SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

Tuesday, 7 October 2025

Report of Councillor Richard Cleaver - Cabinet Member for Property and Public Engagement

ICT and Cyber Security Strategies

Report Author

Gary Andrew, IT Services Manager

gary.andrew@Southkesteven.gov.uk

Purpose of Report

To approve the updated ICT Strategy and the new Cyber Security Strategy.

Recommendations

Cabinet is asked to:

1. **Approve the adoption of the updated ICT Strategy 2025 - 2028**
2. **Approve the new Cyber Security Strategy 2025 - 2028.**

Decision Information

Is this a Key Decision?	No
Does the report contain any exempt or confidential information not for publication?	No
What are the relevant corporate priorities?	Effective council
Which wards are impacted?	All Wards

1. Implications

Taking into consideration implications relating to finance and procurement, legal and governance, risk and mitigation, health and safety, diversity and inclusion, safeguarding, staffing, community safety, mental health and wellbeing and the impact on the Council's declaration of a climate change emergency, the following implications have been identified:

Finance and Procurement

1.1 The financial implications of delivering the actions arising from the ICT Strategy will be included in the budget proposals once the Strategy has been approved.

Completed by: Richard Wyles, Deputy Chief Executive and s151 Officer

Legal and Governance

1.2 There are no governance comments additional to those already referred to within the report.

Completed by: James Welbourn, Democratic Services Manager

2. Background to the Report

2.1. The Council's ICT Strategy covers the period 2022 - 2025 and has been reviewed in order to ensure it remains up to date and reflects changes in technology.

2.2. The vision for the new Strategy is made up of 2 key principles which are:

ICT platform – end to end interactions are simple and streamlined as possible.
A Digital workforce – enabling our staff to have access to the right tools to do their job and be confident in maximising the use and benefits of technology in daily work

The Strategy also introduces technology principles which set corporate technology standards. These will be built into future technological designs and replacement of corporate ICT systems.

2.3. The updated ICT strategy ensures that digital infrastructure aligns with the Council's evolving business priorities. SKDC's draft ICT Strategy 2025 -2028 emphasises the role of ICT in enabling agile working, modern service delivery, and digital transformation across services.

2.4. By embedding innovation and collaboration into the strategy, SKDC can empower services to exploit digital tools, create process efficiencies and improve customer experience.

2.5. The growing threat posed by cyber activists and other malicious activists also highlights the need for a robust ICT Cyber Strategy. This Strategy addresses not only technological advancements but also the increasingly sophisticated nature of cyber threats, ensuring the organisation's digital assets, services, and stakeholder data remain protected. Proactive investment in cybersecurity measures, ranging from staff training and awareness to advanced detection and response tools, will be critical to maintaining trust, operational continuity, and compliance with regulatory requirements.

3. Key Considerations

3.1. The recommendation is to seek approval of the updated ICT Strategy and Cyber Security Strategy 2025-2028. The current ICT Strategy is coming to an end in 2025 and needs review and update to provide the Council clear strategic direction going forwards.

3.2. The increased threat of cyber-attack or breach necessitates the need for a cyber strategy to ensure the Council is prepared and protected. The Cyber Security Strategy 2025–2028 outlines the critical need for robust defences to protect sensitive data and maintain public trust.

4. Other Options Considered

4.1. The Council could choose not to have an ICT or Cyber Security Strategy, but this would not provide a robust framework in which to manage and develop ICT platforms.

5. Reasons for the Recommendations

5.1 The refreshed ICT Strategy ensures the Council continues to provide modern services to residents and employees of the authority.

5.2 The ICT Strategy enables the Council to review emerging technologies and adapt systems to ensure they are fit for purpose and future proof.

The Cyber Security Strategy is a crucial part of the Council's duty to ensure that all systems are secure and sensitive data held is safe and secure. Councils must adopt proactive measures to ensure the integrity of the Councils systems such as:

- Two-factor authentication (2FA)
- Antivirus and endpoint protection

- Staff training on cyber hygiene (Cyber hygiene refers to the regular practices, habits, and precautions individuals and organisations take to protect their digital systems, devices, and data from cyber threats like malware, phishing and theft).
- Regular security audits aligned with the National Cyber Security Centre's Cyber Assessment Framework (CAF)

5.3 As Councils increasingly deliver services online, they must ensure digital platforms are secure, accessible, and inclusive. A strong cyber security Strategy reassures residents and businesses that their data is protected, fostering trust in digital services.

6. Consultation

6.1. The Cyber Strategy has been developed around the Cyber Assessment Framework which was created by the National Cyber Security Centre.

6.2. SKDC's ICT team has worked closely with the National Cyber Security Centre to review the Council's Cyber Security and developed and implemented improvements to the Council's systems in based on their recommendations.

7. Appendices

7.1. Appendix 1 – ICT Strategy 2025 – 2028

7.2. Appendix 2 – Cyber Security Strategy