Cabinet

July 8th 2026

Public

Cyber Strategy Report

Cabinet Member:	Councillor Alex Wagner
Lead Director:	Sam Williams – Service Director
Service Area:	Enabling Services
Report Author	David Baker – Head of Service for Automation & Technology
Officer contact details	01743 254 118 – David.Baker@shropshire.gov.uk
Electoral Divisions Affected	N/A
Key Decision?	Non-Key
Cabinet Forward Plan	May 21st 2026
Report considered by	

1. Purpose of Report

Shropshire Council is operating in an increasingly complex and high-risk digital environment. As reliance on digital systems, data and cloud-based services grows, so too does the scale and sophistication of cyber threats facing the organisation. The United Kingdom is currently in a heightened state of cyber threat, reinforcing the need for strong, resilient and well-governed cyber capabilities across the public sector. Cyber security is no longer a technical concern, it is a fundamental enabler of safe, reliable and sustainable public services.

The Cyber Strategy 2026–2030 sets out a clear, outcomes-focused approach to strengthening the Council's cyber resilience. It establishes cyber security as a

corporate risk, embedding security by design, improving governance and assurance, and building a confident workforce capable of operating securely in a modern, digital environment.

Through a structured, risk-led and evidence-based approach aligned to national frameworks including the Cyber Assessment Framework (CAF), the strategy defines how the Council will protect critical services, safeguard sensitive data and ensure it can anticipate, withstand and recover from cyber incidents with minimal disruption.

2. Recommendations

1. Cabinet is asked to Approves the Cyber Strategy 2026-2030 in appendix 1, and the Plan on a Page Cyber Strategy 2026-2030 in appendix 2.

2. Delegate authority to the Service Director Enabling and Head of Automation and Technology in consultation with the Portfolio holder for Transformation and Economic Growth to update the strategy annually aligned with any legislation change and best practice.

3. Background

1. Shropshire Council is operating in a context of increasing demand for services, sustained financial pressure and rising expectations from residents for accessible, reliable and modern public services. At the same time, the Council is becoming increasingly dependent on digital systems, data and technology to deliver critical services, including care, safeguarding, finance and customer operations

2. The cyber threat landscape facing local government has intensified significantly in both scale and sophistication, with the United Kingdom in a heightened state of security against cyber threat. Local authorities are a recognised target for cyber-attacks due to the critical nature of the services they provide and the volume of sensitive data they hold. As digital transformation accelerates and reliance on cloud platforms, automation and integrated systems increases, the potential impact of cyber incidents on service delivery, financial stability and public trust continues to grow.

3. The Council's Digital Strategy 2026–2030 establishes a clear direction for transforming services through digital, data and automation. Cyber security is a fundamental enabler of this transformation. Without strong, resilient and well-governed cyber capabilities, the Council cannot modernise services safely, share data effectively with partners or adopt new technologies with confidence. The Cyber Strategy 2026–2030 has therefore been developed to ensure that digital transformation is delivered securely, resiliently and in a way that protects critical services and data.

4. The Cyber Strategy 2026–2030 sets out a structured and risk-led approach to strengthening the Council's cyber resilience. It is not a technical strategy or a compliance exercise, but a corporate, leadership-led framework that positions cyber

security as a core organisational risk and capability. The strategy aligns with national policy and best practice, including the UK Government Cyber Security Strategy 2022–2030 and the Cyber Assessment Framework (CAF), ensuring the Council meets increasing expectations for assurance, governance and transparency.

5. At its core, the strategy focuses on protecting what matters most, ensuring that critical public services remain available, reliable and safe, and that sensitive data is protected as a public trust. It recognises that cyber security is not solely a technical issue but a shared responsibility across the organisation, requiring strong leadership, clear accountability and a workforce that is confident and capable of operating securely in a modern, digital environment.

6. The strategy is underpinned by a clear vision of “trust-driven, resilience-built”, supported by guiding principles including secure-by-design technology, people-powered security, risk-led decision making and collective defence. These principles ensure that cyber security is embedded into everyday operations, decision-making and service delivery, rather than applied as a separate or reactive control.

7. Delivery of the strategy is organised around six strategic priorities: secure-by-design foundations, governance and assurance, protection of data and critical services, workforce capability, strengthened detection and recovery, and national collaboration. Together, these priorities establish a coherent and structured approach to improving cyber resilience over time, balancing prevention, protection, detection and response in line with the Council’s risk profile.

