OUTLINE STRATEGIC BUSINESS CASE

Directorate	**Corporate Services**
Scheme Name	**ICT systems upgrades & server replacements**
Budget Holder	**- Director Resources**

Project aims and objectives:

The five elements of this capital bid will support the Council with its Digital Data & Technology strategy 2024 – 2028 & planning towards digital transformation by providing a stable, modern and fit for purpose infrastructure.

Procurement will be through an approved Local Government Procurement Framework (CCS or similar) to ensure that best value is demonstrated.

Commissioning and migration activity will be carried out by the Councils contracted IT provider – Hoople Ltd and a third party to provide consultancy and professional serves to complete the migration works.

Key deliverables-

1.The update of key Software which provides the GIS services for the Council.

This project is to update ageing GIS Software with the latest version which will ensure manufacturer support and is up to date to allow security and operational integrity to be maintained, in line with emerging vulnerabilities and Cyber Security threats.

The aim of the project is as follows:

- Replace ageing software which is required to run the time services for key line of business systems, with supported 'in life' equipment which is actively supported by the supplier for cyber security/vulnerability patches.
- Provide support and maintenance contract with the manufacturer or partner for a period of five years.
- Migrate services from the aging version of the software to a newer version which is supported.

2.Introduction of a Security Incident and Event Monitoring (SIEM) solution into the council

The primary objective for the project is to support the council's requirements to operate IT solutions in a secure manner protecting the Confidentiality, Integrity and Availability of the Councils data and service delivery. The authority is obliged to ensure that the underlying infrastructure is secure and that the systems hosting environment is maintained securely. Infrastructure must not be vulnerable to common cyber- attacks and this should be maintained through secure configuration and software patching.
This project is to introduce a SIEM solution which will safeguard the council data, systems, and services from increasing cyber threats. In June 2024, an ICT Security Assurance Framework Review was conducted by our Auditors – SAFR – who reported in their Findings & Risk Assessment that
"There is no Security Incident and Event Monitoring (SIEM) solution and no alternative central logging system in place, as such this potentially creates unnecessary difficulty in monitoring security logs. it is considered best practice to implement a SIEM or equivalent solution for security monitoring purposes".

Within the section "Our Ambition - Cyber security" in the Councils Digital Data & Technology strategy 2024 – 2028 it states:
"There is a high and increasing threat to cyber-security, requiring investment in security and privacy measures to protect data and the services we provide. We will continue to use the latest technology for device security and management" – Introduction of an SIEM solution would meet the level of ambition stated.

The aim of the project is as follows:

- To plug the gap identified by the ICT Security Assurance Framework Review to introduce a centralised monitoring system that provides real-time visibility into security events across the council's IT environment.
- This will Improve the council's ability to detect, analyse, and respond to security incidents in real-time, reducing the risk of data breaches and service disruptions.
- Centralize and automate security event monitoring to enhance efficiency and accuracy.
- Ensure compliance with relevant cybersecurity regulations and standards.
- Implement a SIEM solution capable of real-time log collection, correlation, and analysis across all council IT systems.
- Reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents.
- Establish automated reporting and alerting mechanisms to meet compliance requirements.

This will support the Council with its Digital Data & Technology strategy 2024 – 2028 & planning towards digital transformation by providing a stable, modern and fit for purpose infrastructure, enabling the flexibility required to adapt to changing service delivery models throughout the short to medium term (i.e. the initial life of the solution - 5 years). Also, this will aid to counteract the potential for significant financial, reputational, and operational damage due to undetected security breaches. Implementing a SIEM will demonstrate a proactive approach to cybersecurity, thereby enhancing the council's reputation and public confidence.

3.Replacement of Key IT Hardware which provides the CCTV Case Management solution for the Council.

The primary objective for the project is to support the council's requirements to operate IT solutions in a secure manner protecting the Confidentiality, Integrity and Availability of the Councils data and service delivery. The authority is obliged to ensure that the underlying infrastructure is secure and that the systems hosting environment is maintained securely. Infrastructure must not be vulnerable to common cyber-attacks and this should be maintained through secure configuration and software patching.
This project is to replace a system which is running on an operating system which will be unsupported from October 2025. This will allow the system to run on an operating system where security and operational integrity can be maintained, in line with emerging vulnerabilities and Cyber Security threats.

