

Cabinet

4 August 2026

ICT Infrastructure Refresh Programme Capital Investment

Portfolio Holder: Councillor Alex Paterson, Portfolio Holder for Community Safety, Highways and Enforcement (including Digital Services).

Report from: Phil Watts, Chief Operating Officer

Author: Keith Baker, Head of Technology

Summary

This report asks Cabinet to approve a five-year capital programme to refresh Medway Council's Information and Communications Technology (ICT) infrastructure between 2026 and 2031. A significant proportion of the Council's current infrastructure is approaching or has reached end-of-life and no longer receives vendor support, security updates or patches. This creates increasing risks to service continuity, cyber security and operational resilience.

The programme covers core infrastructure including networking, cyber security, server and storage hardware, connectivity, backup and CCTV systems. The preferred approach is a phased refresh over five years to balance affordability, risk reduction and service continuity.

In preparation for Local Government Reorganisation (LGR) in 2028, the ICT service has been engaging with neighbouring borough and district councils to help ensure that infrastructure procured through this programme is interoperable, scalable and capable of being used within the future authority structure. This is intended to future-proof the Council's infrastructure and reduce the risk of duplicated investment during transition.

The current ICT infrastructure includes hardware and systems that are approaching or have reached manufacturer-declared end-of-life (EOL) status. This means they will no longer receive critical security patches, firmware updates, or vendor support. Continuing to operate these assets poses significant risks to service continuity, cybersecurity, and compliance. A refresh program is essential to maintain operational resilience, reduce vulnerability exposure, and align with modern performance and capacity requirements, especially in preparation for the demands of the LGR programme.

1. Recommendations

- 1.1. The Cabinet is asked to agree Option 2 as set out in section 7 of the report, to implement a structured enterprise ICT infrastructure programme to ensure long-term compliance, stability, and cyber resilience, in line with the National Cyber Security Centre's (NCSC's) Cyber Essentials requirements.
- 1.2. The Cabinet is requested to recommend to full Council the addition of £3,869,000 to the Capital Programme to be funded by prudential borrowing.

2. Suggested reasons for decisions

- 2.1. The programme will address key technical control areas outlined by the NCSC, including:
 - **Firewalls and boundary security:** Ensuring all internet-connected devices are protected by properly configured firewalls
 - **Secure configuration:** Replacing legacy systems with modern, securely configured hardware to reduce vulnerabilities.
 - **Access control:** Enforcing least-privilege access and identity management across the infrastructure.
 - **Malware protection:** Ensuring all endpoints and servers are protected with up-to-date anti-malware solutions.
 - **Patch management:** Refreshing hardware to support timely updates and vendor support, reducing exposure to known exploits.
 - **Security Operations Centre (SOC)** will provide 24/7 monitoring, threat detection, and incident response capabilities ensuring real-time protection of critical systems and data.
- 2.2. This investment is essential to maintain compliance with national standards, protect sensitive data, and support the Council's digital transformation and LGR program. Without this refresh, ageing infrastructure will fall short of baseline security expectations, increasing the risk of service disruption, data breaches, and regulatory non-compliance.

3. Background

- 3.1. Since 2020, Medway Council's investment in ICT infrastructure has played a pivotal role in maintaining a robust, secure, and resilient digital environment. The capital funding approved in 2020 enabled the replacement of outdated servers and network components, significantly improving system performance and ensuring compliance with evolving security standards.
- 3.2. The Council's hybrid infrastructure model anchored by resilient on-site data centres at Gun Wharf and the West Service Building has delivered 99.95% service uptime, supporting 24/7 operations across critical services. This stability has been essential in enabling staff and elected Members to work effectively, particularly during periods of increased demand and remote working.

- 3.3. Strategic upgrades to Wi-Fi, telephony, and connectivity have enhanced internal collaboration and public engagement, while the introduction of cloud-based services and contact centre tools has modernised service delivery. These improvements have also supported Medway's commitment to its residents.
- 3.4. Importantly, the infrastructure programme has underpinned the Council's ability to meet cybersecurity obligations, with investments in firewalls, encryption, and endpoint protection aligned to best practice. This has reduced risk exposure and ensured continuity of services in the face of growing cyber threats.
- 3.5. Looking ahead, the next phase of investment (2026–2031) will build on this strong foundation to address end-of-life systems and enable further innovation and compliance.

