Funding for the safe use of technology in care services
Medium sized grants for local projects during 2019/20

Application Guide (Phase Two)

1. Introduction

Digital technology helps care services spend more time caring. It helps the people we support keep control of their lives and of their care; and it helps us to share information safety and appropriately.

But there can be risks – for example how digital information is kept confidential, what happens if something goes wrong with the technology, and the risk of cyber attacks.

Digital Social Care[1] is working with the Local Government Association and NHSX[2] to help ensure that the benefits of digital technology can be achieved safely. We are inviting applications for grants to fund local projects to develop practical solutions to some of the challenges that have been identified.

Grants can be applied for by local councils, by local care associations or by other local groups of providers. Each grant is expected to be of between £20,000 and £40,000.

Eight grants were awarded in Phase One of this programme. Brief details of the eight projects it was decided to fund can be downloaded from the Digital Social Care website.

A similar number of grants are expected to be awarded in this second phase. Those who applied in Phase One but who were unsuccessful are welcome to reapply. However, please read this guide carefully because the type of projects being sought has changed.

All the work funded by a grant must be completed by 31st March 2020.

2. The context

Last year we worked together on programme which asked:

[1] Digital Social Care is is a dedicated space to provide advice and support to the social care providers on technology and data protection. It is a joint project between six of the national trade associations and Skills for Care. Digital Social Care is funded by NHS Digital.

[2] NHSX brings teams from the Department of Health and Social Care, NHS England and NHS Improvement together into one unit to drive digital transformation and lead policy, implementation and change across health and social care.

- To what extent is digital technology used in the adult social care provider sector?
- What are the risks?
- How effective are existing national support materials?

To answer these questions, we commissioned the Institute of Public Care at Oxford Brookes University (IPC) to visit 70 adult social care services in three local areas. Their report has now been published and it can be downloaded here. Organisations considering applying for a grant for a local project are strongly encouraged to read the report before submitting their application.

The services visited by the researchers varied from those that were mainly paper based, and which used very little technology, to those that are were almost paperless. The research found a significant trend towards the increased use of digital technology, including areas such as workforce rostering, digital care planning, electronic sharing of information, and the use of technology to give family members and carers greater awareness of what care has been delivered and when.

The increased use of digital technology means that greater consideration is needed as to how information is kept safe and secure. The research found that, for care providers, the most common risks were around password management, smart phone security and arrangements to ensure that information is backed up.

The report of the research includes a total of 19 recommendations for national bodies, the NHS, local commissioners and service providers. Our aim now is to support and encourage the implementation of those recommendations, with particular focus on the nine recommendations for local commissioners and service providers. Those nine recommendations are appended to this document for your information.

3. What we are asking each local project to do

We now know a lot more about where there are risks, and about the kind of things adult social care services need to do to manage those risks. There are also some very good suggestions about how local councils can give providers more support in this area. But adopting digital technology for the first time, or driving digital innovation, is complex. It's a particular challenge for smaller providers who often don't have their own in-house IT support.

We would therefore like each local project to take a defined problem to research or solve, or an idea or methodology to pilot. These are discussed in more detail in section 4 of this guide.

We think each project will need a project manager and we would like each project manager to recruit a group of 10-12 relevant providers to be involved in the project. As well as being involved with the specific issue of the local project, those 10-12 providers would also be supported to complete the Data Security and Protection Toolkit (DSPT). Grants applications will need to demonstrate how they would support their group of local providers to complete the toolkit to at least Entry Level, and preferably at the Standards Met level, by March 2020.

We expect that the toolkit will, in future, be the only mechanism that most adult social care providers need to use to assess their digital risks. Its completion will support improved information sharing, and it will enable care providers to access NHSMail.

At the end of the project, the project manager will be expected to write up what has been learnt so that it can be shared across the whole sector.

The Institute of Public Care at Oxford Brookes University (IPC) has been appointed to act as an expert advisory organisation and will support each local project. The following table summarises the actions to be completed by each project, and who will be responsible for what.

