Shared Technology Services Cyber Security Strategy 2021-2024

THE CHALLENGE

In a world of electronic information, the protection of our data is becoming ever more important. The amalgamation of data stored in smart watches to the far stretched ‘misunderstood’ cloud means we don’t understand the footprint and trail our data leaves behind.

We exist in a culture powered by interconnecting data, constantly evolving and allowing us to make better decisions. We experience the benefits of this in public sector but due to our need and want to share, we create a weakening around our control of the data. Once it has left our environment and spreads out into other infrastructure the legislation, we use to govern our data may no longer have application.

This makes it even more critical for us to put in controls around how we use, store and process our data. It makes it critical for us to follow the guidance from the experts and to ensure that our systems are appropriately hardened and locked down to keep the attackers out and our systems continuously working well.

The real challenge comes when there is a need to encourage more collaboration, more access to information and to encourage transformation within an organisation. Very often, the rules around responsible data management stifles the ability to share. One of the most difficult jobs in this area is to effectively balance and enable transformation but also to continue the responsible use of data that we are accountable for.

Cyber incidents are on the rise, especially within public sector. We know that the ramifications are serious and widespread, from personal to economic. Protection and remediation are service disrupting and of significant financial expense. The impact on people affected by their stolen information can be disturbing and life altering in some cases.

This Cyber Security strategy outlines the focus we shall be adopting for our councils and customers. It is imperative that we put the right controls in place to protect and react to cyber threats going forward. We have a strong relationship with National Cyber Security Centre and other private cyber agencies which we will harness to help us to protect the data of our citizens and our customers.

We want to continue to use the benefits of technology to improve the lives of local people. This strategy will safeguard us all. It will build confidence in the way we operate and deliver our services and keep us at the forefront of the digital revolution.

\

INTRODUCTION

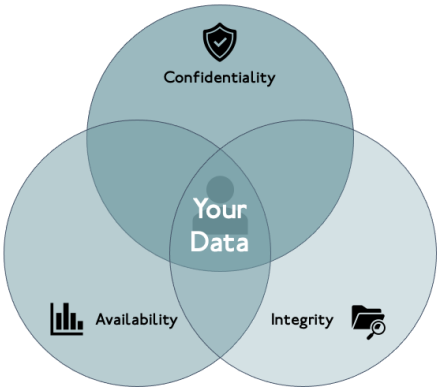
The Shared Technology Services (STS) is an IT shared service for the councils of Brent, Lewisham and Southwark. Brent council is the host borough for the service. STS is governed by a Inter Authority Agreement, a Joint Committee of two elected members from each council and the executive directors.

This document sets out the STS application of information and cyber security standards to protect our systems, the data held on them, and the services we provide from unauthorised access, harm or misuse. It is our cyber security commitment to the people we represent and is of national interest. It emphasises the importance of cyber security in the role of all staff.

WHY IS CYBER SECURITY IMPORTANT?

Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information.

- Attacks on Confidentiality – stealing, or rather copying personal information.
- Attacks on Integrity – seeks to corrupt, damage or destroy information or systems and the people who rely on them.
- Attacks on Availability – denial of services, seen in the form of ransomware.



Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorised access. Cyber security may also be referred to as information technology security.

Cyber security is important because, in order to effectively deliver services, we all process and store large amounts of data on computers and other devices. A significant portion of this data is sensitive information. It includes financial data, personal information and other types of data for which unauthorised access or exposure could have negative consequences.

We transmit sensitive data across networks and to other devices in the course of providing services or even just using your mobile to look at social media. Cyber security is the discipline dedicated to protecting this information and the systems used to process or store it. It is everyone's responsibility to ensure that we manage our data appropriately.

Cyber security is crucial in ensuring our services are kept up and running. It is also vital in ensuring in building and keeping our public's trust. A cyber-attack would have very serious consequences both in terms of a disruption to our services (many of which serve some of our most vulnerable residents), council's reputation and impact to our fiscal position.

