Shropshire Council

Cyber Strategy

2026 – 2030

A people-centred approach to cyber resilience

Foreword

Shropshire Council's ability to deliver safe, reliable and modern public services depends on a strong and resilient cyber security foundation. As threats grow in scale and sophistication, and as the council accelerates digital transformation, cyber security must sit at the heart of how we work.

This strategy outlines how we will protect our systems, our data, our people and our communities. It aligns tightly with:

- The UK Government Cyber Security Strategy 2022–2030
- The Government Cyber Action Plan
- DLUHC/MHCLG's leadership role in local government cyber assurance
- The Cyber Assessment Framework (CAF) for local government
- National initiatives including Local Digital Cyber, the Cyber Support Programme, and Defend as One
- Our own Digital Strategy 2026–2030

This is a practical and strategic roadmap. It strengthens security "by design", builds a confident workforce, modernises our technology, and ensures Shropshire Council plays a full, active role in the national effort to defend local government as one community.

Introduction

Shropshire Council stands at a critical juncture, where the demands on public services are greater than ever and the responsibility to safeguard our data has never been more pressing. The landscape in which we operate is rapidly changing, driven by advances in technology, evolving public expectations and the increasing sophistication of cyber threats. As we embrace digital transformation, our commitment to cyber security forms the backbone of this journey, ensuring that every technological advancement is matched by robust protection and resilience. This commitment extends to every corner of our organisation, from the systems that power our daily operations, to the frontline staff and communities we serve.

This strategy is not simply about technology, it is about people, trust, and the council's promise to deliver safe, reliable, and modern services for all. Our approach places as much importance on building a culture of security awareness as it does on deploying the latest technical safeguards. We recognise that cyber security is a shared responsibility, involving everyone from senior leaders to every member of staff, as well as our partners and suppliers. By fostering an environment where best practice is standard and vigilance is second nature, we aim to create a council that can anticipate, withstand, and recover from cyber incidents with minimal disruption.

By aligning with national strategy, frameworks and initiatives such as the UK Government Cyber Security Strategy 2022–2030, the Cyber Assessment Framework, Defend as One, and by forging strong partnerships with national and local bodies, we are building a future where security is embedded into every aspect of our operations. These partnerships enable us to share knowledge, access the latest support and resources, and ensure that Shropshire Council remains at the forefront of local government cyber resilience. Our goal is to protect not only our own systems and data, but also the trust and confidence of our residents, ensuring Shropshire remains a safe, secure, and thriving community in the digital age.

Sam Williams
Service Director Enabling

David Baker
Head of Service – Automation and Technology

Our Vision:

Trust-driven, Resilience-built

Our vision is simple:

"Shropshire Council will be a resilient, trusted and secure organisation, protecting residents' data, ensuring uninterrupted public services, and embedding security into every part of our digital future."

What makes this strategy different is its deliberate focus on outcomes, accountability and collective improvement rather than compliance for its own sake.

This is not a technology strategy, and it is not a checklist exercise. It is a leadership-led cyber resilience strategy that explicitly prioritises the protection of critical public services, accepts and manages residual risk transparently, and recognises that cyber security is fundamentally about people, behaviours and organisational choices.

Shropshire Council's ambition is not only to strengthen its own cyber resilience, but to act as a responsible sector partner, sharing learning, contributing to national initiatives and helping to raise cyber maturity across local government as a whole.

Our vision for cyber security is ambitious and forward-thinking, reflecting the council's unwavering dedication to safeguarding the interests of our residents, staff, and partners. We are committed to developing an organisation where resilience is built into every process, trust is continually earned through responsible stewardship of information, and robust security underpins every aspect of the council's digital transformation. By setting the highest standards for data protection and operational continuity, we aim to preserve the confidence of the communities we serve, ensuring that essential public services remain available without disruption regardless of the evolving threat landscape.

This vision is underpinned by four key pillars:

People-Powered Security

People-powered security means more than awareness, it means designing ways of working that support people to make safe decisions, especially under pressure.

Shropshire Council will focus on reducing reliance on individual vigilance alone by:

- removing unnecessary complexity and insecure workarounds
- embedding secure defaults into systems and processes
- clearly defining leadership accountability for cyber-related behaviours
- supporting staff to escalate risks early without fear of blame

Cyber security expectations will be proportionate to role, recognising the different risks faced by frontline staff, Members, managers and privileged users. Secure behaviours will be reinforced through leadership practice, operational controls and everyday processes not solely through training.

Secure-by-Design Technology

Our approach is to embed security into the very fabric of our digital infrastructure. All new systems, processes, and services are designed with security as a core component, ensuring they are modern, interoperable, and resilient to current and emerging threats. We continually assess and upgrade our technology, prioritising solutions that offer both robust protection and seamless integration into our existing operations. By adopting a secure-by-design philosophy, we strengthen our defences while enabling innovation and efficiency across the council.