Local project manager	Expert advisory organisation (IPC)
• Attend an initial national training day and a concluding workshop delivered by the expert advisory organisation. • Develop local project proposal and refine it in discussion with the expert advisory organisation and with any feedback from the Programme Board. • Develop and oversee their project plan. • Recruit and manage a group of 10-12 local providers. • Ensure that, particularly where the project manager is not from a local council, the input and	• Deliver an initial national training day for local project managers. • Support local project managers to refine their project proposals and plans. • Have an ongoing coaching / mentoring role for each project manager – allow 3 days per project manager to be used flexibly by agreement. • Devise and deliver locally an initial half day training session for each group of providers, introducing the subject matter and the DSPT. • Have a time budget of 4 further days to support providers in each

engagement of relevant local commissioners is actively sought. • Host initial workshop for participating providers locally which will include a half day training session from the expert advisory organisation. • Lead the project locally and be responsible for practical local arrangements. • Report regularly to the Programme Board. • Host concluding local workshop, again with input from the expert advisory organisation. • Share responsibility with the expert advisory organisation for progress by members of the provider group in relation to agreed engagement with the DSPT. • Write the project up using agreed format.	local group with project work and with the DSPT. • Deliver a concluding workshop in each area, and a concluding national workshop for project managers. • Share responsibility with project managers for progress by members of the provider groups in relation to agreed engagement with the DSPT. • Where work on the subject of a local project is also being undertaken by Digital Social Care, facilitate a link between it and the project. • Extract learning from each project, and from providers' DSPT experience, and collate into an overall national report.

4. Project topics

Here are some suggestions for projects that you might want to consider.

1	Safer use of mobile devices
Summary	Exploring how providers, particularly small providers, can improve their arrangements for securing smart phones and other mobile devices.
Context	The 2018/19 research identified that the use of smart phones and other mobile devices is one of the most common risks across the sector. This was particularly the case where staff were using their own phones for work purposes. Technical solutions and effective "bring your own device" policies were mainly found amongst larger

	organisations. Practical and affordable solutions need to be developed for smaller providers.
Example	A project that worked with a group of small care providers to help them put in place technical and policy arrangements to minimise the risks arising from the use of smart phones and other mobile devices; using the experience to develop guidance, case studies or other resources that could be used by providers across the sector.

2	Retention of digital information
Summary	Helping care providers to decide how long to keep digital information, and how to implement that in practice.
Context	There is widespread confusion about how long adult social care services should keep records and information, whether they are paper or digital. There is separate national work planned to make this clearer. However, even with a clear policy, without well organised electronic filing and archiving systems, providers may well still struggle to ensure that information is kept for as long as it is needed but not for longer.
Example	A project which linked with the national work planned on the development of clearer guidance on how long records should be kept, and which worked with a group of providers of different types and size to develop ways of working that make it as easy as possible to follow agreed schedules reliably.

3	Completing a data protection impact assessment for a new digital system
Summary	Helping care providers ensure that, before they implement a new digital system, they have fulfilled their obligations under data protection legislation to consider and act on any data risks their new development could entail.
Context	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. It is good practice to complete one for any project

	involving significant data processing, and sometimes it will be a legal requirement. For care providers introducing a new digital system, a DPIA is likely to be at least good practice.
Example	A project that worked with a group of providers who are in the process of introducing a new digital system, for example care management, rostering or medication software, and helped them work through the DPIA process; using the experience to develop guidance, case studies or other resources that could be used by providers across the sector.

