castlepoint
benfleet | canvey | hadleigh | thundersley

STRATEGY FRONT COVER

Name of Strategy / Policy: Cyber Security Strategy

Date last updated: Current Strategy (May 2021)

Links to Council Priorities:

Priority	Linked Yes / No?
Environment	No
Housing and Regeneration	No
Health and Community Safety	No
A Commercial and Democratically Accountable Council	No

Links to Other Strategies and Policies
IT Strategy.

SMART Action Plan in this document?
Yes – Cyber Security Action Plan

Actions linked to corporate plan objectives?
No

Name of lead officer responsible for producing the action plan:
Mike Greenwood – ICT Service Manager
Phone: 01268 8822497
E-mail: mgreenwood@castlepoint.gov.uk

Name of lead Member and Member body responsible for monitoring implementation of the action plan:
Cllr Wayne Johnson – Cabinet Member for Resources

Equality impact assessment undertaken: Yes

Sustainability appraisal undertaken: N/A castlepoint

benfleet | canvey | hadleigh | thundersley

Castle Point Borough Council

Cyber Security Strategy

Produced by ICT Service Manager

Date of next review: May 2022

Approved by:

- Executive Management Team
- Cabinet

1 Introduction

1.1 Copies of the Council's Strategies and Policies can be obtained at the Council Offices or on our website at www.castlepoint.gov.uk.

1.2 The Cyber Security Strategy was a new strategy introduced in 2017 following several successful and high-profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to residents and other stakeholders that every effort has and is being made to render our systems safe and to protect our data and our networks from attack or interference.

1.3 This strategy is supported by several policies and a separate action plan which indicates timeframes and officers responsible for implementation. Resource and financial implications are set out in the ICT strategy, individual Service Action Plans and reflected in approved budgets, reported to Members and Executive Management Team (EMT).

1.4 The actions identified within the action plan and required within the policies which support the strategy, are funded through existing budgets as contained within the Policy Framework and Budget Setting report (incorporating the Council's medium-term financial forecast, financial planning and capital strategy).

1.5 It is the Council's intention to comply with the principles of the government backed scheme - Cyber Essentials and to follow the 10 Steps to Cyber Security as published by the National Cyber Security Centre and set out within this document.

2. Our Key Priorities

2.1 Our present Key Priorities established from the Sustainable Community Strategy together with our internal priority are: -

- **E**nvironment
- Housing & Regeneration
- Health & Community Safety
- A Commercial & Democratically Accountable Council

2.2 The Cyber Security Strategy sits alongside the ICT Strategy and is supported by a suite of operational policies.

3. Cyber Security

3.1 Cyber security refers to the protection of information systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, because of failing to follow security procedures.

3.2 Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade crucial services on the network of their organisations or wipe data from the network.

3.3 Of equal concern are those insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the internet.

3.4 Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider. These individuals can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.

3.5 The overall cyber risk to an organisation from insider threats is not just about unauthorised access to information systems and their content. The physical security controls protecting those systems from inappropriate access, or removal of sensitive data or proprietary information on different forms of media are equally important. Similarly, a robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workplace and industrial and other forms of espionage is an important element in a comprehensive approach to security.

3.6 In forming this strategy, the Council has referred to the National Cyber Security Strategy 2016-2021 and adopted the “10 steps to Cyber Security” as the basis of its Cyber Strategy.

4. Cyber Security Governance / Roles and Responsibilities

4.1 The Council’s nominated Senior Information Risk Owner (SIRO) is the Legal Services Manager who holds responsibility for the governance of cyber security and information risk within the Council. However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all staff having a role to play.

4.2 The Council’s procedures give emphasis to prevention of an attack and minimising the impact of a successful attack on the organisation, its information and systems. Managers and staff throughout the organisation have a role to play and procedures are in place to maintain awareness of cyber security issues.

4.3 The Council’s Managed ICT Service Provider has responsibility to protect the Authority’s Systems, Networks and Applications from physical loss, damage or unauthorised access always but employees, management, and the Managed ICT Service Provider work jointly to achieve this. For example, employees and management are responsible for basic day-to-day security by ensuring that access to the office and devices used at home are restricted, and passwords are not accessible to others. Management must ensure that staff are aware of the need for security and must back up security recommendations with disciplinary procedures where they are not adhered to. The Council’s Managed ICT Service Provider is responsible for ensuring that; Client devices are password protected, public devices are secured to desks, all wiring cabinets are secured, and access to Servers and other shared equipment is physically protected.

