise scenarios
- Business continuity plan template

Peterborough and Cambridgeshire Care Association
- Policy for using mobile devices in the provision of care
- Clauses for staff employment contracts regarding the use of mobile devices.

Shropshire Partners in Care
- Cyber security conference flyer and materials
- DSPT workshop email invite
- DSPT training materials for workshops – slides
- Staff guidance on data breaches v1
- Staff guidance on individual's rights under GDPR
- Staff guidance on information guidance

- Standards for staff with privileged access rights
- Privacy notice

Staffordshire County Council

- Action plan and checklist to support providers to collate appropriate evidence against the DSPT Standards Met assertions
- Information governance and data security and protection training materials - slides

Stonewater

- List of digital consent products on the market with pros and cons for each
- Brief guide for organisations considering moving from evidencing consent via hard copy to digital signatures

Voluntary Organisations Disability Group and Association of Mental Health Providers

- Data and cyber security survey questions and analysis
- Project summary for providers with associated appendices:
  - DSPT experiences
  - Skills and Training
  - Information Sharing
  - Third party applications
  - Other cyber security issues
  - Glossary

West Midlands Care Association

- Templates for confirmation emails prior to workshops, with details of preparation work needed, and follow up email if successfully opened NHSmail account or not
- NHSmail opening checklist
- DSPT Entry Level Workshop training materials – slides
- Information Asset Register Template
- Data Sharing with Suppliers Template

Wiltshire Care Partnership

- Legal Specification to establish a comprehensive ethical and legal framework suitable for such technology's wider use
- Amazon Echo Guidance and start up tips
- Feedback from participating providers on how the devices could be used within the care sector

6 Appendix Two: Feedback from providers participating in local projects

IPC was asked to send a short survey to participating providers of local projects that were part of the Adult Social Care Data and Cyber Security Programme 2019/20. The aim of the survey was to help inform sector learning and to influence next year's programme, including how best to engage providers with this subject. Providers were asked about their experiences of taking part in the programme and their ideas for improvements.

6.1 Methodology

Local project leads were asked to provide contact details (name and email address) of providers who had participated in local projects. Most leads (18) provided contact details, whilst others (3) preferred to send the questionnaire out themselves. The online survey that providers were asked to complete is reproduced in section 6.3. The survey was sent out on Monday 24 February 2020 and the deadline for completion was Friday 6 March 2020.

6.2 Findings

6.2.1 Responses

390 questionnaires were sent out by IPC and links were sent out to further providers by three of the project leads. Ninety-nine responses were received, of which 27 were partial, and 72 were complete. The response rate for completed surveys (based on a minimum of 390 potential respondents) is therefore 18%.

The local projects with the most respondents included Central Bedfordshire (9); Shropshire Partners in Care (6) and West Midlands Care Association (14). These were all projects supporting providers to complete the Data Security and Protection Toolkit (DSPT) and had higher than average numbers of participants. For four local projects, no feedback was received: Blackburn with Darwen; Care England (LD and London); North Tyneside. These were all phase two projects.

The timeframe for completion was short, and at the time, some providers had not completed (or in some cases had not even begun) their participation in the programme and this may have affected the response rate overall, particularly for phase two projects.

6.2.2 Organisation type

Organisation types of responding providers were as follows:

Survey respondents by type of organisation

Type of organisation	Proportion of respondents	Respondents %	Number
Care home		54%	39
Domiciliary care		35%	25
Supported living		8%	6
Other		3%	2
Total		100%	72

