

# **Code of Corporate Governance**

## **Impact of the COVID-19 pandemic and cyberattack**

### **October 2021**

#### **Introduction**

The COVID-19 pandemic and the cyberattack of October 2020 have made significant demands of the Council's governance arrangements. The Council has had to respond to these significant challenges by working at pace, ensuring that the needs of Hackney's residents and businesses were met despite the impacts on the Council's services.

In both cases the delivery of the Council's response has involved complex work in an unpredictable and rapidly changing environment. Reflecting this, the Council has used the framework set out in the Council's Incident Plan to ensure effective governance and coordination. The impacts of both the pandemic and cyberattack are ongoing, and the Council will continue to operate and iterate the governance and management arrangements as required.

The sections below provide an overview of how the principles of the Code of Corporate Governance has been applied in response to these unprecedented challenges.

#### **A. Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.**

The response to both the pandemic and cyberattack have benefited from the clear ethical values in the organisation and the Council's corporate values. These have enabled colleagues from across disparate services, facing a myriad of challenges, to come together around a set of clear priorities set by the Council's GOLD command and have provided a clear framework for collaborative work, in the interests of our residents and businesses, despite the adversity and stresses of the situation.

Inclusion of the Council's Director for Legal & Governance Services in the Council's GOLD command group has ensured that legal powers and obligations are clearly defined and embedded in the governance of the Council's response.

#### **B. Ensuring openness and comprehensive stakeholder engagement**

Throughout the response to both the pandemic and cyberattack the Council has sought to sustain open and transparent communication with residents. This has used a wide range of channels, including print communications and engagement with the media to ensure that residents who are not online have access to information. This has included:

- Service status updates published on the Council website
- Regular updates via the Council's social media channels
- Updates published in print through Hackney Today and Hackney Life, and also a leaflet inserted with all Council Tax bills
- Interviews with local, regional and national media

- Internal communications, including livestreams with senior officers, and regular updates through fortnightly Silver presentations to Heads of Service and email updates
- Briefings to the Resident Liaison Group (housing)

The Council has worked closely with local partners in the statutory and voluntary sectors, including senior representatives from the health system and Metropolitan Police in the COVID-19 GOLD command group, and Metropolitan Police in Cyber GOLD.

The response to the pandemic was coordinated across London at a regional and sub-regional level, with the Council represented by the Chief Executive.

The response to the cyberattack has involved extensive coordination with the sector, national Government and regulators, including:

- Daily and weekly contact with the NCSC, NCA and MHCLG to coordinate the response and links into central Government.
- Regular updates to central Government departments, coordinated by the Cabinet Office.
- Alerts reported through *Information Security for London* - the London Warning, Advice and Reporting Point (WARP).
- Briefings to London Chief Information Officers, the Local Government Association, the local Cyber Technical Advisory Group and other sector groups.
- Briefings and meetings with the Local Government Ombudsman, Department for Work and Pensions, the Housing Ombudsman, Ofsted and the Care Quality Commission.
- Continued cooperation with the Information Commissioner's Office to support their investigation into the cyberattack.

### **C. Defining outcomes in terms of sustainable economic, social, and environmental benefits**

[The Council's Corporate Plan](#) was refreshed in 2020 to reflect the challenges presented by the COVID-19 pandemic. The priorities set out in the plan are centred on an understanding of the lived experiences of our residents, and the refresh looks at everything through the prism of inequalities, vulnerability and poverty. Support for the most vulnerable and tackling key inequalities will be embedded across 7 key priorities:

- Poverty reduction
- Building an inclusive economy
- A lasting solution to the housing crisis
- Supporting children and young people to thrive
- Enabling community wellbeing and tackle health inequalities
- Reducing harm
- Responding to the climate emergency

The cyberattack has made the task of defining outcomes and tracking progress more difficult, but not impossible. Much of the Council's performance data has been unavailable as

a result of the attack and whilst key datasets and business intelligence tools are now available, the gradual return to 'business as usual' will make it harder to identify clear points of 'pre' and 'post' cyberattack to understand the impacts on the Council's services.

#### **D. Determining the interventions necessary to optimise the achievement of the intended outcomes.**

In line with the Council's Incident Plan, the GOLD command set out clear priorities to direct the Council's response. These priorities have been kept under review to respond to changing events (eg the introduction and later step down of Shielding for people who are clinically extremely vulnerable to the COVID-19 virus).

Both the pandemic and cyberattack have had a significant and sustained impact on the capacity of Council services to deliver their intended outcomes. Considerable resources, effort and energy are being invested to sustain critical service delivery and this comes with an opportunity cost associated with delivering change and transformation.

There are, however, many examples of where the Council's services, working together with our partners, have been able to respond by redesigning business processes and creating new services to meet the needs of residents and businesses. For example:

- The emergency food service set up by the Council and partners to support people who were Shielding has continued to develop and is now providing enhanced advice, support and referral through the Here to Help service.
- The Council is providing a higher level of first contact resolution to residents accessing services and has reduced the number of enquiries handled by specialist staff as a result of services working more closely with Customer Services.
- Under dispensations made in the Coronavirus Act, Registrars were able to register deaths remotely and the service has also increased online appointment booking which wasn't possible with the Council's legacy system.
- The work to recover from the cyberattack has accelerated the delivery of the Council's planned technology strategy, which will enable further service improvements. For example, Housing services has accelerated the move away from legacy systems and introduced more customer-friendly ways of recording noise and anti social behaviour.

#### **E. Developing the Council's capacity, including the capability of its leadership and the individuals within it.**

The impact of both the pandemic and the cyberattack will continue to present significant challenges but is also accelerating the Council's capabilities in leading change, being resilient and finding creative solutions to complex challenges.

Working groups set up under the GOLD command have driven forward a comprehensive and coordinated programme of work. Aligned with the refreshed Corporate Plan these have embedded a far greater level of cross-functional working, which will continue beyond the immediate recovery work.

Coordination between officers and Members has also been enhanced through the Council's approach to the pandemic and cyberattack. This includes ways of working with the Mayor and Cabinet, and also the work of Audit Committee and Scrutiny to ensure effective oversight of the Council's response.

## **F. Managing risks and performance through robust internal control and strong public financial management.**

In line with the Council's Incident Plan, the GOLD command has provided clear oversight and leadership of the Council's response and risk management.

This is supported by a range of governance arrangements, including:

- Continued review of the Council's risk register, reporting into Audit Committee.
- Continued review of service performance by the Hackney Management Team.
- Engagement with internal and external auditors to ensure that effective arrangements remain in place, despite the disruptive impacts of the pandemic and cyberattack.
- Regular Silver meetings to ensure robust coordination across services.

## **G. Implementing good practices in transparency, reporting, and audit to deliver effective accountability.**

The Council has continued to operate its normal management, audit and scrutiny functions throughout the period since the pandemic. These have, however, been subject to some disruption due to the impacts of the urgent response to the initial lockdown and lack of access to key systems and data as a result of the cyberattack.

The Council has kept these impacts under continued review, and used tools such as the Google Workspace productivity tools (which were unaffected by the cyberattack) to ensure that continued management and audit oversight is in place.

Audit Committee and Scrutiny have defined their programmes of work to provide effective oversight. This includes a programme of thematic 'deep dive' reviews carried out by Audit Committee to explore areas of the response and future plans in greater depth.

The cyberattack has had an impact on the Council's ability to deal with statutory requests for information (Freedom of Information and Subject Access Requests) as a result of the impact on access to information held in the impacted systems. We continue to liaise with the Information Commissioner to ensure that these issues are dealt with appropriately.