Risk-Led Decisions

We make informed choices based on a thorough understanding of the risks we face, drawing on the latest threat intelligence, internal assessments, and national frameworks such as the Cyber Assessment Framework (CAF). Our decisions are guided by evidence, ensuring that our investments in cyber security deliver maximum impact and value. By proactively identifying vulnerabilities and addressing them in a structured manner, we reduce exposure and enhance our ability to withstand and recover from cyber incidents.

Collective Defence

Recognising that cyber threats do not respect organisational boundaries, we adopt a collaborative approach to defence. We work closely with the Ministry of Housing, Communities and Local Government (MHCLG), the National Cyber Security Centre (NCSC), and other local authorities to share knowledge, intelligence, and resources. Through joint initiatives such as "Defend as One," we contribute to a resilient sector-wide posture, ensuring that Shropshire Council benefits from the latest support, guidance, and innovations in cyber security.

By embedding these principles into the heart of our strategy, Shropshire Council is committed to delivering safe, reliable, and modern digital services. Our vision is not just about technology, it is about building trust, empowering people, and establishing a culture of security that enables our community to thrive securely in the digital age.

Why We Must Change

Shropshire Council is operating in an environment of increasing demand, constrained finances, heightened public scrutiny and accelerating digital change. At the same time, the cyber threat landscape facing local government has intensified significantly, both in scale and sophistication. Against this backdrop, cyber security can no longer be treated as a technical concern or an ICT issue alone. It is now a fundamental enabler of safe, resilient and sustainable public services.

The council is undergoing significant digital transformation to modernise services, improve outcomes for residents, and achieve long-term financial sustainability. This transformation increases our reliance on digital systems, data, automation, cloud platforms and external partners. Without a corresponding step-change in cyber resilience, this reliance materially increases organisational risk. In short, we cannot deliver digital transformation safely at pace using our current cyber operating model.

Cyber security is therefore not about preventing change; it is about enabling the council to change with confidence.

Financial and Operational Pressures

Like all councils, Shropshire faces sustained financial pressure, rising demand for services and limited capacity to absorb disruption. Major cyber incidents across the public sector have demonstrated that the financial impact of cyber failure extends far beyond recovery costs. Disruption to services, loss of data, emergency procurement, reputational damage and regulatory intervention can result in multi-million-pound impacts and long-term operational harm.

In an environment where unplanned spend undermines financial recovery, preventing avoidable cyber incidents is a financial imperative, not an optional enhancement.

Rising Digital Dependency

The council increasingly relies on digital platforms to deliver critical services, including health and social care, safeguarding, democratic services, finance, and workforce operations. These systems underpin day-to-day service delivery and the safety of some of the most vulnerable people in Shropshire.

As the council modernises legacy systems, migrates services to the cloud, expands automation and explores the responsible use of AI, the attack surface continues to grow. Without stronger, more consistent cyber controls embedded by design, this creates unacceptable exposure to service disruption and data compromise.

Changing Threat Landscape

Local government is now a recognised target for organised crime groups, opportunistic attackers and, increasingly, state-linked threat actors. The sector holds large volumes of sensitive personal data, relies on complex supply chains, and delivers services where disruption has immediate real-world consequences.

National evidence shows a clear rise in the frequency and impact of cyber incidents affecting councils. The UK Government has responded by strengthening expectations around cyber assurance, including the adoption of the Cyber Assessment Framework (CAF) for local government. The direction of travel is clear: higher assurance, greater transparency, and stronger accountability.

Workforce Capability and Behaviour

Technology alone will not deliver cyber resilience. Human behaviour remains one of the most significant risk factors in cyber incidents, whether through phishing, weak practices, or insecure workarounds driven by operational pressure.

As the council adopts new tools, platforms and ways of working, staff and Members must be supported to work securely and confidently. Cyber security must become part of everyday practice across the organisation, not a specialist activity carried out in isolation. This requires a sustained focus on skills, culture and leadership, not just controls and policies.

Governance, Assurance and Accountability

Cyber security is now a corporate risk, not an ICT sub-risk. National bodies, auditors and regulators increasingly expect councils to demonstrate clear ownership, structured assurance and evidence-based decision-making in relation to cyber resilience.

Continuing with fragmented or implicit approaches to governance increases exposure to audit challenge and regulatory intervention. Adopting the Cyber Assessment Framework as our primary assurance model, strengthening oversight, and embedding cyber risk into organisational governance are essential to meeting these expectations and maintaining trust.