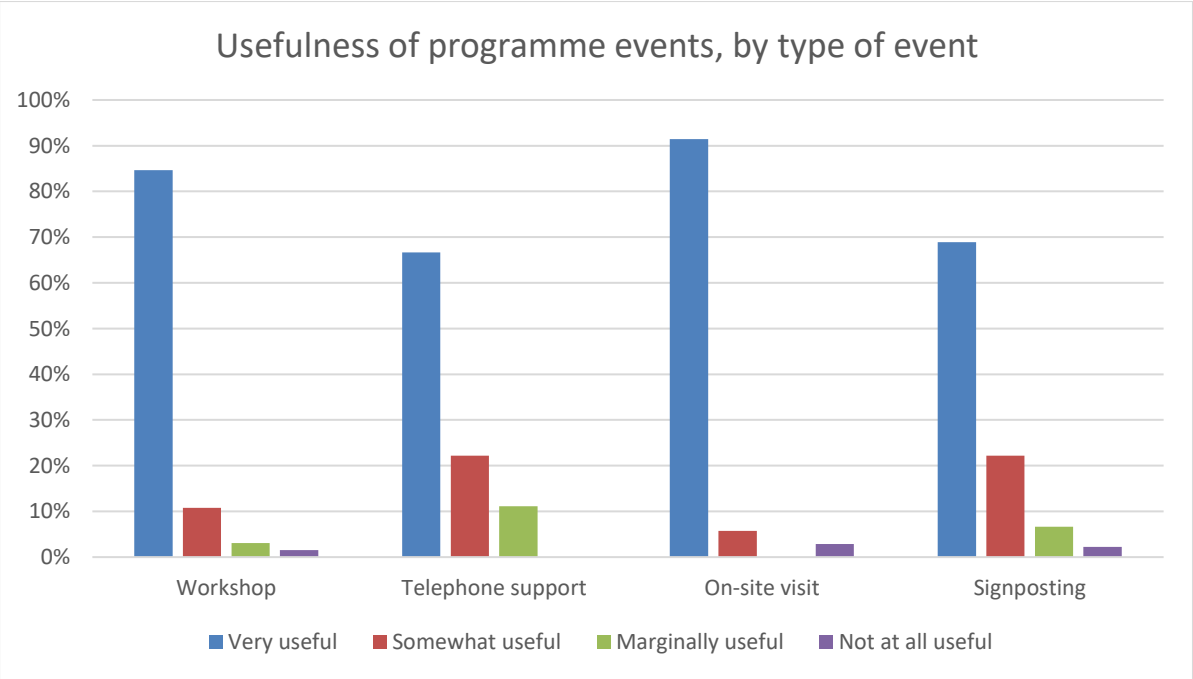
6.2.3 How did people participate in the programme, and how useful did they find these events

Participation was possible through workshops, telephone support, on-site visits and signposting to sources of help and guidance.

Participation in the programme, by type of event

Type of event	Number of providers attending	Proportion of total respondents %
Workshop	65	90%
Telephone support	27	38%
On-site visit	35	49%
Signposting to e.g. websites	45	63%

The majority of providers (90%) participated in the programme through attending workshops, which reflects the nature of the local projects, with a number focussing on DSPT training, and others offering project set up and completion workshops. Almost two thirds of providers (63%) were signposted to sources of information. To support providers to work on the toolkit, nearly half (49%) received an onsite visit, and just over a third (38%) received telephone support to do this. The graph below shows how useful providers felt those different types of events were.



Providers experiences of events were on the whole positive. Onsite visits (perhaps understandably given the one to one nature of the support) were cited by 91% as being very useful, although this figure was lower for telephone support (67%) suggesting that face to face support is a more effective medium for working on the toolkit. The majority of providers also found workshops very useful (85%) and also the signposting of information (69%). Where providers had found events not useful at all this appeared to be to do with logistical issues.

6.2.4 What did providers learn through participation in the programme?

Providers stated what they had learned through the programme and a number of themes emerged.

People cited learning in terms of how to use the **toolkit** and gain access to **NHSmail**:

"Everything about the Data Protection Toolkit and the things we need to be aware of and implement as a care home".

Other key themes were increased knowledge around **data protection** and learning around **cyber security**, and some learning around **digital** more generally. For example:

"As an organisation [we] have improved our whole IT system and storing of our information".

"Extensive awareness of cyber threats and how to work proactively to prevent the likelihood".

Providers also talked about learning from colleagues and how the **networking** had been beneficial: "*[it gave me] more confidence"*.

There was also some learning around **policies** and what needed to be in place:

"It has made me look more in depth at our policies and procedures and question how much more we can include in them – some things we have changed immediately".