8. Governance and delivery will be embedded within the Council’s existing digital and technology operating model, ensuring cyber security is integrated into all major programmes, projects and service change. Cyber risk will be managed as a corporate risk within established governance structures, with clear oversight, accountability and assurance at all levels of the organisation.

9. A strong emphasis is placed on evidence-based assurance and continuous improvement. Progress will be measured through Cyber Assessment Framework maturity, independent assurance activity and risk trend analysis, ensuring that leadership has a clear and defensible understanding of cyber risk and resilience over time.

10. Overall, the Cyber Strategy 2026–2030 provides a clear, disciplined and forward-looking framework for how Shropshire Council will strengthen cyber resilience as a core enabler of safe, sustainable and modern public services. It ensures that the Council can operate with confidence in an increasingly complex threat environment, protect its communities and maintain the trust placed in it by residents, partners and regulators.

4. Summary of Main Proposals

1. Shropshire Council is operating in an environment of increasing digital dependency, heightened cyber threat and sustained financial pressure.

Strengthening cyber resilience is therefore essential to ensuring the safe, reliable and sustainable delivery of critical public services, and to maintaining the trust and confidence of residents, partners and regulators.

2. The Cyber Strategy 2026–2030 provides a clear, structured and risk-led approach to managing cyber security as a corporate capability. It establishes strong governance, accountability and assurance, ensuring that cyber risk is understood, prioritised and managed effectively across the organisation. The strategy positions cyber security as a key enabler of the Council's digital transformation and long-term financial sustainability.

3. Approval of the strategy will establish a clear and consistent approach to protecting critical services, safeguarding sensitive data and strengthening organisational resilience. It ensures that cyber security is embedded by design into all digital and service change, enabling the Council to operate confidently in an increasingly complex threat environment.

4. The strategy will operate on a four-year cycle, with regular review to reflect changes in threat, regulation, technology and organisational priorities. Cabinet is therefore recommended to approve the Cyber Strategy 2026–2030 and endorse its implementation as a key component of the Council's overall improvement, risk management and financial resilience programme.

5. Key risks and Opportunities

1. Protection of critical public services.

2. Strengthening cyber resilience ensures that essential services, including care, safeguarding and finance, remain available, reliable and safe, even in the face of cyber incidents

3. Reduced financial exposure and unplanned cost.

4. A proactive, risk-led approach reduces the likelihood and impact of cyber incidents, avoiding significant unplanned expenditure associated with service disruption, recovery and regulatory response.

5. Enabling safe digital transformation.

6. Embedding secure-by-design principles enables the Council to modernise services, adopt cloud platforms and scale automation confidently, ensuring transformation reduces rather than increases organisational risk.

7. Strengthened governance, assurance and audit position.

8. Adoption of the Cyber Assessment Framework (CAF) and clear governance arrangements provides structured assurance, transparency and defensibility in managing cyber risk at a corporate level.

9. Improved workforce capability and culture.

10. Investment in cyber awareness and secure ways of working reduces reliance on individual vigilance alone and embeds secure behaviour as standard practice across the organisation.

11. Enhanced protection of sensitive data and public trust.
12. A consistent, organisation-wide approach to cyber security strengthens the protection of personal and sensitive data, maintaining trust and confidence from residents, partners and regulators.

13. Stronger sector collaboration and collective defence.

14. Active participation in national initiatives, including “Defend as One”, enables shared learning, improved threat intelligence and a stronger collective defence across local government.

15. The risks associated with delivery of the Cyber Strategy are cross-cutting and align to multiple risks within the Council’s Strategic Risk Register. They contribute to:

16. The risk of failure to protect systems, services and data from cyber-attack, given increasing dependency on digital systems

17. The risk of service disruption impacting vulnerable residents and critical public services

18. The risk of financial instability arising from unplanned cyber incidents and recovery costs

19. The risk of failure to meet national expectations, regulatory requirements and audit standards for cyber resilience

20. The risk of insufficient organisational capability, including workforce behaviour and leadership accountability

21. The risk of ineffective governance, assurance and oversight of cyber risk at a corporate level

22. Delivery of this strategy therefore represents a key mitigating response to these corporate risks, ensuring cyber security is managed as an organisational capability rather than a technical function.