4. Strategic context

- 4.1. This ICT infrastructure refresh programme directly supports Medway Council's strategic priorities as outlined in the Council Plan, the Digital and ICT Strategy, and the Local Digital Declaration. It underpins the Council's commitment to delivering high-quality, accessible, and secure public services that meet the evolving needs of residents, businesses, and staff.
- 4.2. The refresh will:
 - **Enable digital innovation:** By modernising core infrastructure, the Council can continue to adopt new technologies that improve service delivery, support self-service, and enhance customer experience key goals of the Customer Pledge and Medway's Smart City ambitions.
 - **Support organisational transformation:** The programme provides the technical foundation for the Local Government Reorganisation (LGR), ensuring systems are scalable, interoperable, and ready for cross-authority collaboration.
 - **Maintain compliance and security:** Aligning with National Cyber Security Centre (NCSC) best practices, the refresh will ensure the Council's infrastructure meets legal, regulatory, and data protection standards, reducing risk and safeguarding public trust.
 - **Improve operational efficiency:** Replacing end-of-life systems and consolidating legacy platforms will reduce maintenance overheads, improve system performance, and support agile working across the organisation.
 - **Deliver value for money:** Strategic investment in resilient, future-proofed infrastructure will reduce long-term costs, support income generation through hosted services, and ensure continuity of critical operations.
- 4.3. This programme is essential to maintain momentum from the 2020–2025 infrastructure improvements and to position Medway Council for sustainable, secure, and citizen-focused service delivery through 2031 and beyond.

5. Case for change

- 5.1. Medway Council's ICT infrastructure has served as a stable and resilient foundation for digital service delivery since the 2020 investment programme. However, much of the core infrastructure is now approaching end-of-life (EOL), with critical components no longer supported by vendors. This presents increasing risks to service continuity, cybersecurity, and compliance with national standards.
- 5.2. The Council's strategic direction anchored in the Council Plan, the ICT Technology Strategy demands a modern, secure, and scalable infrastructure capable of supporting digital transformation, hybrid working, and the LGR programme. Without further investment, the Council risks falling behind in its ability to deliver efficient, accessible, and secure services to residents and staff.

Key drivers for change include:

- **Compliance and security:** To meet National Cyber Security Centre (NCSC) best practice, including Cyber Essentials, the Council must replace unsupported systems, improve patch management, and strengthen perimeter and endpoint defences. As part of this, the introduction of a dedicated Security Operations Centre (SOC) will provide 24/7 monitoring, threat detection, and incident response capabilities ensuring real-time protection of critical systems and data.
 - **Operational resilience:** Ageing infrastructure increases the likelihood of system failures, performance degradation, and costly emergency interventions.
 - **Digital service expectations:** Residents and businesses expect seamless, 24/7 access to services. Legacy systems limit the Council's ability to meet these expectations and integrate with modern platforms.
 - **Support for transformation:** The LGR programme and Smart City ambitions require a flexible, infrastructure that can scale and adapt to new service models.
 - **Cost efficiency:** Proactive investment in modern infrastructure reduces long-term maintenance costs, energy consumption, and reliance on legacy support contracts.
- 5.3. This business case sets out the investment required to address these challenges and ensure Medway Council remains secure, compliant, and digitally capable through 2031 and beyond.

6. Options analysis

- 6.1. **Critical Success Factors:** Specify the critical success factors for the investment proposal, i.e. the attributes essential for successful delivery, against which the options will be appraised, together with the agreed spending objectives.