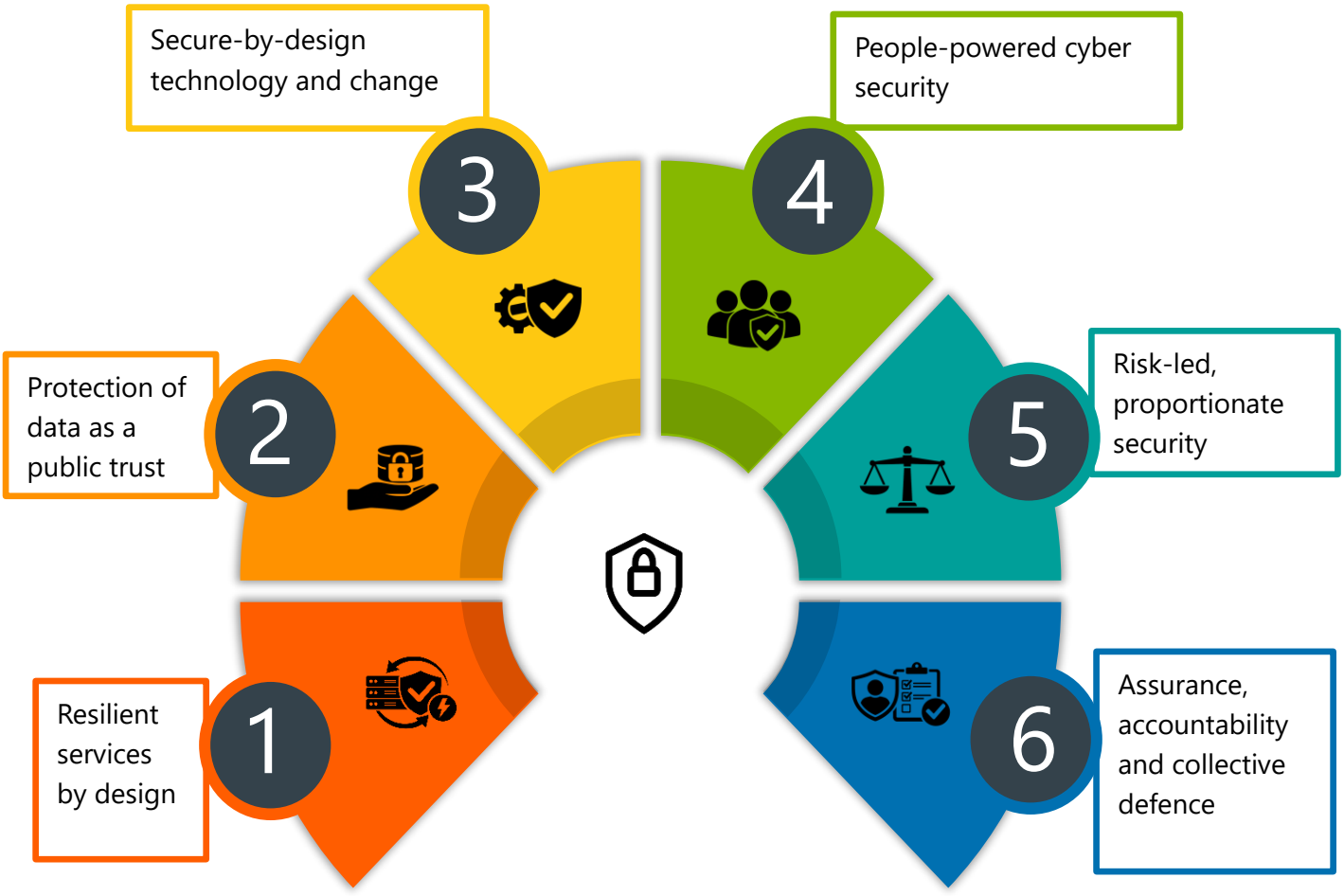
Enabling Safe and Sustainable Transformation

Ultimately, cyber security is not a barrier to innovation, it is what makes innovation possible. Without secure, resilient foundations, the council cannot move faster, automate services, share data safely with partners or adopt new technologies responsibly.

This strategy responds to that reality. It sets out how Shropshire Council will strengthen cyber resilience as a core enabler of digital transformation, protect critical services and data, and ensure the organisation can modernise with confidence in a rapidly evolving threat environment.

Guiding Principles

Our cyber approach follows six guiding principles, aligned directly to the council's Digital Strategy and national cyber expectations. These principles focus on outcomes, resilient services, protected data, and confident people, ensuring cyber security enables rather than constrains effective local government.



1) Resilient services by design

Plain message: "We build cyber resilience into services, so they keep running, even when things go wrong".

Why it matters: Residents rely on council services at moments of vulnerability, including safeguarding, care, housing and democratic processes. Cyber incidents increasingly lead to service disruption rather than just technical inconvenience. Designing resilience into services, systems and recovery arrangements is essential to protect continuity, safety and public confidence.

Link to policy: Cyber Assessment Framework (CAF) for local government Objective D (Minimising the impact of cyber security incidents), including Principle D1 (Response and recovery planning) and Principle D2 (Lessons learned), alongside Principle B5 (Resilient networks and systems). UK Government Cyber Security Strategy 2022–2030 and the Government Cyber Action Plan (public sector cyber resilience). LGA Security & Resilience guidance (including "Building a cyber resilient service" resources for directors).

