

**Meeting:** Improvement and Innovation Board

**Date:** 15 December 2022



## **Cyber, Digital and Technology Improvement Programme Update**

### **Purpose of report**

For information

### **Summary**

The LGA's Cyber, Digital and Technology (CDT) Programme is funded to support the cyber-resilient digitalisation of councils. It does so through convening networks, providing general support (such as advice, guidance and training), policy advice and advocacy, and offering bespoke support through Cyber-360s and Reaction exercises.

Funding for 2022/23 totals £6.2 million. This is comprised of £3.55 million of Cabinet Office funding carried over from 2021/22; £1.9 million of new Cabinet Office funding; and £0.75 million of DLUHC funding that was granted this month.

The Programme for 2023/24 will be funded by the carrying over of a minimum of £1.65 million of this year's funding.

**Is this report confidential?** No

### **Recommendation**

That the Improvement and Innovation Board notes the progress of the Programme.

### **Contact details**

Contact officer: Owen Pritchard and Rebekah Wilson

Position: Head of Programme and Programme Manager

Phone no: 07795 842478 and 07464 652838

Email: [owen.pritchard@local.gov.uk](mailto:owen.pritchard@local.gov.uk) and [rebekah.wilson@local.gov.uk](mailto:rebekah.wilson@local.gov.uk)

# Cyber, Digital and Technology Improvement Programme Update



## Background

1. The LGA's Cyber, Digital and Technology (CDT) Programme is primarily funded by the Cabinet Office's National Cyber Programme. It aims to support councils as they adjust to the ever-increasing use of technology within society. The Programme is not just about cyber security or IT but serves as an enabler of public service modernisation. It has delivered, over its five-year lifespan, a wide package of support on digital change and cyber resilience.
2. Councils, like much of society, have embraced digital technologies to change the way they operate and do business. We saw this during the pandemic when councils switched to hybrid and remote working overnight. But, while the pandemic has pushed forward digitalisation, it has also '...broadened the surface area for attacks and has often made cyber security more challenging for organisations' (NCSC Annual Report 2021).
3. Local authorities across the UK are experiencing an average of 10,000 attempted or successful cyber-attacks every single day and have seen a 14 per cent year-on-year increase in incidents to over two million so far this year, according to figures published this year by insurance firm Gallagher. Over the next decade, councils look set to continue their digital journeys and cyber resilience will be critical component.
4. Set within this context, a lack of money and legacy IT are two serious problems for councils. Additionally, few senior leaders in councils are digital natives, and fewer understand tech-related security and ethics. Managing technology-based risks and opportunities will get harder as the use of technology increases. The tensions between independence and assurance, resilience and efficiency, confidentiality and insight, and transparency and complexity will also intensify.

## Digitalisation outcomes

5. In July this year, the LGA, along with Socitm and Solace, launched an [outcomes-based framework](#) for improving and supporting local government digitalisation programmes. The framework is intended to promote the use of a common language and shared strategic outcomes by local government. The 12 strategic outcomes relate to: connectivity, data, democracy and participation, ethics and sustainability, inclusion, leadership, local productivity, organisational capability, partnership, security & resilience, services and value. To support and advance the framework, we are developing a local government digitalisation almanac to be published in the New Year.

## Programme structure and approach

6. The Programme is broken down into several overlapping workstreams that are aligned to the [DLUHC Local Digital Collaboration Unit objectives](#). A full outline of our programme of work for 2022/23 and outcomes to date can be found in **Appendix 1**.
7. Some key highlights include:
  - 12 councils have taken part in the Cyber 360 programme.
  - 3 councils have been supported through technical response 'Reaction' exercises.
  - 217 councils have been supported through a grant to fund cyber professional qualifications for officers (to a value of over £1m).
  - 8 officer focussed events have taken place.
  - 2 councillor focussed leadership essentials programmes have been run.

## Other activities

8. We have significantly redesigned our [webpages](#) around the 12 outcomes for digitalisation. Our webpages also feature details of our bespoke cyber support offer and the work we are doing to ensure that local government voices are shaping national priorities. We have also redesigned and relaunched our monthly [Cyber, Digital and Technology bulletin](#), as well as a new [Twitter account](#).
9. So far, this financial year, we have hosted a series of other events on these topics:
  - A roundtable discussion with officers from our Transformation Network on learnings and opportunities from hybrid working.
  - A roundtable discussion with officers from our Digital Democracy network on the opportunities that exist for councils to boost participation, consultation, and engagement in project planning and local policy making through digital democracy.
  - Two webinars run by Microsoft on maximising security and compliance features from Microsoft 365 E3 and E5 licenses, attended by 160 officers across the two events.
  - A closed Chief Executive session at the LGA's annual conference on lessons learned from the Gloucester City Council and Hackney cyber-attacks and a plenary session on the role of digital in levelling-up.
10. The Programme runs a policy, research and collaboration strand. This strand helps to ensure that local government voices are shape national priorities, and that councils are supported to implement national cyber, digital and technology policy and programmes locally. This part of the Programme works closely with councils, developing an evidence-base of best practice and experiences, and engages with policy-makers to achieve the best outcomes for local government and the communities they serve.
11. Significantly, the Programme is engaging with DLUHC as it tests with a small number of councils the feasibility of a Local Government Cyber Assessment Framework (CAF). The original CAF was developed by the National Cyber Security Centre to provide a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. A version of