4.4 System Administrators must ensure that; Access to systems is granted only to authorised users, access levels are controlled, and password controls are in place.

5.0 Strategic Awareness

5.1 The Council recognises the need to be proactive in maintaining an awareness of Cyber Security issues and recognises this by; Including Cyber Security as a risk on its corporate risk register, undertaking regular vulnerability testing of its systems and ICT infrastructure, and undertaking a planned programme of staff awareness exercises.

5.2 The Council is committed to compliance with the Cyber Essentials Scheme which was developed by the UK Government in partnership with information security industry experts and defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats from the Internet:

- Within the context of the Government's 10 Steps to Cyber Security guideline published in September 2012 (updated 2018) as part of the 'Keeping the UK safe in cyber space initiative'.
- Offers a mechanism using the 'assurance framework' by which an organisation can demonstrate to customers, investors, insurers, and others that it has taken these essential precautions to protect itself from Internet based threats.

5.3 Provision for security management, covering the security and integrity of the Authority's Systems, Networks and information is included within the Council's Managed ICT Service Agreement.

6. Our Strategy – 10 Steps to Cyber Security

6.1 The Council's Cyber Security Strategy is based on the "10 Steps to Cyber Security" framework produced by the National Cyber Security Centre in 2012 (updated 2018).

6.2 This guidance is now used by a majority of the FTSE350. The guidance is complemented by the paper Common Cyber Attacks: Reducing The Impact (updated 2019) which sets out what a common cyber-attack looks like and how attackers typically undertake them.

Understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means for organisations to protect themselves from attacks. The following "At-a-glance" diagram and supporting paragraphs are taken directly from the 10 steps guidance and have been slighted tailored to suit operations within the Council.

7. 10 Steps To Cyber Security

7.1 An effective approach to cyber security starts with establishing an effective organisational risk management regime (shown at the centre of the following diagram). This regime and the 9 steps that surround it are described below the diagram.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

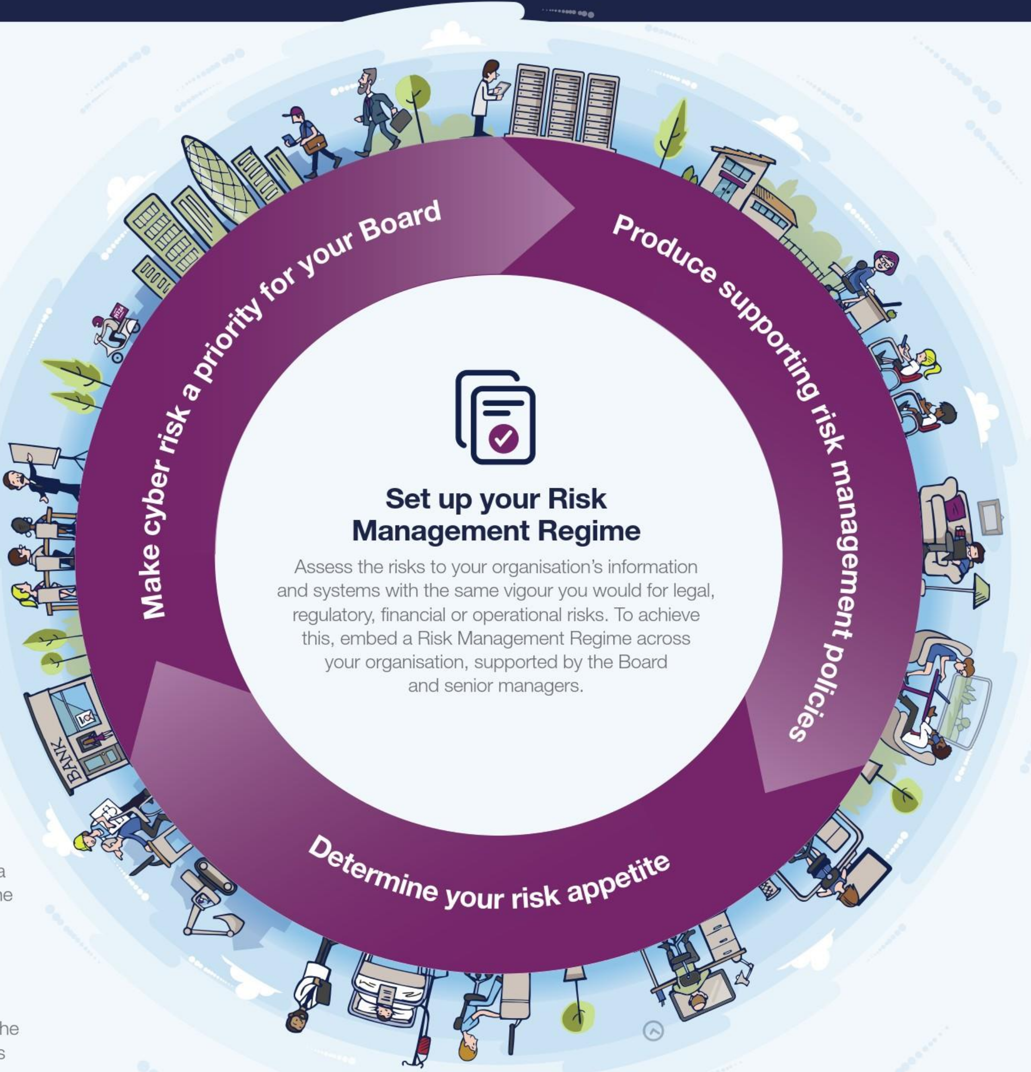
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