2) Protection of data as a public trust

Plain message: "We protect personal and sensitive data because people trust us to do so."

Why it matters: Councils hold large volumes of personal, sensitive and legally protected information. A loss of confidentiality or integrity can cause direct harm to individuals and long-term damage to trust in public institutions. Strong cyber security underpins effective information governance, lawful data sharing and ethical service delivery.

Link to policy: UK GDPR and the council's Information Governance Framework (lawful, fair and secure handling of personal and sensitive information). CAF for local government Objective A (Managing security risk) including Principle A1 (Governance), plus Principle B3 (Data security) and Principle A3 (Asset management) for understanding what data we hold and how it is protected. LGA Security & Resilience guidance emphasising public confidence and trust. The LGA frames this agenda explicitly around "instilling public confidence and trust" through security and resilience

3) Secure-by-design technology and change

Plain message: "Security is built in from the start not bolted on afterwards."

Why it matters: Retrofitting security is costly, disruptive and often ineffective. As the council modernises legacy systems, migrates to cloud platforms, and increases automation and integration, security must be a design requirement for all change. This reduces long-term risk, avoids rework and enables faster, safer transformation

Link to policy: NCSC Secure design principles (designing and operating services with security as a core consideration). CAF for local government Principle B1 (Service protection policies and processes), Principle B4 (System security), and Principle B5 (Resilient networks and systems), supported by Objective A governance and risk management. UK Government Security "Secure by Design" principles for embedding cyber security practices in digital delivery.

NCSC notes that "the very worst outcomes can be avoided if services are designed and operated with security as a core consideration.

4) People-powered cyber security

Plain message: "Cyber security is everyone's responsibility, not just ICT's."

Why it matters: Human behaviour remains one of the most significant contributors to cyber incidents. Staff and Members must be supported to work securely, confidently and pragmatically, without creating unsafe workarounds. A strong cyber culture, supported by training and leadership, is as important as technical controls.

Link to policy: CAF for local government Principle B6 (Staff awareness and training) and Principle A1 (Governance), reinforcing leadership accountability and role-based expectations. NCSC public sector guidance (pragmatic behaviours and reducing common attack paths). LGA Security & Resilience resources, including councillor-focused "questions to ask" materials that strengthen scrutiny and organisational ownership

5) Risk-led, proportionate security

Plain message: "We apply the right level of security to the right level of risk."

Why it matters: Over-engineered security can reduce usability, accessibility and staff productivity, while under-investment leaves the organisation exposed. In a financially constrained environment, cyber controls and investment must be proportionate, evidence-based and focused on the areas of greatest risk and impact.

Being risk-led also means making explicit and defensible choices. In a financially constrained environment, the council will not seek to apply the same level of control to every system or dataset.

Lower-risk systems may carry acceptable residual risk where the cost or operational impact of further controls would outweigh the benefit. These decisions will be made transparently, recorded through governance and kept under review as risk, threat and service dependency change.

Link to policy: CAF for local government Objective A (Managing security risk) including Principle A2 (Risk management) and A1 (Governance), supported by CAF's outcome-based approach (focused on what needs to be achieved rather than a checklist of controls). MHCLG/Local Digital CAF programme guidance emphasising consistent understanding of cyber risks to essential services and prioritisation of activity and investment.

6) Assurance, accountability and collective defence

Plain message: "We are open about cyber risk and stronger when we work together."

Why it matters: Cyber security is a corporate and sector-wide concern. Councils are expected to demonstrate clear ownership, transparent assurance and continuous improvement. By adopting recognised frameworks, strengthening governance and participating in national collaboration, the council improves its own resilience and contributes to a stronger local government sector overall.

Link to policy: MHCLG/Local Digital "Defend as One" programme (collective defence through collaboration and knowledge sharing) and the Government Cyber Security Strategy commitment to "defend as one". CAF for local government Objective A (Governance and risk management) and Objective D (Response, recovery and lessons learned), supported by independent assurance expectations built into the CAF for local government approach. LGA Cyber 360 Framework (sector-led, collaborative improvement model aligned to NCSC guidance) and wider LGA Security & Resilience resources for councils.

Strategic Priorities

Priority 1: Secure-by-design foundations

A modern, resilient and secure technology foundation that enables digital transformation while protecting critical services, data and public trust.

Shropshire Council's ability to deliver safe, reliable and efficient public services increasingly depends on digital systems and data. Many of these systems underpin critical activities including health and social care, safeguarding, democratic processes, finance and workforce operations.

Legacy technology, inconsistent security controls and accumulated technical debt increase the council's exposure to cyber risk and service disruption. As the organisation modernises systems, adopts cloud platforms, expands automation and increases integration between services, the impact of any weakness in underlying foundations becomes more significant.

Secure-by-design foundations are essential to ensuring that digital transformation reduces risk rather than amplifying it. This priority ensures that security, resilience and recoverability are treated as core design requirements, not after-thoughts or compensating controls.

