

Operations Director – Digital and IT

> NHG Digital > Digital > Digital and IT Operations

What's it all about

The Operations Director – Digital and IT Operations is the single accountable executive for the safe, reliable and continuously improving operation of all live digital and IT services at Notting Hill Genesis.

The role ensures digital services are trusted in practice by staff and residents - working consistently, recovering with integrity when they fail, and improving over time through learning from lived experience. It translates NHG's Digital Vision and Mission into dependable day-to-day reality by embedding strong operational discipline across platforms, infrastructure, service management and end-user technology, reducing failure, eliminating workarounds, improving staff productivity and maintaining regulatory confidence.

How you'll make a difference

You will make a difference by ensuring that digital and IT services are stable, predictable and trusted across the organisation, particularly in moments of operational stress, service failure and regulatory scrutiny.

Your leadership will convert operational control into enterprise service confidence, reducing systemic risk, eliminating habitual workarounds and enabling staff and residents to rely on digital services as part of everyday life.

You will ensure that operational risk is actively surfaced, assessed and addressed at the right level, rather than absorbed within teams, protecting NHG's reputation, regulatory standing and service outcomes.

How you'll do it

Enterprise service operations and reliability

- Ensure robust Information Technology Infrastructure Library (ITIL) -aligned service
- Hold accountability for organisation-wide digital and IT service performance, ensuring live services operate safely, reliably and in line with regulatory and consumer expectations, across multiple platforms and service lines.

- management operates at enterprise scale, embedding clear service ownership, escalation and accountability for service outcomes.
- Hold accountability for enterprise-wide service capacity and demand sustainability, anticipating where growth, change or regulatory pressure will place future strain on live services and ensuring risks are addressed before they translate into service failure.
- Assure the executive team and regulators of sustained operational control, using assured evidence, trends and learning rather than point-in-time confidence.

Operational risk, resilience and recovery

- Define and apply clear operational risk tolerance and escalation thresholds, ensuring unacceptable risk is surfaced, understood and acted on at the appropriate executive or board level.
- Hold accountability for enterprise-level operational risk, anticipating and addressing systemic failure across platforms, dependencies and suppliers.
- Own organisation-wide resilience and recovery capability, ensuring backup and disaster recovery arrangements are realistic, tested and continuously strengthened.
- Balance performance, resilience, cost and regulatory expectations, making
- high-judgement decisions in ambiguous and high-pressure operational contexts.
- Provide assurance and escalate material operational risk early, enabling timely executive and board decision-making rather than silent risk absorption.

Platforms, infrastructure and workplace

- Lead and own the live operation of NHG's digital and IT estate, including platforms, containers, infrastructure, connectivity and end-user computing.
- Ensure lifecycle discipline, patching and vulnerability hygiene are consistently applied and runtime performance is optimised across diverse user groups, so that service degradation, capacity constraints and technical debt do not translate into resident or

- staff-visible failure or reliance on workaround.

Service management, improvement and lived experience

- Embed continuous improvement as a core enterprise operating discipline, informed by service data, incident learning and lived experience.
- Ensure staff and resident experience actively shapes operational priorities, particularly where friction indicates structural or systemic failure.
- Eliminate repeat failure, treating entrenched workarounds as organisational operational debt requiring leadership attention and investment

Commercial and supplier performance

- Hold suppliers accountable for enterprise service outcomes and value for money, using clear performance measures and trend-based insight.
- Ensure NHG retains operational control and assurance, avoiding dependency that weakens resilience, capability or regulatory confidence.
- Balance commercial performance with service risk and user impact, escalating where supplier performance threatens enterprise outcomes.

Leadership and line management

- Build and lead a high-performing senior operational leadership team, setting clear expectations for accountability, behaviour and decision-making.
- Hold leaders accountable for service outcomes, operational risk management and culture, intervening decisively where performance or behaviours fall short.
- Shape operational capability and talent across the portfolio, ensuring NHG sustains the leadership depth required for reliable services at scale.
- Direct financial resources across the digital and IT operations portfolio, ensuring budgets are aligned to service reliability, operational resilience and regulatory assurance, and that investment decisions balance cost, risk and

value for money

- Ensure that you follow and keep up to date with all relevant Notting Hill Genesis and statutory policies and related procedures including health and safety and financial regulations.
- Hybrid arrangements – at least two days in an office working with others. Depending on work and interactions required working from home may be possible one day a week.

All about you

You bring strong experience leading cyber security, information security, security operations, cyber risk, security assurance or resilience in a complex, regulated or similarly accountable environment where sensitive data, essential services, supplier dependencies and public trust all matter.

You can operate confidently between strategic risk and technical detail: able to advise senior leaders on cyber risk appetite, assurance and incident decisions, while also understanding the practical controls needed across identity, access, monitoring, vulnerability management, cloud, platforms, suppliers, integrations and live operations.

You are calm, credible and proportionate. You understand that effective cyber security is not about saying no to change; it is about enabling digital services to be designed, delivered, operated and improved safely, with clear evidence, informed risk decisions and strong accountability.

You are visible, collaborative and values-led, able to build trust with technical teams, service owners, suppliers, governance forums and senior leaders while constructively challenging practice that creates avoidable cyber, operational, data or service risk.

Our values

We succeed together

By working as one and respecting diverse perspectives, we support each other to

consistently deliver better outcomes for our residents and communities.

leading complex live services at scale.

We keep our word

We do what we say we will do, and act with integrity and ownership to build trust and provide the high-quality service people expect from us.

We do better every day

We are always looking for better ways to work and raising standards and strengthening communities through continuous improvement.

For each value, we've created example behaviours to help you understand our expectations in more detail. This role is at Leadership level.

Essential knowledge, experience and skills

Pending confirmation of legislative changes, this role may require a qualification to demonstrate competence. If not already qualified, there may be an expectation to study towards a professional qualification.

- Senior leadership experience with organisation-wide accountability for digital and IT operations in complex, regulated environments.
- Proven track record of owning service failure, recovery and resilience at enterprise scale.
- Deep understanding of service management, operational risk and assurance, and their interaction with regulatory confidence.
- Experience leading through multiple layers of management and technical leadership.
- Strong executive-level judgement and influence, particularly in ambiguous, high-pressure operational contexts.
- Advanced digital and IT literacy.
- A recognised senior leadership/management qualification or equivalent senior-level leadership experience operating at enterprise scale).
- Qualification or formal training in service management, operational risk, resilience or assurance, or equivalent experience