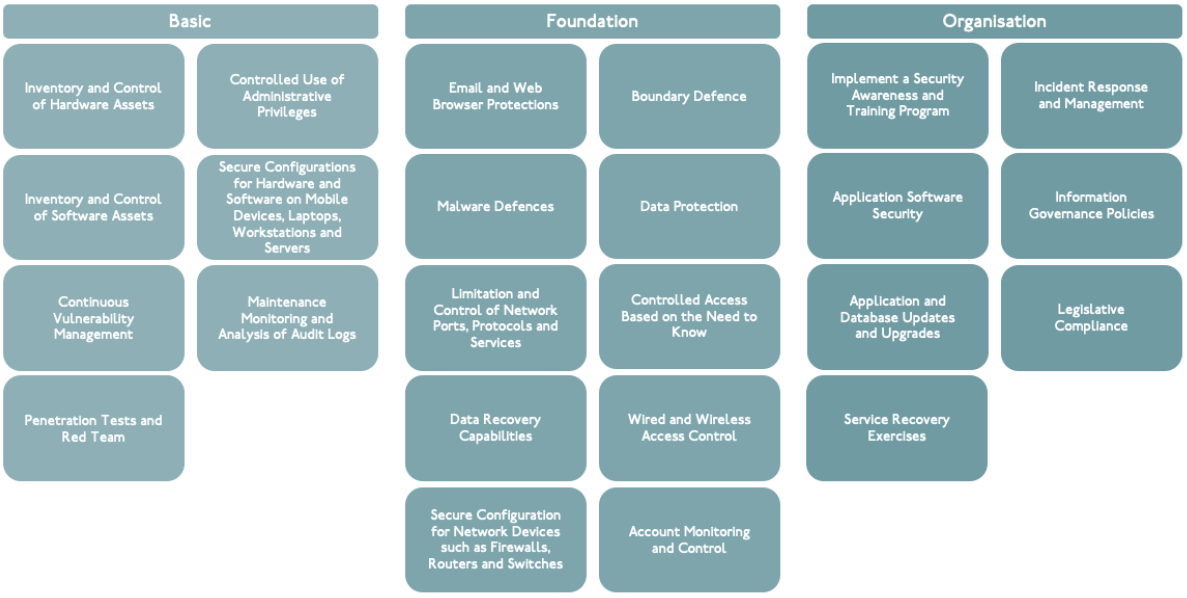
PURPOSE AND SCOPE

STS seeks to enable its partners to deliver its corporate and digital strategies, it is required that we allow our organisations to navigate cyber obstacles. The scale of transformation represents an unprecedented culture shift for staff, residents, partners and businesses. This in turn creates risk.

The Cyber Security Strategy is a new strategy introduced in response to several successful and high-profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to our councils and customers and to explain our commitment in delivering robust information security measures.

Through delivery of this strategy, we will comply with and embed the principles of 'Cyber Essentials'; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

This strategy is intended to cover all partners and customers, the data on the systems we are responsible for, and the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which we implement. It will also set out the best practices that will be rooted in our business as usual.



ASSETS

STS will regularly review the value of all assets across the partnership, ensure that political, social and economic values are considered to place the appropriate levels of protection around those digital and physical assets. Our assets:

- Data
- Services
- Infrastructure

VULNERABILITIES

Vulnerabilities are weaknesses or other conditions in an organisation that a threat actor; such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security.