Main options:

Table 1: Summary of Options Appraisals

Option	Description	Advantages	Disadvantages	Conclusion
Option 1: Do Nothing (Business as Usual)	Continue operating with existing infrastructure, replacing only when failure occurs.	- No immediate capital outlay - Minimal disruption in the short term	- High risk of service failure - non-compliance with security standards - Increased support and maintenance costs - Inability to support LGR and digital transformation	Not viable. This option exposes the Council to significant operational, financial, and reputational risk.
Option 2: Phased Refresh (Preferred Option)	Replace end-of-life infrastructure over a 5-year programme, prioritising critical systems and aligning with LGR and digital strategy.	- Maintains service continuity - Supports compliance with NCSC best practice - Enables cost avoidance (e.g. circuit consolidation) - Scalable and future-proof	- Requires sustained capital investment - Coordination needed across multiple service areas	Recommended. Balances risk, cost, and strategic alignment while enabling transformation and resilience.
Option 3: Full Refresh in Year 1	Complete infrastructure replacement in a single financial year.	- Immediate uplift in performance and security - Simplifies procurement and project management	- High upfront cost - Greater risk of disruption - Resource-intensive	Not recommended. Financially and operationally challenging; lacks flexibility and may exceed annual budget constraints.

7. Recommended option

7.1. The recommended option is Option 2.

7.2. Under Option 2: Phased Refresh, the Council will procure a range of goods and services and works over a five-year period to modernise and secure its ICT infrastructure. This phased approach allows for prioritisation of critical systems, alignment with budget cycles, and minimised disruption to services.

8. Procurement route

8.1. The procurement of ICT infrastructure for the 2026–2031 refresh programme will follow Medway Council's Contract Procedure Rules and comply fully with the Public Contracts Regulations 2015. The Council will utilise established and compliant procurement frameworks such as Crown Commercial Service (CCS) or Kent Commercial Services (KCS), which provide pre-vetted suppliers and ensure value for money, transparency, and legal compliance.

8.2. Where appropriate, mini competitions will be conducted within these frameworks to ensure competitive pricing and alignment with technical requirements. All procurement activity will be supported by the Council's Procurement and Legal teams to ensure due diligence, risk mitigation, and adherence to internal governance processes.

8.3. This approach ensures that the Council meets its statutory obligations, achieves best value, and maintains auditability and accountability throughout the procurement lifecycle.

8.4. Under the recommended Option 2, the Council will procure a phased set of goods, services, and works over a five-year period to modernise and secure its ICT infrastructure. This approach ensures continuity of service, aligns with budget cycles, and supports strategic transformation goals.

8.5. **Good**

- Replacement server and storage hardware for data centres.
- Core, distribution, and edge network switches to replace end-of-life Brocade infrastructure.
- Next-generation firewalls, Fortimail gateways, and Forti Sandbox appliances.
- Wi-Fi 7 access points and controllers.
- CCTV cameras and NVRs to replace legacy surveillance systems.
- End-user computing devices and accessories where applicable.

8.6. **Services**

- Design, configuration, and installation of all infrastructure components.
- Security Operations Centre (SOC) services for 24/7 threat monitoring and response.
- Network redesign and KPSN circuit consolidation consultancy.
- Ongoing support, maintenance, and vendor-backed warranties.

8.7. **Works**

- Data centre upgrades (e.g. flooring, power, cooling, access control).
- Cabling and physical infrastructure works to support new network and CCTV deployments.

8.8. **Payment**

Procurement will be staged across the five-year programme, with capital (CAPEX) and revenue (OPEX) funding allocated annually. Payments will be structured around key delivery milestones, such as hardware delivery, installation, and go-live. Multi-year support contracts and SOC services will be funded through revenue budgets, with options for renewal based on performance and operational need.