6.2.5 What did providers say was good about the programme?

6.2.6 What further support does the sector need, locally or nationally?

Providers were asked what further support the sector needs. The overwhelming message from providers is that more support is needed; recurring themes on what forms that should take included:

- Raising awareness throughout the sector
- More help on the toolkit, including:
  - Reminders to refresh

  - Training: *"A refresher would be handy when the next year's submission is due. This would support in running through answers and inform members how it would look when you revisit the site. Such as 'If you were to resubmit now, you would not be at Standards met'. This was a bit of a shock to me."*
  - Simplified wording on screen/more user friendly: *"I consider myself to be well educated and very computer literate, but this baffled me, so perhaps more support whenever something like this is being implemented."*
- More training, including more workshops / on-site visits
- More information about digital options: *"The sector needs assistance with technology to be able to benefit from the technology that is available to them".*

Time was cited as an issue; here providers want more time to participate in programmes and complete the toolkit.

A small number of providers thought that they had received sufficient support and that further support was not needed.

6.3 Provider survey

About this questionnaire
Why are we sending you this survey?
What are the questions about and how long will it take me to complete?
When should I complete it by?
Who can I contact if I have any questions?
Will my responses be confidential? What will happen to the information I supply?

About you

1. Choose the local project you participated in

2. Your organisation type (Care home, Domiciliary care, Supported living, Other)

3. How did you participate in the programme? And how useful were these event/s?

	Very useful	Somewhat useful	Marginally useful	Not at all useful	N/a did not attend
Workshop	☐	☐	☐	☐	☐
Telephone support	☐	☐	☐	☐	☐
On-site visit	☐	☐	☐	☐	☐
Signposting to e.g. websites	☐	☐	☐	☐	☐

4. What have you learnt through participation in the Programme? (free text)

5. What was good about the Programme? (free text)

6. What further support does the sector need, either locally or nationally? (free text)

7 Appendix Three: Example email from helpdesk – provider could not publish at Entry Level and helpdesk reply did not resolve the issue

To: EXETER, Helpdesk (NHS DIGITAL)

Dear Sirs

I have now completed the DSPT as a Social Care Provider at Entry Level responding to all 14 evidence items. They now show COMPLETED and I have also completed some mandatory items and my screen shows the following:

Progress dashboard and reports

37 of 56 mandatory evidence items provided
0 of 42 assertions confirmed
Your assessment status (if you were to publish now)
Standards NOT Met

From: Andrew (A***)

From EXETER, Helpdesk (NHS DIGITAL)

Good afternoon Andrew.

Thank you for your email.

I can confirm that an entry level assessment is only available when completing the DSPT under the site code.

The code you are using to complete the toolkit is a HQ code and entry level is not applicable as you can complete one toolkit on behalf of multiple sites.

You will need to complete all the mandatory questions under the HQ code and confirm all of the assertions before you publish the assessment to achieve Standards Met.

If you have any further questions, please reply to this email.

If your organisation has an HSCN connection you can now log and monitor your own calls using our Self Service Portal. If you would like to use the portal please contact the service desk for an account to be set up

Exeter Service Desk

To: EXETER, Helpdesk (NHS DIGITAL)

Thanks for this and I'm not sure how this has happened as we are a small social care provider with a thirteen bed residential care home and I will not be able to fulfil many if any of the mandatory questions or assertions for that very reason.

Maybe I have done something wrong in establishing our account and I've been following the guidance for social care providers hence the 14 areas of evidence.

What would you suggest I do now as either way when I publish it's going to come out as not all standards met?

Andrew

To: Fiona Richardson

Good Morning

I am due to submit my report following receipt of funding for the safe use of technology in care services, however as you will see from the email trail my organisation appears to have been given an HQ code rather than a site code for completion of the DPST. I have completed all the 14 areas where evidence is required at entry level as a small social care provider and I am concerned that without such a site code, I will fail to be compliant and will have no way of being measured fairly against the standards for a small social care provider.

Can you help?
Andrew

From: Fiona Richardson

Hi Andrew, it may be because of the organisational type you have registered on the toolkit as.

Entry Level is only for social care organisations, and the toolkit only recognises the organisational types "Care home" or "Domiciliary Care Organisation" as being social care organisations. If you have registered your organisation as anything else (such as Charity) then you won't be able to publish at Entry level.