Step 1 - Risk Management Regime

Embed an appropriate risk management regime across the organisation. This is supported by an empowered governance structure and clearly communicates the approach to risk management through the development of applicable policies and practices. These policies and practices aim to ensure that all employees, contractors, and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Step 2 - Secure configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. The Council has developed a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching.

Responsibility for this step rests mainly with the Council’s Managed ICT Service Provider but system administrators also have a role to play.

Step 3 - Network security

The connections from our networks to the Internet, and other partner networks, expose our systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, we have reduced the chances of these attacks succeeding (or causing harm to the organisation). Our organisation's networks span several sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, the Council considers where our data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Step 4 - Managing user privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users are provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges is carefully controlled and managed. This principle is sometimes referred to as ‘least privilege’.

Step 5 - User education and awareness

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This is supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Step 6 - Incident management

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. The Council works with their ICT Service Provider to implement recognised specialist incident management expertise.

Step 7 - Malware prevention

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact on our systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Step 8 - Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows the Council to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

Step 9 - Removable media controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. The Council has clear policies in place to manage and apply security controls over the use of removable media.

Step 10 - Home and mobile working

Mobile working and remote system access offer great benefits but exposes new risks that need to be managed. The Council has established risk-based policies and procedures that support mobile working and remote access to systems that are applicable to users, as well as service providers. Employees are trained on the secure use of their mobile devices in the environments they are likely to be working in.

8. Policies and Protocols

8.1 The following policies & protocols support this strategy and may be located on the Council's intranet.

Policy / Protocol	Description
Information Security	Information security refers to the defence of information or information systems from unauthorised or unintended access, destruction, disruption, or tampering.
Physical Security	Security of the premises to prevent unauthorised access, damage and interference to business premises, Information, and Information Technology.
Acceptable Use	Obligations on users before they are authorised to access systems and information and supported by a signed declaration by each employee.
Email & Digital Communications	Good practice and advice, describing the organisation's expectations for use and warnings regarding suspicious emails.

8.2 Each of these policies / protocols is reviewed every four years, coordinated by the ICT Manager who works closely with the Legal Department and other colleagues who have a role to play in their implementation. Where available policy templates provided by the Essex Online Partnership (EOLP) are tailored to local requirements.

8.3 In addition to the above, before an organisation can connect to the Public Services Network (PSN) it needs to pass the PSN compliance process as determined by the Cabinet Office. This effectively requires an organisation to demonstrate that their infrastructure is sufficiently secure and that its connection to the PSN would not present an unacceptable risk to the security of the network.