What we will do

- Modernise legacy systems to reduce security risk, complexity and support dependency
- Embed security requirements into all technology design, procurement and change activity
- Standardise identity, access, network and endpoint security across the organisation
- Adopt Zero Trust principles to reduce implicit trust and limit the impact of compromise
- Strengthen backup, recovery and disaster recovery capabilities, with regular testing
- Ensure all major digital change is subject to appropriate technical and security assurance through established governance routes

Priority 2: Governance, Assurance and Accountability

Cyber security is owned, governed and assured as a corporate risk, with clear accountability, transparent decision-making and evidence-based improvement.

Cyber security is no longer a niche technical risk; it is a strategic organisational risk with the potential to disrupt critical services, harm residents, undermine financial recovery and damage public trust. Nationally, councils are increasingly expected to demonstrate clear ownership, structured assurance and continuous improvement in cyber resilience.

Historically, cyber risk across local government has often relied on informal controls, technical expertise and fragmented governance. This approach is no longer sufficient in an environment of increased threat, regulatory scrutiny and dependency on digital services.

Without clear governance and assurance, cyber investment becomes reactive, risks are poorly understood, and accountability is diluted. This priority ensures the council has a disciplined, transparent and defendable approach to managing cyber risk, aligned to national expectations and corporate governance standards.

What we will do

- Treat cyber security explicitly as a corporate risk, owned at senior leadership level
- Adopt the Cyber Assessment Framework (CAF) as the primary assurance and maturity model
- Establish clear oversight arrangements, reporting and escalation routes for cyber risk
- Maintain a transparent cyber risk register aligned to the council's wider risk framework
- Use independent assurance, including IT Health Checks, to validate controls and maturity
- Ensure significant cyber risks, incidents and non-compliance are reported and addressed consistently
- Align cyber governance with audit, information governance, business continuity and digital oversight structures

These actions create clarity over who is responsible, how risk is understood, and how decisions are made.

Priority 3: Protecting Data and Critical Public Services

Sensitive data is protected and critical public services remain available, reliable and safe, even in the face of cyber incidents.

Shropshire Council delivers services that directly affect people's safety, dignity and wellbeing. This includes safeguarding children and adults, supporting people with complex needs, administering democratic processes and managing public finances. These services depend on the confidentiality, integrity and availability of digital systems and information.

Cyber incidents increasingly affect service availability and trust, not just data loss. Disruption to care systems, corruption of records, or loss of access to critical applications can have immediate and serious consequences for residents, staff and partners.

In addition, the council must share information securely with health, care, voluntary and community partners. This increases dependency on interconnected systems and supply chains, making the protection of data and service continuity a collective responsibility rather than an isolated technical concern.

This priority ensures that cyber security efforts focus on protecting what matters most.

What we will do

- Apply strong access controls, encryption and monitoring to sensitive and high-risk data
- Prioritise cyber protection for systems supporting:
- health and social care
- safeguarding and vulnerable cohorts
- democratic and electoral services
- finance, payroll and core corporate functions
- Strengthen vulnerability and patch management to reduce exposure to known threats
- Expand monitoring, logging and detection to identify suspicious activity early
- Improve cyber resilience within the council's supply chain and partner-hosted systems
- Ensure data protection, cyber security and business continuity considerations are aligned and mutually reinforcing

Priority 4: Building a Digitally and Cyber-Confident Workforce

Staff and Members are confident, capable and supported to work securely, reducing cyber risk through everyday behaviour and decision-making.

Technology alone does not deliver cyber resilience. Across local government, human behaviour remains one of the most significant contributors to cyber incidents, whether through phishing, insecure practices, poor password hygiene or informal workarounds created under operational pressure.

Shropshire Council's workforce operates in complex, high-demand environments, often dealing with sensitive information and time-critical decisions. As the council increases its reliance on digital tools, mobile working, automation and shared systems, staff confidence and understanding become critical to maintaining security without undermining service delivery.

A lack of confidence or clarity can lead to increased risk, not through negligence, but through uncertainty. This priority recognises that supporting people to work securely is as important as implementing technical controls.

What we will do

Under this priority, the council will:

- Ensure all staff and Members receive appropriate, proportionate cyber awareness training
- Provide targeted cyber skills development for ICT, digital and technical roles
- Embed clear, practical guidance on secure working into everyday processes and tools
- Use regular, realistic exercises and simulations to reinforce good cyber behaviours
- Support managers and leaders to understand their role in managing cyber risk
- Promote a positive cyber culture that encourages reporting, learning and improvement rather than blame

Priority 5: Accelerate Detection, Response & Recovery

Rapid detection, effective response and safe recovery are the hallmarks of a mature cyber-resilient organisation. For Shropshire Council, the ability to restore critical services quickly and safely is as important as preventing incidents occurring in the first place. This priority shifts the council's cyber posture from one that is predominantly preventative to one that is operationally resilient, tested and continuously improved.

