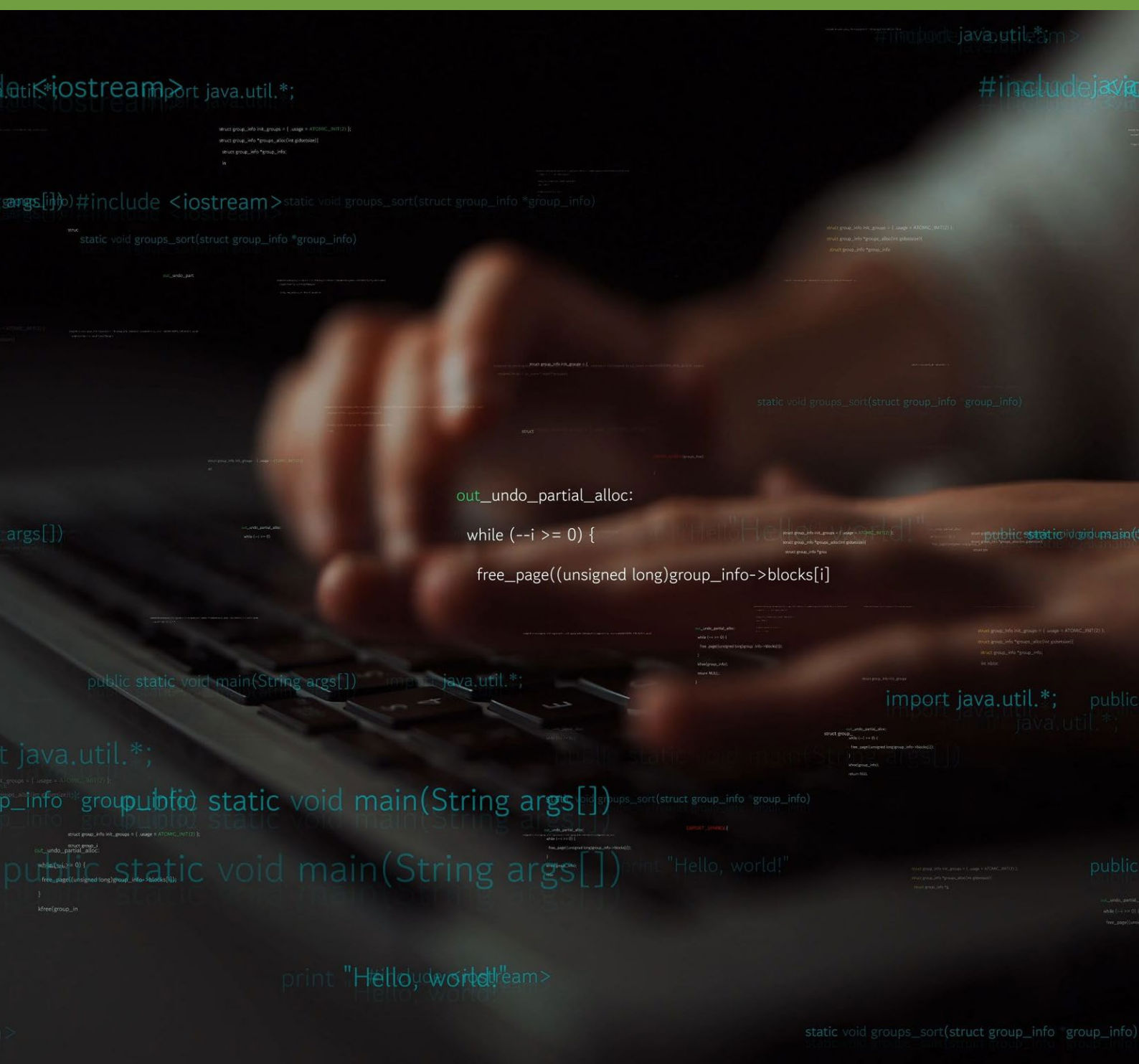
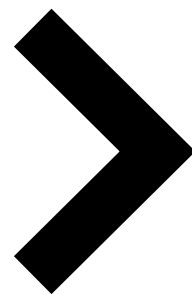


CYBER SECURITY STRATEGY

2026 - 2028





Why cyber security matters

Cyber security protects council services, personal information and public trust. As more services move online, everyone has a part to play.

The Leicestershire ICT Partnership supports Hinckley and Bosworth Borough Council and Melton Borough Council. Shared systems and support bring benefits, but cyber risks must be managed consistently across both councils.

This strategy sets out how the partnership will manage risk, protect systems and data, detect threats, respond to incidents and build good cyber behaviours.



The risk

Councils rely on digital systems for essential services and hold sensitive information. This makes them targets for threats such as ransomware, phishing and supply chain attacks. A successful attack could disrupt services, expose personal data, create financial costs, damage public trust and put extra pressure on staff.