If that is the case then I suggest you change your organisational type to Care Home then publish the toolkit at entry level - you can always change it back again afterwards. To do that, log in to the toolkit and click on 'Admin' then 'Organisational Profile' then under 'Sector Information' you should be able to change your organisational type.
If that is not the case ie you are already registered as a care home then give me a call.

If you would like me to have a look at your toolkit assessment then add me as an 'auditor' view.

Hope that helps
Fiona Richardson

To: Fiona Richardson

Thank you so much Fiona, that worked and I have now published as a ‘Care Home’

Andrew

8 Appendix Four: Suggested changes to DSPT questions and Digital Social Care guidance

We suggest the following changes to the questions asked of social care providers in the toolkit:

- Delete the requirement for social care providers to complete question 2.1.1 as it is a repeat of 1.4.3.
- Assertion 3.2 and evidence item 3.2.1, change the wording so that it doesn't suggest that there is a specific, national data security and protection test that it is mandatory for all staff to complete.
- Delete 6.2.1, 6.2.2 and replace with one question that asks whether providers run up-to-date antivirus software.
- Delete 6.2.8 and replace with one question that asks whether they have spam or junk email filtering in place.
- Delete 6.3.1 as social care providers do not have access to CareCERT.
- Delete 8.1.1, 8.2.1, 8.2.2 and replace with one question that ask “List the software you use and your plan to keep it updated” or similar.
- Section 9 - add in one mandatory question asking about staff and volunteers having strong, separate passwords for email and other important accounts.
- Change wording of 9.1.1.
- Add in a question about backups.

In addition, we suggest that the DSPT Entry Level Guide and Standards Met Guide, that are available to download from Digital Social Care, are amended to:

- Give brief details about HQ (A***) and site (V****) ODS codes and signpost to further information about registering on the DSPT.
- Better explain the key roles mentioned in the DSPT e.g. SIRO and IG lead.
- Make it clear that Entry Level is only available for social care providers, and organisations have to register as either a care home or a domiciliary care organisation to be classed as a social care provider (in the toolkit).
- Highlight that new users added to the DSPT need to activate their accounts within 24 hours.
- Reflect the new Entry Level view in screenshots.
- Be clearer that social care providers don’t have to complete all the evidence items, only the mandatory ones, to reach Standards Met.
- Highlight a common mistake that is often made – people enter text in the comments box rather than the evidence item, but we recommend that you use comments to make a note for yourself so that you can understand your answer when you republish.
- Give updated instructions on how to publish an assessment.

We also suggest the following changes to some of the ‘answers’ in the Guides and the Entry Level Workbook:

- 1.6.5 and 1.6.6 - the guides and workbook seem muddled on advice about DPIAs. In places providers are advised that they should conduct a DPIA for any system or

process that uses or shares personal data. In other places the advice is to complete a DPIA "when you introduce a new system" or if you have CCTV and elsewhere it states "you only need to carry out a DPIA for 'large' data processing systems." Both the guides and workbook state that providers should have completed a DPIA for their existing care planning system (paper or electronic), which providers think means they have to retrospectively do a DPIA for all their systems, even if they had them prior to 2018.

- 1.4.4 – the situation with the national data opt-out policy is unclear and advice about how social care providers can comply with it is needed.
- 2.2.1 - clarity is needed re the scope of staff guidance available and Care Certificate Standard 14.
- 4.3.1 - provide an example System Administrator agreement.
- 4.3.4 - provide greater clarity on what sort of monitoring of access is needed.
- 5.1.2 – a rewrite is suggested to match question rather than section title.
- 6.1.1, 6.1.3, 6.1.4, 6.1.5 - suggested rewording for greater clarity and to stress the importance of recording near misses for internal learning.
- 9.6.2 - this question needs more advice on mobile encryption, which could be taken from an Introduction to cyber security if the 'detailed advice' mentioned currently has not been developed.
- 10.1.1 – the workbook should be amended to match the advice given in the guides and the examples of hairdressers and window cleaners given in the workbook need to be removed.
- 10.2.1 – the advice needs links to information about the Cyber Essentials scheme and how providers should undertake due diligence on their suppliers.