It is no longer realistic to assume that cyber incidents can always be prevented. Across local government, resilience increasingly depends on how quickly an organisation can detect, contain and recover from an incident, rather than whether an attack attempt occurs.

Delayed detection, unclear response arrangements or untested recovery processes significantly increase impact. This can lead to prolonged service outages, data loss, reputational harm and loss of confidence from residents, partners and regulators.

Given the council's growing digital dependency, it is essential that cyber incidents are treated as a manageable operational risk, with well-understood roles, reliable processes and confidence that services can be restored safely. This priority ensures the council is prepared not just to defend, but to respond effectively when incidents occur.

What we will do

- Strengthen monitoring and detection capabilities to identify suspicious activity early
- Integrate automated alerting and logging across critical systems and environments
- Maintain a clear, tested Cyber Incident Response Plan aligned to business continuity arrangements
- Ensure roles, responsibilities and escalation routes are understood across ICT, services and leadership
- Conduct regular exercises and simulations involving technical teams, services and communications
- Improve backup, recovery and restoration arrangements, including offline and immutable backups
- Ensure learning from incidents and exercises is captured and used to drive continuous improvement
- Ensure Service Directors and Heads of Service understand and exercise their role in service-level cyber readiness, recovery priorities and decision-making during incidents

Priority 6: National Collaboration and Collective Defence

Shropshire Council will actively contribute insight, learning and practical experience to national and regional cyber initiatives, recognising that improving sector resilience is both a responsibility and a force multiplier for our own security.

Shropshire Council strengthens its own cyber resilience while contributing to a safer, more resilient local government sector through collaboration, shared learning and collective defence.

Cyber threats do not respect organisational boundaries. Local authorities face many of the same risks, exploit techniques and threat actors, often operating against shared technologies, suppliers and service models. No council can defend itself effectively in isolation.

National experience has shown that councils which collaborate, share intelligence and improve collectively are better prepared, recover more quickly from incidents and use scarce resources more effectively. This has driven a clear national policy direction towards collective defence, with an increasing expectation that councils will actively participate in shared cyber efforts.

For Shropshire Council, collaboration is not only about receiving support; it is about contributing insight, lessons learned and capability to strengthen the resilience of the whole sector.

What we will do

- Participate actively in national and regional cyber resilience initiatives for local government
- Align cyber assurance and reporting with nationally recognised frameworks and benchmarks
- Share anonymised insights from incidents, assessments and exercises to support sector learning
- Engage with MHCLG, the Local Digital Cyber programme and CAF development activity
- Explore shared tools, services and capabilities where this provides better value or resilience
- Strengthen collaboration across place, including with health, education, emergency services and voluntary partners

Delivery Plan, Governance, and Benefits Realisation

How we will deliver

Cyber security delivery at Shropshire Council will be embedded into the council-wide digital and technology portfolio, ensuring that security is designed into services, systems and ways of working rather than delivered as a standalone technical function.

This strategy will be delivered through a combination of targeted cyber initiatives, continuous improvement activity and the integration of cyber controls into all major digital change. Delivery will be prioritised using risk-based decision-making, aligned to the Cyber Assessment Framework (CAF), and shaped by national expectations for local government cyber resilience.

Cyber security activity will focus on protecting critical services, safeguarding sensitive data and enabling safe digital transformation at pace, while remaining proportionate to the council's risk exposure and financial context.

Operating model

Cyber security is governed as a corporate risk, with clear ownership, oversight and escalation routes integrated into the council's wider governance framework.

Oversight and accountability will be provided through:

Head of Service – Automation & Technology – provides senior strategic leadership across digital, cyber and information security, ensuring alignment between cyber resilience, digital transformation, information governance and organisational risk management. The Head of Service – Automation & Technology is responsible for setting direction, assuring coherence across strategies and providing senior ownership for cyber security as an enabler of safe and sustainable digital change.

Information Governance Leadership and Organisational Oversight (IGLOO) – a governance group responsible for overseeing information governance, data protection, cyber security, and associated compliance activities across the organisation.

Leadership Board - The Leadership Board is the senior-most officer leadership group in Shropshire Council. It sets the organisation's direction, makes or shapes key decisions, oversees major risks and programmes, and ensures all services are aligned to the Council's long-term plan. It owns cyber security as an organisational risk, providing senior oversight and direction.

Support and Enabled Workforce Portfolio Board – Govern's the execution, risk and dependencies of all programmes and projects within its specific portfolio, ensuring effective governance, risk resolution, and benefit realisation at the executive level. The board will meet every 4 weeks.

Digital Transformation Board (DTB) – The DTB provides strategic oversight, governance, and assurance for all digital transformation activities within the council. The DTB will meet monthly, with additional meetings as required.