4	What happens when you want to stop using a digital system, or change to using a different system?
Summary	Helping care providers manage situations in which they want to stop using a particular digital system; ensuring the safe transfer of personal data from the old system to its future location; and/or agreeing arrangements for the archiving or deletion of data from the old system.
Context	There will be times when a care provider wants to change from using one digital system to using another. With the widespread use of digital systems being relatively new, this may not yet be common, but it will be more routine in future. There is the need to ensure that the security of personal data and the on-gong work of the service are both maintained through any such transition.
Example	A project which worked with a number of care providers who are making or planning such a change, identifying any challenges or risks it led to and identifying ways in which these could be minimised. (NB – because fewer providers are likely to be making such a change at any particular time, it is recognised that the group of providers involved in this project is likely to be smaller than the usual 10 – 12.)

5	Staff training and awareness around cyber security
Summary	Researching, trying out and sharing options for staff training and awareness around cyber security.

Context	The research completed by IPC during 2018/19 found that greater staff training and awareness around cyber security were often needed. However, while there are many training options around general data protection and GDPR, it may not be easy for care providers to identify relevant, accessible and affordable training options for cyber security.
Example	A project that identified possible cyber security training options and supported a group of providers to try them out; providing feedback to the training providers and sharing information for the wider sector.

However, while these are our suggestions, other ideas for local projects would also be welcomed!

Please note, however, that this programme is specifically about minimising digital risks, and cyber security in particular. Applications that seek funding for general digital development, for example for the introduction of a new digital system or of a new piece of technology, are unlikely to be accepted unless they can demonstrate clear and specific cyber security benefits.

Whether you are interested in one of these projects, or have other ideas, please think about what the sector as a whole will be able to learn from your project, and about how this would fit with the following three priorities set out in the National Cyber Security Strategy:

- Identify: Understand the level of risk
- Protect and detect: Take action to minimise the risks identified
- Respond and recover: Have plans in place so that, if a problem does occur, you can get back up and running quickly.

We want to fund projects that help the sector learn how best to work under one or more of these priorities. There are more details about these priorities in Appendix 2 of this document.

5. Application process

The closing date for applications for this second phase of the local grants programme is midnight on Friday 11th October 2019. Organisations wishing to apply for a grant during this window should complete the application form and return it by email to cyberproject@rnha.co.uk

Please note that:

- The Programme Board is keen to encourage a collaborative approach locally. Where it is relevant and possible, we would encourage care associations or other provider groupings to seek the support of at least one relevant local council. We would also encourage councils which are applying for a grant to seek the support of at least one local care association or other provider grouping.
- If you have any questions about the application process, please email them to cyberproject@rnha.co.uk by Tuesday 1st October 2019. Anonymised responses will be posted on the Digital Social Care website on a weekly basis during the application window.
- The Programme Board reserves the right to ask applicants for additional information or clarification before making a final decision whether to award a grant. In particular, unless you are a local council, before your grant is confirmed you will be asked to complete an additional form to provide the usual "due diligence" company information. This will include information about your legal status, financial position and any previous legal or regulatory issues.

6. How will grant applications be assessed?

Applications will be reviewed by a group consisting of the Programme Board members listed in section 8 of this guide; NHS Digital; the Programme Manager, who is Peter Cheer of Care Inc Ltd; and the Institute of Public Care (IPC). The group will check that applications are complete and will then score the questions in section 3 of the application form.

The group will then select a group of grants applications made up of proposals that scored well and which, together, cover a good range in terms of the topics to be covered, types of organisation, geographical spread etc. It should be noted that this means that the group of projects selected may not necessarily include all of the applications awarded the highest scores.

7. Timetable

The timetable for this second phase of the grants programme is as follows:

Detail	Date(s)
Start of application period	Monday 16th September 2019
Deadline for questions about the application process	Tuesday 1st October 2019

Deadline for completed applications to be submitted	Midnight on Friday 11th October 2019
Notification of grant award decisions	By Friday 25th October 2019
Project managers to finalise their project plan taking in to account feedback from the Programme Board and from the advisory organisation, and to have recruited a group of 10-12 local services to take part in the project	Friday 30th November 2019
Draft project report to have been submitted	29th February 2020
Project to have been completed and final project report to have been submitted	31st March 2020

8. Funding and payment

The budget for this programme is held by the Registered Nursing Home Association (RNHA). The RNHA is one of the members of Digital Social Care and it holds this programme budget on behalf of Digital Social Care, the Local Government Association (LGA) and the NHSX. Together these three organisations form a Programme Board which oversees the programme.