The aim of the project is as follows:

- Replace an ageing solution which provides key line of business systems for the corporate CCTV service, with a supported 'in life' solution which is actively supported by the supplier for the next 5 years.
- Support the Councils obligations to remove end of life operating systems from the environment in line with its security and compliance obligations – Windows 10.
- Migrate services from existing equipment to new supported environment.
- Decommission and dispose of outgoing environment in line with the authorities' security and environmental policies and obligations.

This will support the Council with its Digital Data & Technology strategy 2024 – 2028 & planning towards digital transformation by providing a stable, modern and fit for purpose infrastructure, enabling the flexibility required to adapt to changing service delivery models throughout the short to medium term (i.e. the initial life of the equipment - 5 years).

4. The update of Civica Software.

We are in the process of completely replacing our Planning & Regulatory Software – Civica – as part of a separate project with a completion date of March 2026.

However, there is a residual risk that we may need to upgrade our current version of Civica to v8.10 or higher – the anticipated release date for this is October 2025. This potential software upgrade may be required so the Council's Planning and Regulatory system is compliant with food safety requirements and/or regulatory requirements that may come into force prior to Civica being replaced in March 2026.

It's very likely that we may not need to spend the capital requested, but we feel it's prudent to register this potential expenditure as a Capital Bid.

5. Investment in ICT systems with Artificial Intelligence (AI) capabilities

In line with the council's Digital Data and Technology Strategy 2024 – 2028, we have pledged to consider the introduction of AI opportunities to support our staff to deliver services to our communities. AI can significantly enhance efficiency in public services by automating routine tasks which will in turn free up staff to focus on more complex issues. By leveraging AI, we can not only streamline operations but also deliver more responsive and personalized services to our constituents.

We have written an AI usage policy and set up an AI Ethics board to support the introduction of AI into the Council.

6. Migrating Data into M365 Cloud

Migrating data into the Microsoft 365 (M365) Cloud offers numerous benefits for the council. This piece of work will enhance data security with advanced encryption and compliance features, ensuring sensitive information is well-protected. Additionally, M365 provides improved collaboration tools, enabling council staff to work more efficiently and effectively. The cloud-based platform also offers cost savings by reducing the need for on-premises infrastructure and maintenance.

Estimated costs and funding sources:

	2025/26	2026/27	2027/28	Future Years	Total
	£'000	£'000	£'000	£'000	£'000
Capital cost of project					
Upgrade of GIS service software	65				65
SIEM solution Hoople	32				32
CCTV systems hardware replacement	20				20
Upgrade of Civica software	65				65
ICT systems with AI capabilities	151				151
Contingency	68				68
Migrating Data into M365 Cloud	99				99
TOTAL	**500**				**500**
Funding sources					
Corporate Funded Borrowing	500				500
TOTAL	**500**				**500**
Revenue budget implications					
SIEM solution Hoople	68	68	68	68	272
Supplier support for the CCTV systems hardware	-	1.6	1.7	1.8	5.1
TOTAL	**68**	**69.6**	**69.7**	**69.8**	**277.1**

***Revenue implications associated with ICT systems with AI opportunities will need to be assessed as projects come forward**

Benefits and risks:

The anticipated benefits and risks of the proposed project plus risks of not going ahead with the scheme.

Supported 'in life' equipment will provide:

- Continued Cyber Security protection through manufacturer support for vulnerabilities (i.e. loss of data or disruption to service through Ransomware, Malware & Virus exploitation)
- Continued feature support through manufacturer software development. Potential for cost avoidance associated with exploitation of advances in technology.
- Reduces risk for potential loss of Confidentiality, Integrity and Availability of Council key Data due to Cyber Attack or Catastrophic Hardware Failure.
- Protects the Council's Data and Service Delivery obligations through fit for purpose equipment.
- Additional overhead to support future data growth/transformation in line with current planning.
- By updating this software, we reduce the risk of not being compliant with civil contingencies and PSN.

- Increased Public Trust: Demonstrating a proactive approach to cybersecurity, thereby enhancing the council's reputation and public confidence.
- Operational Resilience: Enhanced ability to maintain uninterrupted public services even in the face of cyber threats.
- Continued hardware failure protection through manufacturer support for parts and components (i.e. loss of data or disruption to service through catastrophic hardware or component failure)
- Provides operational efficiencies with opportunity for reduced power consumption & improved performance due to technology advancement in modern solutions.
- By upgrading this software we can move away from an unsupported solution.
- If food safety requirements change or new regulatory requirements come into force, the Council will have compliant Civica software installed to fulfil this criteria. By updating this software, we reduce the risk of not being compliant with civil contingencies and PSN.

Risks

Non-compliant software would put the Council in a position where they are not following legislative requirements