Digital Design Authority (DDA) - The DDA is responsible for the technical and architectural oversight of all digital programmes and projects. Its purpose is to own and maintain the overarching programme design and design principles. Evaluate and make decisions on technical and digital design matters. Ensure all design activities align with strategic objectives, comply with standards, security-by-design is embedded into all technology and digital change, and deliver quality and consistency. Provide assurance that design decisions support operational service delivery and council priorities. The DDA will meet weekly, or as required based on the volume and urgency of design decisions.

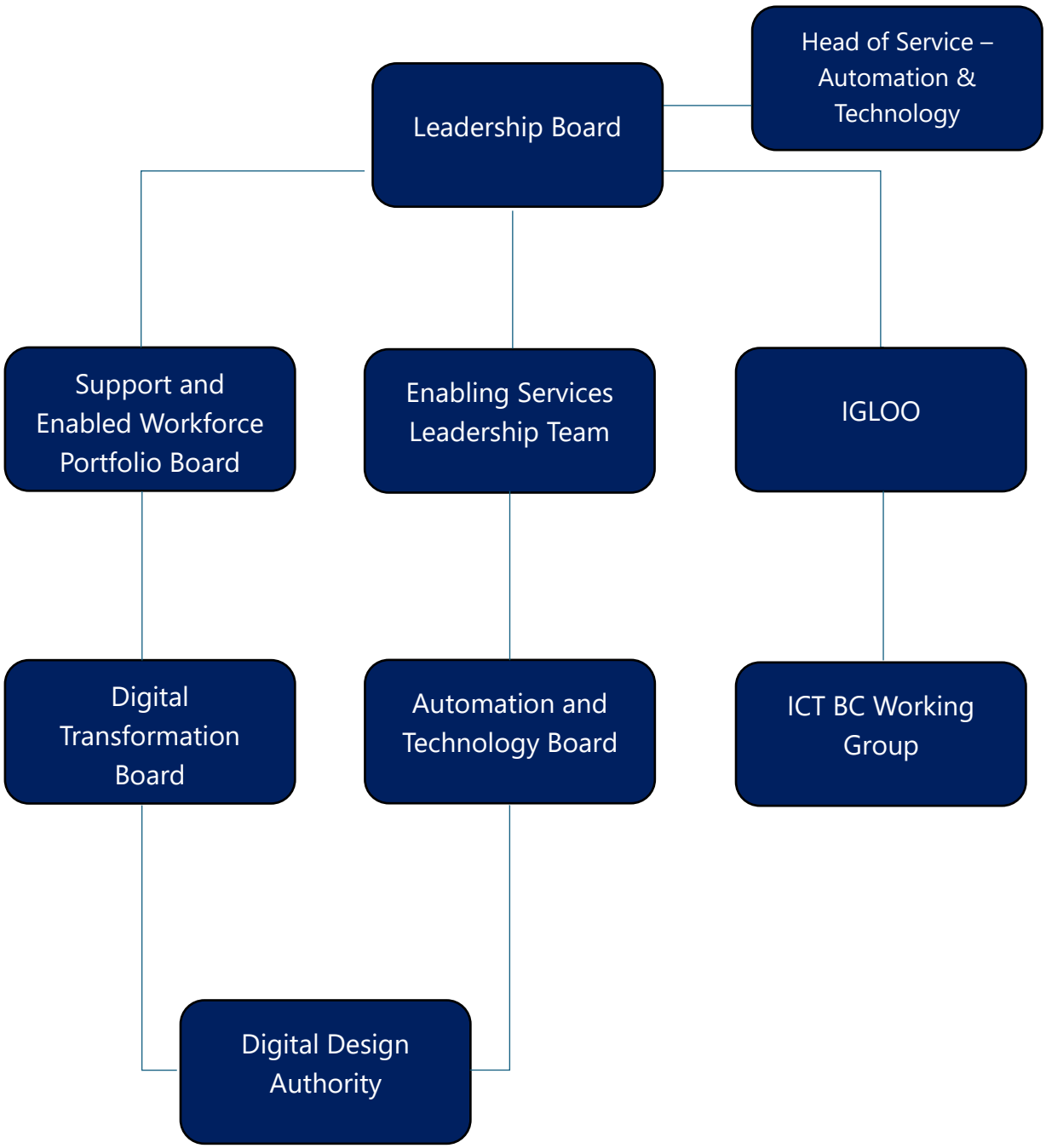
ICT Business Continuity Working Group –focuses on ICT business continuity, disaster recovery (BC/DR), cyber preparedness, and organisational resilience.

Enabling Services Leadership Team (ESLT) – The Enabling Services Leadership Team (ESLT) is the senior leadership group for Enabling Services within Shropshire Council. It is chaired by the Service Director – Enabling Services and brings together the Heads of Service and senior managers from all Enabling Services functions to coordinate delivery, provide updates, share risks and issues, and align activity with the Council's strategic direction.