the CAF is being introduced across central government as part of the Government Cyber Security Strategy. Our Programme has recently established a working group of senior technical officers to discuss with DLUHC what the sector needs from a local government CAF.

12. The Programme also regularly brings together council representatives and key partners to support transformation and improvement. These networks are designed to support officers working in cyber, digital and technology roles. Participants discuss emerging issues and trends affecting councils, and hear from each other and guests on new policies, programmes and practices. The networks identify barriers and facilitators to implementing digital and cyber security policies or solutions and formulate positions from which to engage with central government. Crucial to our groups is having the space to share support, opportunities and good practice. Our networks include:
- The Local Government Digital Committee
  - The Digital Inclusion Network
  - The Cyber, Digital and Technology Policy Group
  - The Transformation Network
  - The Digital Democracy Partnership
  - The Digital Construction Working Group
  - The Digital Switchover Working

## **Risks**

13. The Cabinet Office has asked DLUHC to secure the long-term position of the Programme beyond March 2023. However, we are yet to secure a long-term funding arrangement. We have so far secured funding from DLUHC for the last quarter of this financial year. Additionally, we have been given permission to carry forward some Cabinet Office funding into the next financial year. A key priority remains the negotiation of a longer-term settlement.

## **Implications for Wales**

14. Funding for the CDT Programme is intended for English councils only.
15. The development of new policies and tools will frequently benefit Welsh councils. Moreover, technical learning is shared with Welsh councils through C-TAG which our Programme part-funds. Welsh councils are invited to events organised and paid for by our Programme. We also collaborate with the Welsh LGA on some initiatives.

## **Financial Implications**

16. Funding for 2022/23 totals £6.2 million. This is comprised of a £3.55 million of Cabinet Office funding carried over from 2021/22; £1.9 million of new Cabinet Office funding; and £0.75 million of DLUHC funding that was granted this month.
17. The Programme for 2023/24 will be funded by the carrying over of a minimum of £1.65 million of this year's funding.

## **Equalities implications**

18. The Programme funds and supports inclusivity projects which in turn improve accessibility to public services.
19. The Programme seeks to ensure that EDI aims are met operationally, for example, through recruitment practices, media accessibility, representation at events, meetings, Cyber 360 teams, project boards and procurement panels.

## **Next steps**

20. Beyond the delivery of this year's programme of work, we will begin planning our programme of work for 2023/24 in line with the conditions of our grant funding.

**Meeting:** Improvement and Innovation Board

**Date:** 15 December 2022

## Cyber, Digital and Technology Improvement Programme Update

### Appendix 1: CDT Full Programme Structure and Approach

The Programme is broken down into several overlapping workstreams that are aligned to the [DLUHC Local Digital Collaboration Unit objectives](#).

**Table 1:** CDT Programme of work 2022/23

Workstream	Details	Outputs
1. Work with councils to assess and manage the cyber risk to local government		
Cyber 360s	Free for councils. These are managed and facilitated by the LGA to support cyber improvements in key areas against established good practice through peer-to-peer support from a multi-disciplinary team.	Our target is to support 20 councils in FY22/23. 12 councils have been supported so far as of December 2022.
Cyber Reaction Exercises	Free for councils. These help to establish how well a council reacts to a cyber incident, and to practise their response in a safe, constructive environment.	Three councils supported with cyber reaction exercises as of December 2022.
Cyber resilience in Local Government	In-house research with councils on how to collectively improve the way in which cyber threats and attacks are monitored, detected and responded to in local government.	Report to help inform the way in which we approach conversations with the sector and government.
Cyber Technical Advisory Group (C-TAG)	Grant funding for C-TAG (sub-group of the Local CIO Council and the Local Government Digital Committee) to pay for technical advice and guidance.	Monthly meetings with regular input from key stakeholders including the LGA.