Because the ICT partnership supports two councils, an incident affecting one council could also affect the other.



Vision

To protect both councils, the services we deliver and the information we hold, so services remain trusted, resilient and available.

What we aim to achieve

- **Protect** essential services and safeguard personal, sensitive and council information.
- **Build trust** with residents, partners, suppliers and other organisations.
- **Strengthen** cyber defences, capability and capacity across both councils.
- **Improve** cyber awareness and positive cyber behaviours.
- **Focus** effort and resources where they reduce the greatest risk.





How will we do this?

1. Manage cyber security risk

Understand key systems, data, vulnerabilities and threats; use recognised standards and assurance, including the Cyber Assessment Framework, PSN, Cyber Essentials and Cyber Essentials Plus; make sure cyber risks have clear owners and senior oversight; and manage supplier and partner risks.

2. Protect systems and services

- Put proportionate security controls in place based on risk.
- Build security into new and changing services from the start.
- Use protective technologies and good practice to reduce the chance of incidents.

3. Detect cyber security events

- Monitor systems, networks and devices for suspicious activity.
- Use alerts, logs, threat intelligence and anomaly detection to identify potential incidents early.
- Test detection arrangements and work with trusted partners to share threat information.

4. Respond and recover well

- Maintain and test incident response plans and runbooks.
- Include cyber incidents in business continuity and disaster recovery planning.
- Use testing and threat intelligence to find weaknesses, anticipate attacks and improve after incidents or exercises.

5. Build skills, knowledge and culture

- Provide cyber awareness training tailored to different roles.
- Support managers and elected members to understand cyber risk in service delivery and governance.
- Develop technical cyber skills, run exercises and promote a positive cyber security culture.



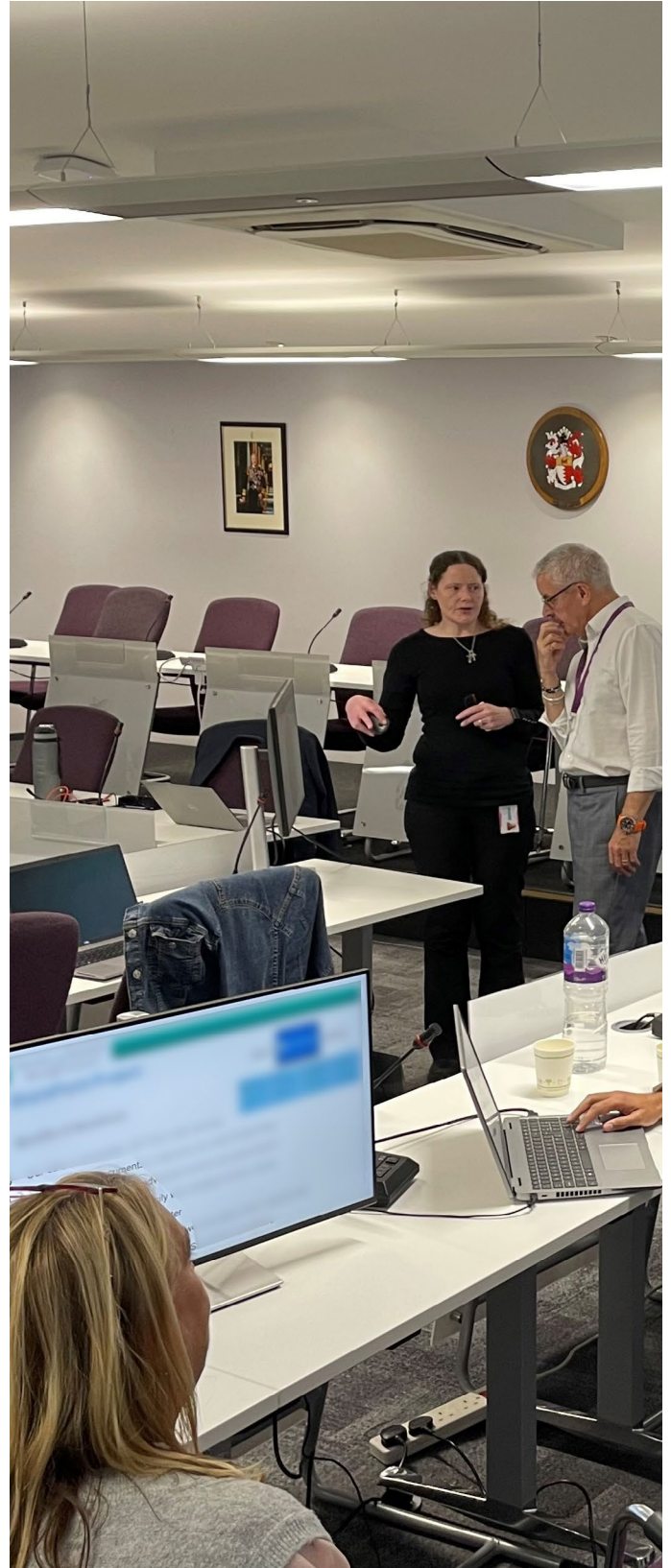
What staff and elected members need to do

Staff and elected members should complete required training, follow council policies and processes, report suspected incidents or phishing promptly, consider cyber risk when planning services or projects, and handle information carefully using approved systems.