8.4 An infrastructure is defined as 'the situation from which PSN network traffic can be sent or accessed. This encompasses the networks, systems, hardware, processes and staff that will have direct and unmediated access to the PSN'.

8.5 To achieve compliance, the Council is required to meet Information Assurance (IA) requirements as determined by the Cabinet Office, which have been designed to provide an achievable and sensible baseline for security. Along with these IA requirements, the Council is required to make several commitments about how it will work to ensure the ongoing security of the PSN. The compliance assessment is undertaken annually.

8.6 The compliance process for obtaining a PSN connection certificate focuses on connecting a specific, predefined infrastructure to the PSN.

8.7 The full PSN compliance certification process is set out here:

www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate#Code-of-Connection

9.0 Incident Response & Recovery

9.1 If a cyber-attack is identified the Council has policies and practices in place to minimise impact and ensure an efficient recovery. The instruction to staff is clear and simple - In the event of an IT information breach, or suspected breach, the protocol will be triggered by contacting:

ABS Helpdesk
Extension: 4444
Email: SPOC@smartnetservices.uk

And

Mike Greenwood – CPBC IT Services Manager
Telephone: 01268 882497
Email@ mgreenwood@castlepoint.gov.uk

Equalities Impact Assessment

Policy Name	Cyber Security Strategy
Aim of Policy *(ask yourself why the policy is needed, what does the authority hope to achieve by it and how will the authority ensure that it works as intended)*	To demonstrate how the Council has aligned its activities with the wider National Cyber Security Strategy, the Cyber Essentials Accreditation and to express how the Council is responding to the cyber security threat.
Time Frame *(you should record the start date which should be prior to policy development or at design stages and end date should consider informing the decision-making process)*	The Cyber Strategy is ongoing. Work began in earnest in developing the strategy in September 2017.
Date of EqIA	23rd November 2017
Decision making & quality control *(you should identify sign off by responsible officer/senior management team/members)*	Executive Management Team are required to approve the Strategy. The EQIA is contained within the Strategy.
Policy Author	Chris Mills, Head of Resources

Identify potential impact on which groups (Protected characteristics) *(you should outline what the relevance of the policy, service, function etc. is to one or more of these groups. Who does it benefit, who doesn't benefit and why not and who should be expected to benefit and why don't they.* *If you conclude it is not relevant this should be recorded here with the reasons and evidence)*	Age Disability Gender reassignment Marriage and civil partnership Pregnancy and maternity Race Religion or belief Sex Sexual orientation	There is no negative impact for these groups.
Relevant existing data/information including relevant legislation *(you should identify what evidence is available and set it out here. This includes evidence from involvement and consultation)*	N/A	
Data/information to be obtained *(here you should identify where there are gaps in the evidence and set out how these will be filled)*	N/A	
Potential actions to minimise negative impact and maximise positive impact	N/A	
What consultation has been used or undertaken? *(you should identify who needs to be involved e.g. decision makers, frontline staff implementing the policy, partner/parent organisations etc.)* Include Date of consultation and methods used	Consultation with ICT Manager, Capita, Corporate Management Team and Operational Management Team.	
What were the findings of the consultation?	To be completed	
Agreed actions to maximise positive impact and minimise negative impact of this policy. *(you should identify the range of options to address the impact, one of four possible options*	No major change, the policy meets the requirements of the Council. Review to be performed with new IT supplier post-April 2022	

will apply: no major change, adjust the policy, continue the policy, or stop and remove the policy. Give reasons for your decision. **These actions must now be transferred to the relevant service plan.**	
Timescale for actions above to be completed	1st December 2021
Lead Officer (s)	Mike Greenwood
Review date and monitoring mechanism	To be completed

Agreed at DMT - Date:	
Agreed – Head of Service	
Agreed – Equality Lead Officer	
Policy Register updated:	

Revision History

Revision Date	Reviewed By	Role
01/12/20	Mike Greenwood	IT Service Manager
20/05/21	Mike Greenwood	IT Service Manager

Appendix A

(Withheld due to Security issues)