By applying, you are agreeing that, if successful, you will accept the programme's grant conditions and sign a grant agreement with the RNHA. A pro-forma version of the grant agreement can be downloaded from the Digital Social Care website.

50% of each grant will be paid at the start of the project. 25% will be paid at the mid-point, subject to satisfactory progress. The final 25% will be paid when the project has been successfully completed.

9. Useful information

Detailed guidance on safe data management, and on cyber security, designed specifically for adult social care providers, has been funded by NHS Digital and can be found on the Digital Social Care website. This includes detailed guidance on completion of the Data Security and Protection Toolkit (DSPT).

Appendix 1

Extract from the report by IPC of the research completed by this programme during 2018/19.

Recommendation numbers given below are as per the published version of IPC's full report.

Recommendations for local commissioners

11 Councils to consider supporting local care providers with provision of data and cyber security information, advice and guidance and/or services, which could be on a charged for basis. This support could include data and cyber security training and signposting 'packs' for small or local services that are entering or new to the market.

12 Councils to consider extending local contract management arrangements that already take place with providers so that they include an emphasis on safe and secure handling of information.

13 Councils and CCGs to encourage their local care provider markets to comply with recommendation 1, i.e. to complete the Data Security and Protection Toolkit, and consider including this as part of local contractual arrangements and practice.

Recommendations for Service Providers:

14 Subject to the recommended improvements to the Data Security and Protection Toolkit (see recommendation 2), care providers should complete the toolkit to self-assess their data and cyber security. In the meantime, care providers should check their organisation's IT security against the National Cyber Security Centre's guidance.

15 Care providers to review password and smartphone security practice against the National Cyber Security Centre's guidance (and where possible consider multi-factor or two factor authentication).

16 Care providers to support staff and volunteers to maintain awareness of data and cyber security risks and good practice through induction training and ongoing awareness raising.

17 Where IT support is outsourced to external organisations, undertake data and cyber security due diligence checks to ensure compliance with national guidance (as per recommendation 7).

18 Care providers to ensure that they have access to a secure electronic data transfer method. Where secure email (other than NHS mail) is in use, register this using the secure email accreditation process so that this is

recognised by other care and health professionals and to further support the sharing of information.

19 Care providers to review their business continuity plan to ensure it extends to information technology and digital systems, and to test this at least annually.

Appendix 2

National Cyber Security Programme Priorities

The overall objective of the National Cyber Security Strategy is that:

> "Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence and trust that their information is safe."

The strategy sets three outcome priorities and, for the purposes on this programme, they have been summarised for the adult social care provider sector as follows:

Identify	Protect & Detect	Respond & Recover
Understanding the level of risk	Taking action to minimise the risks identified	Have plans in place so that, if a problem does occur, you can get back up and running quickly

The research in adult social care services completed by IPC during 2018/19 has provided a good understanding of the level of cyber security risk at sector level. Funding applications for projects that would develop our knowledge and understanding under the headings "Protect and Detect" and "Respond and Recover" are therefore more likely to be successful.

"Protect and detect" could cover a wide range of projects designed to make the systems and working practices of adult social care services more secure, and more resistant to cyber security risks. This could include looking at whether systems handling sensitive information have been designed and built with security in mind; whether know vulnerabilities in systems, networks and services could be addressed; and how services can check that companies that supply them have appropriate data and cyber security arrangements themselves.

"Respond and recover" could cover projects that focus on what would happen if there was a cyber incident, or if access to digital systems was interrupted for some other reason. Do services have documented and regularly tested plans to respond to cyber incidents? How could the disruption that could be caused by a cyber-attack be minimised? How could providers have access to the skills needed to respond to a cyber-attack?