What residents and service users can do

- Use official council contact routes and online services.
- Be cautious of unexpected messages claiming to be from the council, especially if they ask for personal details, payments or urgent action.
- Report anything suspicious using the council's published contact routes.
- Keep personal login details secure.





Who is responsible?

- Elected members provide democratic oversight and assurance.
- Strategic leadership teams own cyber risk and ensure appropriate governance, resources and prioritisation.
- The Senior Information Risk Officer provides senior accountability for information and cyber risk.
- ICT leadership implements and operates cyber security controls.
- The Data Protection Officer advises on data protection risks linked to cyber incidents.
- Staff, members, suppliers and partners must follow relevant policies, standards and contractual obligations.



How we will measure progress?

- The partnership will track progress, report through senior leadership and governance boards, and use the findings to improve the strategy and action plan.

Measures will include:

- Training completion and staff survey results.
- Reported phishing attacks and cyber incidents, including time to resolution.
- Cyber Essentials, Cyber Essentials Plus and PSN certification.
- Annual Cyber Assessment Framework review results and CCoE health check scores.
- Engagement with cyber communications and campaigns.



Keeping the strategy up to date

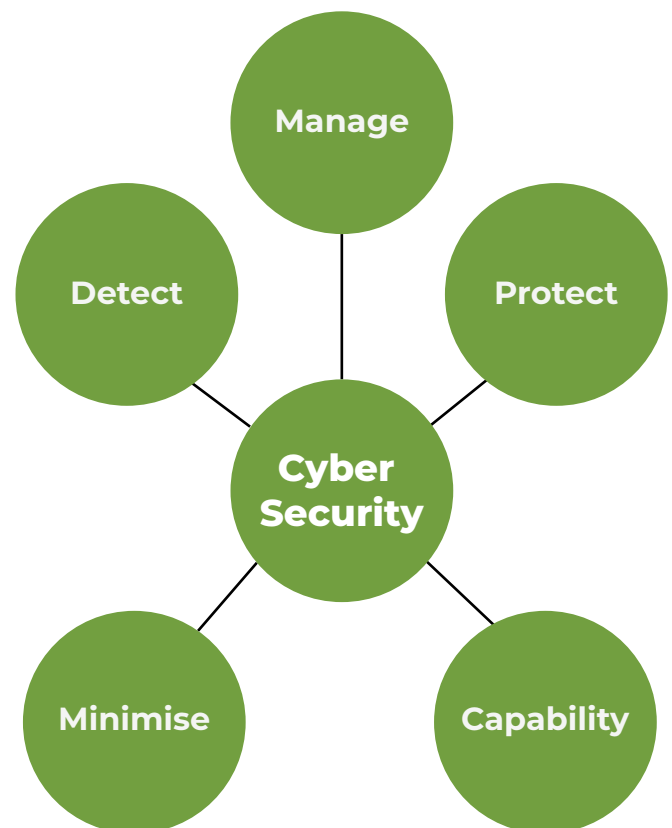
The strategy will be reviewed regularly, taking account of progress, emerging threats, legal or regulatory changes, best practice, organisational change, assurance findings, performance data and feedback.



How it will be delivered

The strategy sets the direction for managing cyber risk across the ICT partnership. Detailed activity, timescales and resourcing will be set out in a separate cyber security action plan.

Because resources are constrained, activity will be prioritised where it gives the greatest reduction in cyber risk and the greatest protection to essential services and residents.





Some useful terms

Key terms used in this summary:

Phishing: fake messages designed to trick people into sharing information, clicking unsafe links or making payments.

Ransomware: malicious software that locks systems or data and demands payment to restore access.

Supply chain attack: an attack that reaches the council through a supplier, contractor, software provider or other partner.

Cyber hygiene: basic good practice that helps keep systems safe, such as updates, strong passwords and secure access.

Incident response plan: the agreed steps to follow if a cyber incident happens.

PSN, Cyber Essentials and Cyber Essentials Plus: recognised checks or standards for cyber security arrangements.

Cyber Assessment Framework: a structured review of how well cyber risks are being managed.