The DSPT Entry Level Workbook is linked to a series of webinars - it was designed to be completed in parallel to providers participating in the webinars. But there are no 'live' ongoing webinars or recordings of past webinars available. We recommend that, if possible, webinar recordings are made available on Digital Social Care or are created. We also suggest that a DSPT Standards Met Workbook, in the same format as the Entry Level one and with accompanying, recorded webinars is developed.

9 Appendix Five: Issues with National Administration Service NHSmail registration process pre-pandemic

To open the shared site account, providers need the site postcode where they are registered, their CQC location ID (which is on their registration certificate) and the CQC Contact ID. Other problems were caused by the unclear time constraint and requirement for personal communication details to be provided for all staff registering for individual NHSmail accounts, which happens at the same time as opening the shared site account, and log in instructions received as well as the lack of a local administration function. These issues were experienced consistently across all local projects and are explored in more detail below.

Provider not being identified on the system from postcode

Care providers enter the postcode of their site in the Care Provider Registration Portal. Organisations registered at that postcode in the ODS portal are displayed for the applicant to choose from to begin the process. However, there were several instances when the provider has not been listed when they enter their postcode to sign into the system and their postcode generates the message *"Postcode mismatch, Cannot find an organisation name at this postcode"*. This apparently is a security feature if either the postcode is different in the ODS data set or the care site has already registered and obtained an account (to stop duplicate accounts being created) – we have discovered though that this will happen if someone has attempted to create an NHSmail account in the past even if that attempt was not successful. Unfortunately, there is no explanation of why this happens – in the guidance or via error message from the system – or how to rectify the issue(s). Providers are stumped at this point and cannot progress any further; many will give up, assuming their site is not eligible to open an account.

CQC location ID not accepted

The CQC location ID is printed on the provider's CQC registration certificate. In many instances the location ID is not accepted by the portal (even when the provider has their CQC certificate to hand and the data input was triple checked). There appears to be some discrepancies between the data set used by the portal and the information given to providers. We have found a work around to check location IDs online through the CQC website, but this method is not obvious unless you know about it, although it does mean we can now be sure the location code used by providers at the workshops is the same at that held in the CQC data set. It would be helpful if the NHSmail registration portal told you which details (the Location ID or Managers ID) was incorrect rather than having to do it by a process of elimination.

CQC Contact ID not known or accepted

A more significant problem is the requirement for the CQC Contact ID (also known as the CQC registered manager's ID). Given the churn in the system a significant minority or care providers either have no registered manager currently or there has been a change of manager in the last six months. We understand that the NHSmail data set is a few months 'behind' the CQC data set (which in itself is not that up to date) which causes problems if there has been a recent change of manager.

Notwithstanding issues of churn of managers, there also seems to be a glitch in that the registration portal does not accept some current CQC Contact IDs. The WMCA experience is that 20-30% of IDs are not accepted by the system – even if the provider has documentary proof of the ID, potential data entry/keystroke errors are triple

checked, and there has been no recent change of manager. CQC manager ID's are usually 9 or 10 digits long (usually either 1-123456789 or CON1-1234567891). The portal seems to accept 10 digit manager ID numbers with fewer problems than the 9 digit numbers. These sometimes work and sometimes they don't with no discernible pattern as to why. We have not found a work around to be able to check managers IDs online through the CQC website.

If the CQC Contact ID is not accepted or not known (or there is no manager), a one-time passcode can be requested via email, which does at least arrive quickly. However, to be able to make that request the provider must enter the correct email address (for the manager) that is held by CQC, which is not possible for a training provider to check. If that email address is not known by the provider or not recognised by the system the only option is a one-time code sent by post within two weeks, which further delays the process and reduces the chances of the account being opened successfully.

Individuals' personal data

If the CQC ID numbers (or one-time passcode) are accepted the provider can then set up the accounts on the care provider registration portal. The portal creates the generic shared account and up to 10 individual accounts. For each person, an existing email address and a mobile phone number must be given - the mobile phone number provided is automatically added to the individual's personal profile within the NHS Directory, however you can opt for this to not be visible. The email and mobile phone number must be unique to both that user and the registration portal. Many care providers do not give their staff email accounts or mobile phones and staff are often reluctant to give their personal details out to be used in this way.