- 8.9. This structured approach ensures affordability, compliance with procurement regulations, and alignment with the Council's strategic and operational priorities.
- 8.10. To ensure value for money and reduce financial and delivery risk, the following payment mechanisms will be applied:
- 8.11. **Milestone-based payments:** Major infrastructure components (e.g. servers, switches, firewalls) will be paid for in stages, such as upon delivery, successful installation, and completion of testing. This ensures suppliers meet agreed technical and operational standards before full payment is released.
- 8.12. **Performance-linked payments:** For services such as the Security Operations Centre (SOC), payments will be tied to service level agreements (SLAs), including availability, response times, and incident resolution metrics.
- 8.13. **Usage-based or subscription models:** Where applicable (e.g. cloud services, licensing, or support contracts), payments will be structured as annual or monthly subscriptions, allowing flexibility and scalability.
- 8.14. **Retention and warranty clauses:** A portion of payment for works (e.g. network refresh) may be retained until post-installation validation is complete, ensuring defects are addressed promptly.
- 8.15. These mechanisms will be embedded in supplier contracts to ensure accountability, reduce the risk of non-performance, and align payments with tangible outcomes. All procurement and payment processes will comply with Medway Council's financial regulations and public procurement law.
- 8.16. Where possible, the Council will utilise pre-approved public sector frameworks such as Crown Commercial Service (CCS), Kent Commercial Services (KCS), or G-Cloud. These frameworks offer standardised contract templates that are compliant with the Public Contracts Regulations 2015 and ensure value for money, transparency, and legal robustness.
- 8.17. For more complex or bespoke elements such as Security Operations Centre (SOC) services, data centre works, or multi-year support agreements—a bespoke contract may be required. These will be developed in consultation with the Council's Legal and Procurement teams to ensure they include

appropriate clauses for service levels, performance metrics, data protection, and risk allocation.

- 8.18. All contracts will include clear deliverables, payment milestones, and termination clauses to protect the Council's interests and ensure accountability throughout the programme lifecycle.

9. Funding and affordability

- 9.1. Table 2: Cost and funding of the recommended option - Please see Appendices A - ICT Capital Strategy 2026 to 2031 attached. Due to LGR we will be only seeking Capital borrowing to support the program of works for years 2026 to 2028.
- 9.2. ICT to identify savings to support the £82,000 interest costs for 2026/27 and review budgets for 2027/28 to cover the interest costs for 2027/28.

10. Delivery arrangements

- 10.1. To ensure the successful delivery of the ICT Infrastructure Refresh Programme (2026–2031), Medway Council will implement a robust governance and delivery framework, incorporating best practices in project management, assurance, and risk control.

10.2. Project Management Arrangements

- **Standards:** The programme will follow PRINCE2 and MSP (Managing Successful Programmes) methodologies, aligned with the Council's internal project governance framework.
- **Governance:** A dedicated Programme Board will oversee delivery, chaired by the Head of Technology and including representatives from Finance, Procurement, Legal, and key service areas.
- **Roles and Responsibilities:**
 - **Programme Sponsor:** Director of BSD.
 - **Programme Manager:** Head of Technology.
 - **Project Managers:** Assigned per workstream (e.g. Network, Security, Data Centre).
 - **Technical Leads:** Responsible for solution design and implementation oversight.
 - **Procurement & Legal:** Ensure compliance with public procurement law and internal procedures.

10.3. Project Assurance

- Independent assurance reviews will be conducted at key stages:
- **Gateway Reviews:** At initiation, procurement, implementation, and closure
- **Internal Audit:** Periodic audits to ensure compliance and value for money
- **External Review:** Optional peer review or consultancy-led assurance for high-risk components (e.g. SOC implementation).

10.4. **Change Management**

- A structured change management plan will be developed to:
- Communicate changes to stakeholders.
- Provide training and support for staff impacted by new systems.
- Ensure smooth transition from legacy to modern infrastructure.
- The Council's Organisational Development team will support cultural and behavioural change where required.

10.5. **Benefits Realisation**

- A Benefits Register will be maintained and monitored throughout the programme.
- Key benefits include:
- Improved cybersecurity and compliance
- Reduced operational risk and downtime
- Cost avoidance through circuit consolidation and support savings
- Enhanced service delivery and user experience
- Benefits will be tracked against KPIs and reported to the Programme Board quarterly.

10.6. **Risk Management**

- A comprehensive Risk Register will be maintained, with risks assessed by likelihood and impact.
- Key risks include:
 - Supply chain delays.
 - Budget overruns.
 - Integration issues with legacy systems.
 - Cybersecurity threats during transition.
- Mitigation strategies include:
 - Supplier performance clauses.
 - Contingency budgets.
 - Phased implementation to reduce exposure.
 - Enhanced monitoring during cutover periods.