Risk	Mitigation	Link to Strategic Risk
Cyber security incident resulting in service disruption or data loss	Secure-by-design approach, CAF-aligned controls, strengthened detection, response an d recovery capabilities	Failure to protect from and manage the impact of a cyber-attack on ICT systems

Failure to embed cyber security across services and workforce	Organisation-wide training, leadership accountability and integration into service delivery	Critical skills shortage impacting capability, behaviour and organisational resilience Failure to protect from and manage the impact of a cyber-attack on ICT systems
Inadequate governance, assurance or risk visibility	Adoption of CAF, clear governance structures, reporting and escalation routes	Failure to adhere to governance arrangements and risk management controls Failure to protect from and manage the impact of a cyber-attack on ICT systems
Increasing reliance on legacy systems and technical debt	Modernisation of platforms and embedding security into all technology design and change	Failure to protect systems and deliver sustainable service outcomes Failure to protect from and manage the impact of a cyber-attack on ICT systems
Insufficient detection, response and recovery capability	Strengthened monitoring, incident response planning, testing and recovery arrangements	Service disruption impacting delivery of organisational objectives Failure to protect from and manage the impact of a cyber-attack on ICT systems
Dependence on third parties and supply chain risk	Strengthened assurance, monitoring and security requirements for suppliers and partners	Failure to protect systems and data and manage third-party risk Failure to protect from and manage the impact of a cyber-attack on ICT systems
Significant financial impact arising from cyber incident, including fines, regulatory action and recovery costs	Risk-led cyber investment, strong governance and assurance, alignment to national frameworks (CAF), and strengthened prevention, detection and recovery capabilities	Inability to contain overall committed expenditure within available resources Failure to protect from and manage the impact of a cyber-attack on ICT systems

6. Financial Implications

1. Shropshire Council continues to manage unprecedented financial demands and a financial emergency was declared by Cabinet on 10 September 2025. The overall

financial position of the Council is set out in the monitoring position presented to Cabinet on a monthly basis. Significant management action has been instigated at all levels of the Council reducing spend to ensure the Council's financial survival. While all reports to Members provide the financial implications of decisions being taken, this may change as officers and/or Portfolio Holders review the overall financial situation and make decisions aligned to financial survivability. All non-essential spend will be stopped and all essential spend challenged. These actions may involve (this is not exhaustive):

- scaling down initiatives,
- changing the scope of activities,
- delaying implementation of agreed plans, or
- extending delivery timescales.

2. The Cyber Strategy 2026–2030 is a critical enabler of financial resilience. While it does not in itself commit the Council to new expenditure, it establishes a structured, risk-led framework through which cyber security investment will be prioritised, governed and delivered. This ensures that limited resources are focused on protecting critical services, data and organisational continuity in line with corporate risk priorities.

3. Investment in cyber security primarily delivers value through risk reduction, resilience and avoidance of significant unplanned costs rather than direct cashable savings. Major cyber incidents in the public sector have demonstrated the potential for substantial financial impact, including service disruption, emergency response costs, recovery expenditure, regulatory fines and long-term reputational damage.

4. All investment arising from this strategy will be subject to separate business cases and approval through the Council's financial regulations and scheme of delegation. These will define expected outcomes, including risk reduction, improved resilience and protection of critical services, with benefits validated through governance and assurance processes.

5. Delivery of the strategy is expected to reduce financial volatility by minimising the likelihood and impact of cyber incidents, protecting the Council's ability to deliver services within available resources and supporting long-term financial sustainability.

7. Climate Change, Biodiversity and Environmental Implications

1. The Cyber Strategy 2026–2030 supports the Council's environmental sustainability objectives through more efficient and resilient digital operations. This includes reducing reliance on inefficient or duplicated systems, improving infrastructure efficiency and supporting more sustainable, digitally enabled ways of working.

2. The strategy promotes the modernisation of technology platforms, including increased use of scalable, cloud-based services and secure infrastructure. These

approaches have the potential to improve energy efficiency compared to traditional on-premises systems, supported by technology providers who operate large-scale, optimised data centres with established sustainability commitments.

3. A key focus of the strategy is embedding security and resilience into digital services by design. This supports long-term sustainability by reducing the risk of disruption, avoiding inefficient recovery activity and ensuring systems operate effectively throughout their lifecycle.

4. As the primary focus of the strategy is cyber resilience rather than environmental change, direct climate impacts are expected to be indirect. Individual initiatives delivered through the strategy will be subject to appropriate appraisal, including environmental considerations where relevant, to ensure alignment with the Council's wider climate change objectives.

8. Appendices

Appendix A – Cyber Strategy 2026
Appendix B – 1 Page Cyber Strategy 2026