Automation and Technology Board - The Automation and Technology Board is the central leadership and governance forum for all ICT functions within Shropshire Council. It coordinates service performance, programmes, digital transformation, risks, staffing, and technology decisions across the whole Automation and Technology service. It oversees cyber delivery, risk, investment and performance within the wider technology portfolio.

Heads of Service and service managers remain accountable for local compliance, risk awareness and secure operation within their services, supported by the Automation & Technology service.

This governance model ensures cyber security is visible, owned and actively managed, rather than implicitly assumed.



RACI (Summary)

Responsible	Service Director Enabling, Head of Service – Automation & Technology, Cyber Security Team, Business Process Owners.
Accountable	Chief Executive (Organisational cyber risk and resilience), s151 Officer (financial exposure and recovery impact).
Consulted	Service Directors, Unions, Information Governance, IGLOO, Internal Audit, Procurement, ICT Business Continuity working group
Informed	Members, staff, partners, suppliers, regulators (as appropriate)

Delivery approach

Cyber security delivery will be structured around:

- A rolling programme of CAF-aligned maturity improvement
- Risk-based prioritisation of activity and investment
- Integration of cyber requirements into projects, programmes and procurement
- Independent assurance to validate controls and identify improvement opportunities
- Continuous learning from incidents, exercises and sector insight

Delivery will balance prevention, resilience and response, recognising that sustainable cyber security is achieved through disciplined improvement over time rather than one-off interventions.

Benefits realisation

Investment in cyber security primarily delivers value through risk reduction, resilience and avoided harm rather than direct cashable savings.

Benefits will be realised through reduced likelihood and impact of cyber incidents, faster restoration of critical services, improved assurance to regulators and insurers, and reduced financial volatility associated with emergency response and recovery.

The council recognises that not all benefits will be immediately measurable or directly attributable. Progress will therefore be demonstrated through evidence-based assurance, resilience testing, CAF maturity outcomes and sustained reductions in unplanned disruption rather than headline financial returns.

Measuring Progress

Progress against this strategy will be monitored using a combination of:

- Cyber Assessment Framework maturity outcomes
- Independent assurance, including IT Health Checks
- Risk trend analysis and incident reporting
- Delivery milestones across priority initiatives
- Evidence of secure-by-design compliance across digital change

This approach ensures leadership has clear, consistent and defensible insight into both cyber risk and improvement over time.

Change & adoption

Successful cyber resilience depends on people, behaviours and decision-making, not just technology. To ensure security controls, processes and ways of working are consistently applied in practice, we will take a focused and pragmatic approach to cyber change and adoption across the organisation.

This will include preparing services early for security impacts, engaging staff and Members in clear, timely communication about cyber risks and expectations, and providing the right level of support so teams can work confidently and securely. Particular emphasis will be placed on helping people understand why controls exist, reducing unsafe workarounds and encouraging early reporting of concerns.

Adoption will be monitored through real-world usage, incident trends, exercise outcomes and observable behavioural change, ensuring secure practices become embedded in everyday work and that the benefits of cyber investment are realised in improved resilience, safer services and reduced organisational risk.

Information Governance Framework

A key foundation of our information security is the Shropshire Information Governance Framework, which ensures that all data is managed securely, ethically, and in accordance with statutory and local requirements. This framework underpins our initiatives, driving transparent practices and safeguarding confidential information across every system and service. By following the principles and protocols set out in the Shropshire framework, we sustain trust among residents, staff, partners, and stakeholders, while guaranteeing that each digital investment aligns with both regulatory standards and the organisational values of Shropshire.

Moving Forward

This strategy has been deliberately designed to be open, transparent and aligned to national frameworks so that it can be shared, reviewed and reused across the local government sector.

Shropshire Council welcomes peer challenge and collective learning and intends this strategy to contribute to raising cyber resilience standards beyond organisational boundaries.

In the next 12 months we will:

- Establish the cyber delivery and governance model, embedding clear ownership, oversight and assurance across the organisation.
- Baseline the council's cyber maturity using the Cyber Assessment Framework (CAF) and agree a priority improvement plan.
- Strengthen protection for systems supporting critical services, including care, safeguarding, democratic and financial functions.
- Improve monitoring, detection and incident response capability, including testing response and recovery arrangements.
- Embed secure-by-design principles into all major digital and technology change through design and assurance routes.
- Expand workforce cyber awareness and confidence, supporting safe and secure ways of working across all services.
- Actively participate in national and sector-led cyber resilience initiatives, contributing to collective defence through Defend as One.

Cyber security is an enabler of trust, resilience, financial sustainability and great public services. This strategy sets out a disciplined, pragmatic and forward-looking plan for Shropshire Council to meet its responsibilities, protect its communities and operate confidently in a complex threat landscape.

By integrating secure by design principles, adopting national frameworks, strengthening our workforce, modernising our technology, and fully participating in collective defence through Defend as One, we will deliver a safer, stronger and more resilient Shropshire.