2. Work with councils to substantially reduce disruption to local government services caused by cyber-attacks		
Incident Response	Funding reserve for councils that experience significant cyber incident to work with an NCSC-certified Cyber Incident Response organisation in the immediate days following a cyber-attack.	Ad hoc support.
Cyber Insurance Research	Research to understand the challenges councils face when it comes to cyber insurance and an understanding of options for the potential pooling of risk.	A report to understand support requirements and options.
Cyber Security Operations Centre Discovery	Research to explore the requirement for, and the feasibility and deliverability of, a cyber security operations centre for local government. This will help us understand how the sector can collectively improve how cyber threats and attacks are monitored, detected, and responded to.	A report identifying technical operational models, to inform future work in this area.
3. Work with councils to develop tried and tested routes for improving the usability, accessibility, and security of local services.		
Digital Pathfinders	Grant funding to 12 councils to support them in delivering pioneering solutions to improve digital inclusion, connectivity, and cyber security.	Final reports and assets to be published on <a href="#">our webpage</a> to scale-up and share learning with the sector.
4. Ensure councils have the skills, knowledge and tools they need to design and deliver modern digital public services.		
Local Government Cyber, Digital, Data and Technology Workforce Capability Framework	We commissioned Phase 1 of a research project that will led to the production of a set of cyber, data and technical job roles that will sit within a new workforce competency framework.	Desk research into existing cyber, digital, data and technology workforce capability frameworks. Production of a model for digital job families that exist within councils.
Skills Uplift	Grants offered to officers in every English council to fund participation in a recognised professional cyber course to improve councils' CDT capability.	217 councils have so far received a grant and a further 5 councils have confirmed take-up.

Digitalisation Almanac	Building on the digitalisation outcomes-based framework mentioned earlier, we commissioned the creation of a 'digitalisation almanac' to promote the use of a common language and a shared vision of what digitalisation means and how to get there.	Provisional publication date of January 2023.
Masterclasses and training for Members	Free masterclasses and training to support councillors to improve their understanding and engagement with cyber, digital and technology – and to build greater leadership capacity in this area.	Two-day, in-person event (19 to 20 November): 11 delegates Two-day, virtual event (6 to 7 December) Four half-day virtual masterclasses (January)
Cyber Explainer videos	Creation of videos for councils covering key cyber security and digital concepts to non-technical audience to make cyber security more accessible.	41 scripts have been written. Video production to start in 2023.
Embedding Cyber Resilience in Local Government Supply Chains	Free resources to help councils embed greater cyber resilience in their procurement processes and supply chains based on NCSC's 12 principles of supply chain security for the local government context.	A free <a href="#">web guide and e-learning</a> is available on our webpages. 40 officers have started/completed the training. Two webinars ran in July for procurement officers and IT/Cyber security officers: Over 250 officers registered.
5. Ensure councils have better access to key business systems that follow the standards outlined in the Technology Code of Practices, which include being accessible, user-centred, cloud first and secure.		
Digital, Data and Technology (DDaT) Playbook	Engagement with Cabinet Office Digital, Data and Technology (DDaT) Playbook refresh process. We are working with the LGA's Procurement Team and central government on how members of the National Advisory Group for Procurement and wider sector could be more engaged with improvements on digital and technology procurement.	Attendance at Cabinet Office DDaT Playbook refresh meetings in November and December.  Roundtable discussion with procurement and central government representatives in mid-December.



6. Ensure local government voices are shaping national priorities, and councils are supported to implement national cyber, digital and technology policy and programmes locally.		
Policy support to councils	Development of relevant cyber, digital and technology policy briefs for councils, and what they mean for local government (soon to be published on our webpages).	4 briefs written so far: Government Cyber Security Strategy, Cyber Assessment Framework, National AI Strategy and Digital Strategy. Updated on ongoing basis.
	Regular CDT Policy Group meetings on national government policy developments.	Meet monthly. Summaries available on <a href="#">CDT webpage</a> .
Policy advocacy to central government	Working with policy team to produce a response to Parliamentary Inquiry on Ransomware.	Response to be approved by the Safer and Stronger Communities Board and submitted to Inquiry by 16 December.
	Tracking progress of policies relevant to the secure digitalisation of councils.	Dependent on the development stage of the policy and its content.
	Engagement with government on relevant local government digital and cyber policy areas including: <ul style="list-style-type: none"> <li>- DHLUC on LG Cyber Assessment Framework (LGCAF)</li> <li>- Government Digital Service (GDS) on One Log In</li> <li>- Cabinet Office on Digital, Data and Technology Playbook</li> <li>- Centre for Data Ethics and Innovation (CDEI) on Algorithmic Transparency Standard</li> <li>- DCMS and NCSC on Secure Connected Places</li> </ul>	Recurring meetings with civil servants.