10.7. **Contract Management**

- All contracts will include:
- Clear deliverables and milestones.
- SLAs and performance metrics.
- Retention clauses and warranty periods.
- Contract managers will be assigned to each major supplier, supported by Legal and Procurement teams.

10.8. **Post-Evaluation and Review**

- A Post-Implementation Review (PIR) will be conducted within 6 months of programme completion (target: Q3 2031).
- Evaluation will assess:
 - Achievement of objectives.
 - Realisation of benefits.
 - Lessons learned for future programmes.

10.9. **Contingency Plan**

- A contingency reserve (financial and operational) will be maintained to address:
 - Unexpected hardware failures.
 - Supplier non-performance.
 - Emerging security threats.
 - Critical systems will be prioritised for early refresh to reduce risk exposure.

11. **Advice and analysis**

11.1. **Strategic Advice and Rationale**

Following the delivery arrangements outlined in the previous section, it is strongly advised that Medway Council proceed with the recommended Phased Refresh approach. This strategy balances operational continuity, financial sustainability, and strategic alignment with the Council's digital transformation goals and Local Government Reorganisation (LGR) programme.

The phased investment will:

- Ensure compliance with National Cyber Security Centre (NCSC) standards.
- Reduce the risk of service disruption due to ageing infrastructure.
- Enable the Council to adopt modern, scalable, and secure technologies.
- Support hybrid working, smart city initiatives, and improved public service delivery.

11.2. **Sustainability Implications**

The ICT refresh programme supports the Council's climate commitments by:

- Replacing legacy hardware with energy-efficient alternatives, reducing power and cooling demands in data centres.
- Consolidating infrastructure (e.g. through KPSN circuit rationalisation), which reduces the environmental footprint of duplicated systems.
- Enabling remote and hybrid working, which contributes to reduced travel emissions and office space usage.

Procurement specifications will include sustainability criteria, such as:

- Vendor commitments to carbon neutrality.
- Equipment with low power consumption and recyclable components.
- Use of cloud services where appropriate to reduce on-premises energy use.

11.3. **Diversity Impact Assessment (DIA)**

A Diversity Impact Assessment (DIA) will be completed to assess the implications of the ICT refresh on service accessibility and inclusion. Preliminary considerations include:

- **Digital Inclusion:** Upgraded infrastructure will improve access to online services for all residents, including those with disabilities or limited digital literacy.
- **Workforce Accessibility:** Enhanced Wi-Fi and end-user computing will support flexible working arrangements, benefiting staff with caring responsibilities or accessibility needs.
- **Public Safety:** Modernised CCTV systems will enhance community safety, particularly in vulnerable areas.

12. Risk management

12.1. Risk management is an integral part of good governance. The Council has a responsibility to identify and manage threats and risks to achieve its strategic objectives and enhance the value of services it provides to the community. The following table outlines the key risks associated with the ICT Infrastructure Refresh Programme (2026–2031), along with mitigation actions and risk ratings.

Risk	Description	Action to Avoid or Mitigate Risk	Risk Rating
Supply Chain Delays	Delays in hardware delivery due to global shortages or vendor issues	Use multiple suppliers; procure early; include delivery clauses in contracts	B2
Budget Overruns	Costs exceed estimates due to inflation or unforeseen technical requirements	Include contingency in budget; conduct regular financial reviews	B3
Integration Issues	New systems may not integrate smoothly with legacy applications	Conduct compatibility assessments; phased implementation; vendor support	C2
Cybersecurity Threats During Transition	Increased vulnerability during infrastructure migration	Enhanced monitoring; SOC oversight; staged cutovers with rollback plans	B1
Resource Constraints	Limited internal capacity to manage concurrent projects	Use external consultants; prioritise critical systems; stagger timelines	C3
Stakeholder Resistance	Resistance to change from staff or service areas	Early engagement; clear communication; training and support	C4

For risk rating, please refer to the following table:

Likelihood	Impact:
A Very likely	1 Critical
B Likely	2 Major
C Unlikely	3 Moderate
D Rare	4 Minor

13. Climate change implications

13.1. Context

Medway Council declared a climate change emergency in April 2019 (item 1038D) and has committed to achieving carbon neutrality by 2050. All Council officers are expected to consider the environmental impact of their services and identify opportunities to reduce carbon emissions.

