CORPORATE SCRUTINY COMMITTEE - WORKPLAN SCOPING DOCUMENT

TOPIC	Cyber Security
PROPOSED COMMITTEE DATE	To be dealt with initially outside of a formal meeting.
BACKGROUND	With the cyber threat landscape continually evolving, and an increased demand for digital public and corporate services, councils face a variety of challenges in developing ever stronger cyber secure and resilient procurement practices. The 10 Questions on Cyber Security Guide by the Local Government Association and Centre for Governance and Scrutiny was recently published and designed to support scrutiny members in understanding how the councils scrutiny function can review policies, practices and procedures relating to cyber security. Cyber security cuts across all council departments and functions. If an attack were to occur, there is the potential for every aspect of the council to be affected. Councils should consider it a case of 'when' not 'if' a cyber-attack will occur. Therefore, all Councils need to continuously review, refresh and reinforce their approach to cyber security, whilst also looking at their capabilities to deal with them Scrutiny can bring about positive change when looking at cyber security by identifying any gaps and vulnerabilities that there may be in the council's current cyber security framework, policies, and procedures. Members of the corporate scrutiny committee need not be experts in the field but need to recognise the importance of cyber security in terms of its pervasiveness throughout the council's departments and infrastructure.
FOCUS FOR SCRUTINY	• Does the council have a cyber security strategy? If it does not, does cyber security form a clear and defined part of the councils Digital Strategy? • How does the organisational leadership, the cabinet and executive effectively incorporate cyber security into the council's central objectives? • How does the council have confidence that members and all staff members have the skills and knowledge to understand and play their part in action on cyber security? • How does the council currently assess its cyber security posture against good practice, and how do we plan improvements where necessary? • Has the council identified risks and vulnerabilities in its systems and networks and are they minimised to an appropriate level? • Does the council have a centralised asset management register and how is this defined, would this be information assets, technical assets or both? • How does the council ensure that risk is effectively monitored in terms of cyber security? • Are risks identified and managed effectively in relation to the councils supply chain (external partners) and is this monitored regularly?

	• With many primary and secondary school run under the local authority, where does the responsibility lie in regard to cyber security for these LA maintained schools? • If a policy was created and adopted would LA schools also be asked to comply, or will they have their own strategies and policies in place that overrule this? • If schools have their own policies and strategies in place will the Isle Of Wight Council also assess these given the fact that schools in recent years have been subject to issues in regards to hacks etc.? • What is our current data retention policy, and does it adhere to the wider information management architecture policies, such as those set out in FOIA, GDPR and EIR? • Do we have a comprehensive, effective response and recovery plan in the event of a cyber-attack or incident? • If an incident were to take place, how can we learn from this and improve?
EXPECTED BENEFITS/ OUTCOMES	• To understand the attitudes and culture within the council about cyber security. • To understand how scrutiny can be more proactive on the issue of cyber security. • To understand how networks and systems are monitored, what for, and how a response might be made if the worst were to be discovered, by who. • To understand the context of asset management within cyber security. • To understand the nature of the supply chain (external partners), and the processes in place to safeguard information and systems from threats. • To understand what methods of back up the council use, e.g., cloud storage, tape, external hard drives and how are these managed. • To highlight where there may be gaps in the incident management plan and the overall incident response strategy. • To ensure decision makers are being transparent and communicating with relevant officers, members and stakeholders.
APPROACH	ICT to spend time looking into the questions posed above and to provide responses to the scrutiny committee outside of a formal setting. The committee will then determine any areas that need to be investigated in more detail at a formal meeting and any recommendations to be put forward to Cabinet.
WITNESSES/ EVIDENCE REQUIRED	• Deputy Leader, Cabinet Member for Digital Transformation, Housing, Homelessness and Poverty • Director of Corporate Services
LINKS TO CORPORATE PLAN	Core values Our purpose is to work with and support the Island's community, finding ways to help it to satisfy its needs independently or to provide services directly where necessary. We value: 1. Being community focused: This means, wherever possible, putting the needs of our residents first. 2. Working together:

	This means engaging realistically with partners to make the most of integrated working, helping communities to help themselves and being a strong council team that delivers on these values. 3. Being effective and efficient This means being the best that we can be in how we organise and deliver our services, using all our limited resources wisely and carefully, getting on with things where we can. 4. Being fair and transparent This means making decisions based on data and evidence and in an open and accountable way.