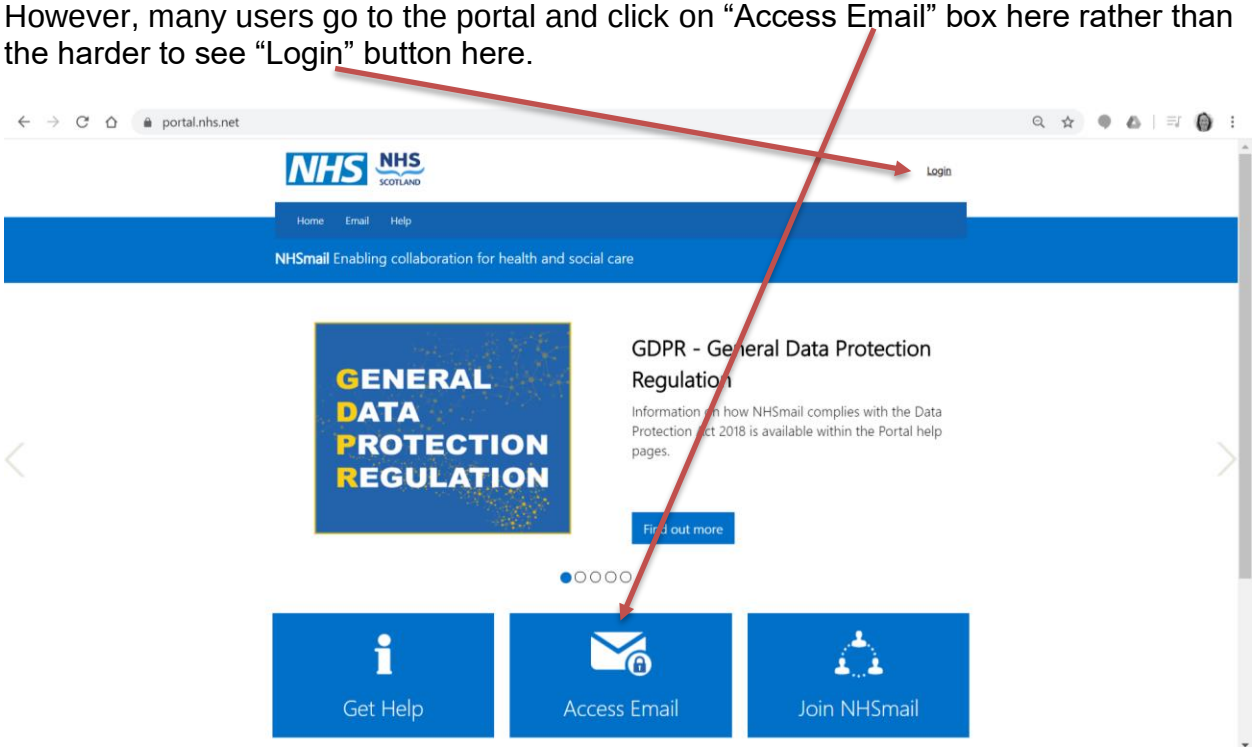
Once the user details have been submitted an email will be sent to the email addresses supplied with instructions on how to activate the new NHSmail account and temporary passwords for these accounts will be sent by text to the individuals' mobile phones. The WMCA was informed by their NHS England and NHS Improvement Regional Lead that individual NHSmail accounts must be activated within one hour. This is not mentioned in the guidance and we have not tested it, but it is widely believed in the sector. If accounts are not activated, because staff are not available at the time of account opening, the registered manager (or shared mailbox owner) cannot create them at a later date. We understand that individual email accounts (linked to a shared mailbox) can be created by NAS administrators at a later date, but we have not been able to test that process. Interestingly, the third party portal allows non social care organisations, such as the WMCA, to create their own users at any time.

In addition, the NAS registration portal is for new users of NHSmail only because the generic shared mailbox is created at the same time as the individual account(s) that are linked to the shared mailbox. This means that owners or managers of services with more than one site cannot open email accounts for all their care sites. This was an issue for dual registered managers who could only open accounts for one of the care homes that they managed. As a work around they would need to get another member of staff to create the shared mailbox for the second site and then subsequently add the manager (who now has an existing induvial account) to the shared mailbox as an owner or member. This is not explained in the guidance.