13.2. Implications of the ICT Infrastructure Refresh Programme

Climate change implications, including:

- **Energy Efficiency:** Replacing legacy servers, switches, and storage systems with modern, energy-efficient hardware will significantly reduce power consumption in Council data centres.
- **Reduced Cooling Requirements:** New infrastructure will generate less heat, lowering the demand for air conditioning and associated energy use.
- **Cloud Adoption:** Where appropriate, the programme will leverage cloud services, which often operate in optimised, carbon-efficient environments.
- **Remote Working Enablement:** Enhanced Wi-Fi and network infrastructure will support hybrid working, reducing commuting and associated emissions.
- **Circuit Consolidation:** Rationalising KPSN circuits will reduce the physical infrastructure footprint and associated energy use.

13.3. Mitigation and Monitoring

Procurement specifications will include sustainability criteria such as:

- Equipment with low power usage effectiveness (PUE)
- Vendor commitments to carbon neutrality and recycling schemes
- Lifecycle assessments and end-of-life recycling plans

13.4. The programme will monitor energy usage before and after implementation to quantify carbon savings and support the Council's broader sustainability reporting.

14. Financial implications

14.1. Summary of Costs and Funding

The ICT Infrastructure Refresh Programme (2026–2031) represents a significant capital investment to modernise Medway Council's digital infrastructure. The total estimated capital requirement over the five-year period exceeds £3.5 million, covering networking, cybersecurity, data centre hardware, and smart infrastructure upgrades.

Funding Source

- All components of the programme will be funded through **borrowing**, in line with the Council's capital financing strategy.

- Some elements, such as the Security Operations Centre (SOC) and KPSN circuit consolidation, are expected to deliver **ongoing revenue savings**, helping offset operational costs.

Key Investment Areas

- **Networking and Firewalling:** £375,000+
- **LAN and Wi-Fi Refresh:** £1,350,000+
- **Security Operations Centre (SOC):** £580,000
- **Server and Storage Hardware:** £1,484,000+
- **CCTV and Smart Infrastructure:** £150,000
- **Backup and Resilience Solutions:** £520,000

14.2. Financial Governance

- The programme will be delivered in **phases**, with annual capital allocations aligned to budget cycles.
- Payments will be structured around **milestones**, ensuring value for money and accountability.
- Multi-year support contracts will be funded through **revenue budgets**, with performance-based renewal options.
- Final finance clearance will be sought from the Council's Finance Manager, following consultation with service accountants to ensure affordability and compliance with financial regulations.

15. Legal implications

15.1. Statutory and Constitutional Powers

The proposed ICT Infrastructure Refresh Programme (2026–2031) falls within the Council's general powers of competence under the Localism Act 2011, which enables local authorities to do anything that individuals generally may do, provided it is not prohibited by legislation. The procurement and implementation of ICT infrastructure also align with the Council's statutory duties to ensure secure, efficient, and resilient service delivery, particularly in relation to data protection, cybersecurity, and public service continuity.

15.2. Procurement and Contractual Compliance

All procurement activities associated with this programme will be conducted in accordance with the Public Contracts Regulations 2015 and the Council's Contract Procedure Rules. The use of established frameworks such as Crown Commercial Service (CCS), Kent Commercial Services (KCS), and G-Cloud ensures compliance with legal requirements, transparency, and value for money.

Where bespoke contracts are required (e.g. for Security Operations Centre services or data centre works), these will be developed in consultation with Legal Services to ensure appropriate clauses are included for:

- Data protection and information governance

- Service level agreements (SLAs)
- Performance monitoring and enforcement
- Termination and dispute resolution

15.3. **Data Protection and Cybersecurity**

The programme includes investment in systems and services that support the Council's compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Legal Services will review all relevant contracts and data processing arrangements to ensure appropriate safeguards are in place, particularly for cloud-based services and third-party support providers.

Lead officer contact

Keith Baker, Head of Technology, keith.baker@medway.gov.uk.

Appendices

Appendix A - ICT Capital Strategy 2026 to 2031

Background papers

None