Login instructions received in initial system email

As part of the account activation process an email is sent to newly registered individuals with instructions on how to activate their new NHSmail account. Users are instructed to go to the portal and click the 'login' button. On activation they are asked to change their temporary password and set some security questions.

However, many users go to the portal and click on "Access Email" box here rather than the harder to see "Login" button here.



If users click Access Email they are not able to accept the T&Cs or set up the security questions and so the account is effectively locked but the new user is not aware of this. We suggest that the activation instructions are amended and/or a technical solution is implemented to prevent this if the NHSmail address is recognised as a new one.

No local mailbox admin function

Care providers that set up a shared site account and individual accounts through the NAS do not have a local mailbox admin function i.e. the ability for the care provider to add and remove staff without going through the help desk. If an employee has an NHSmail address, they can continue to access it when they move care provider / employer unless the employer requests the helpdesk to cancel their email when they leave. Providers reported that there was a significant time lag (two to three weeks) before ex-employees are removed by the helpdesk, during which time they can still access their account, which is a security risk.

10 Appendix Six: Data and cyber security risks from audit visits to services at Standards Met

Category	Homecare 1	Homecare 2	Homecare 3	Care Home Older Adult 1	Care Home Older Adult 2	Care Home Older Adult 3	Adult LD Care Homes 1	Supported living
IT security: firewall, antivirus (AV) and operating systems	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system	Up to date AV, firewall, and operating system
Mobile device security	Encrypted device. System password and up to date AV	Encrypted device. System password and up to date AV	Encrypted device. System password and up to date AV	Two factor authentication and virtual desktop	No laptops or tablets used	No laptops or tablets used	Encrypted device. System password and up to date AV	Encrypted device. System password and up to date AV
Smartphone security	Company phone with PIN, up to date systems and MDM	Company phone with PIN, up to date systems and MDM	Company phone with PIN, up to date systems and MDM	Staff own phones used without enforced BYOD policy	Senior staff use company phone with PIN	Senior staff use company phone with PIN	Company phone with PIN, up to date systems and MDM	Staff use company phone with pin
Logins and passwords	No shared system passwords. Strong password rules.	No shared system passwords. Strong password rules.	No shared system passwords. Strong password rules.	No shared system passwords. Strong password rules.	Shared password on care staff PC. Office staff PCs system password	Shared password on care staff PC. Office staff PCs system password	No shared system passwords. Strong password rules.	No shared system passwords. Strong password rules.
Backups	Daily backups are made and stored off site	In cloud on multiple servers	In cloud on multiple servers	In cloud on multiple servers	External hard drive 3 monthly	External hard drive 3 monthly	In cloud on multiple servers	Daily backups are made and stored off site
Policies (Not BYOD)	Have full range and staff know how to access	Have full range and staff know how to access	Have full range and staff know how to access	Have full range and staff know how to access	Have full range and know where they are	Have full range and know where they are	Have full range and staff know how to access	Have full range and staff know how to access

Category	Homecare 1	Homecare 2	Homecare 3	Care Home Older Adult 1	Care Home Older Adult 2	Care Home Older Adult 3	Adult LD Care Homes 1	Supported living
Physical security	Good building security	Good building security	Good building security	Good building security	Good building security	Good building security	Good building security	Good building security
Staff training and awareness raising	Mandatory on induction re data security and protection. After office staff both and care staff data protection focus	Mandatory on induction re data security and protection. After office staff both and care staff data protection focus	Mandatory on induction re data security and protection. After office staff both and care staff data protection focus	Mandatory on induction and annually	Mandatory on induction re data security and protection. After office staff both and care staff data protection focus	Mandatory on induction re data security and protection. After office staff both and care staff data protection focus	Mandatory on induction and annually	Mandatory on induction and annually
Business continuity plan (BCP)	Have BCP that includes data/ cyber aspects and is tested	Have BCP that includes data/ cyber aspects and is tested	Have BCP that includes data/ cyber aspects and is tested	Have a BCP and experience of recovering data	Have a BCP, but weakness due to backup risk	Have a BCP, but weakness due to backup risk	Have BCP that includes data/ cyber aspects and is tested	Have BCP that includes data/ cyber aspects and is tested