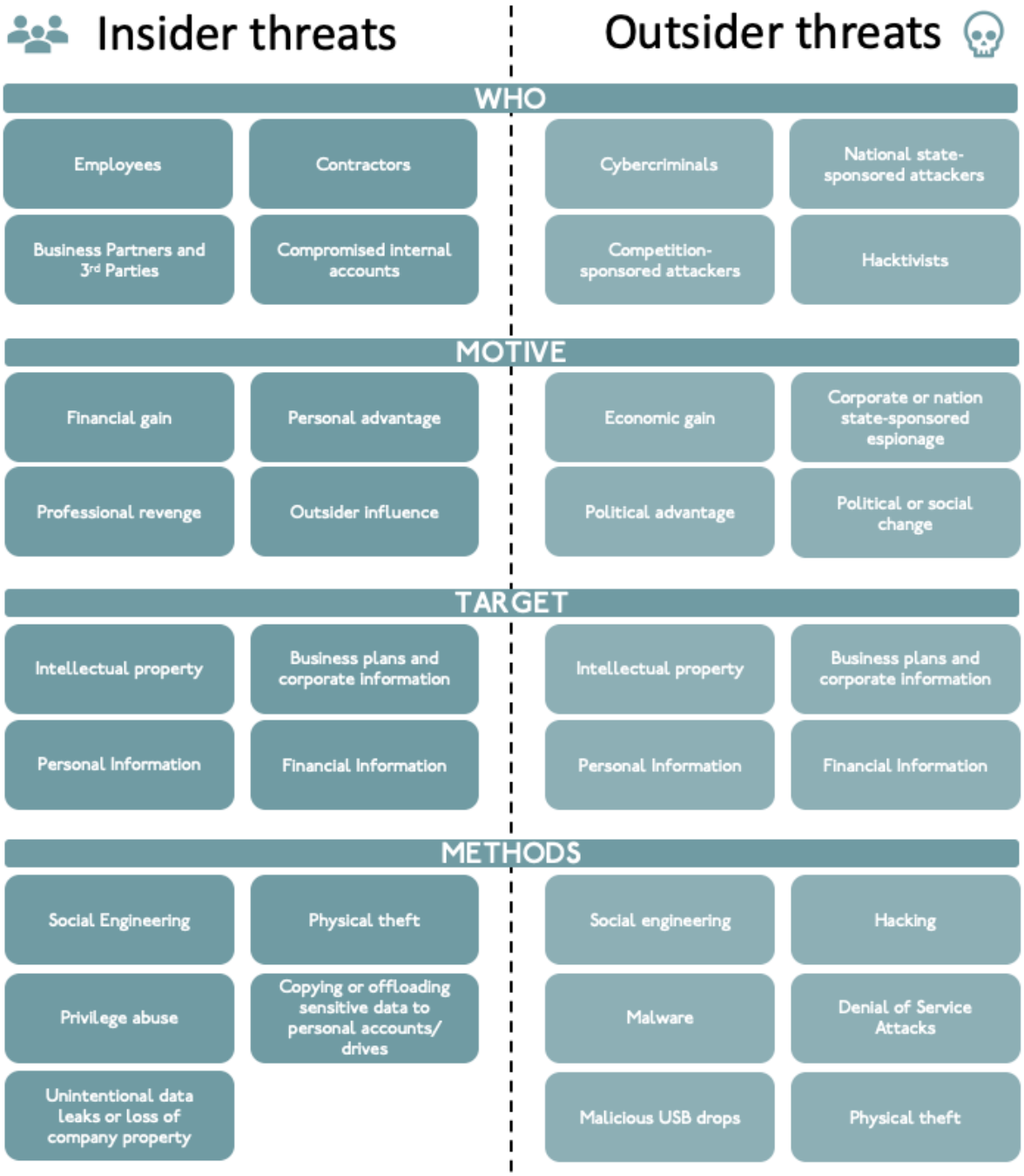
Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organisation uses.

- System Maintenance – IT systems should be updated and checked regularly and effectively. It is essential that the systems are fully updated and appropriate fixes are applied. Poor setup, mismanagement or other issues in the way an organisation installs and maintains its IT hardware and software components is a threat.
- Legacy Software – To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.
- Trend Analysis - The monitoring of organisational working patters to identify unusual behaviour and respond accordingly.
- Training and Skills – It is of paramount importance that all employees have a fundamental awareness of cyber security to support this.

THREATS

If left unchecked, a threat could disrupt the day-to-day operations, the delivery of local public services and ultimately has the potential to compromise national security.

Generally, there are two types of threats. Insider Threats or Outsider Threats they are explained in detail below.



-CYBERCRIMINALS

Generally, cybercriminals are working for financial gain. Most commonly, for the purposes of fraud either by selling illegally gained information to a third party or using directly for criminal means.

Key tools and methods used by cybercriminals include:

- Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid

- Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

-HACKTIVISM

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause.

When targeted against local government websites and networks, these attacks can cause local reputational damage. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in such services.

Hacktivist groups have successfully used distributed denial of service attacks to disrupt the websites of a number of councils already. (DDoS attacks are when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable).

-INSIDERS

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This could be for the purpose of sabotage or in order to sell to another party, but more often than not it is due to simple human error or a lack of awareness about the particular risks involved.

Malicious insider threats may include privileged administrative groups.

-ZERO DAY THREATS

A zero-day exploit is a cyber-attack that occurs on the same day or before a weakness has been discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability.

This poses a risk to any computer or system that has not had the relevant patch applied or the relevant updates to its antivirus software.

-PHYSICAL THREATS

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power failure or other disaster (natural or otherwise).

-TERRORISTS

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

-ESPIONAGE

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic, trade or military negotiations.

RISKS

Cyber Risk Management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified across the councils and appropriate action is carried out to mitigate the risk but also develop effective recovery and containment procedures in the event of an incident.

A risk consists of a threat and a vulnerability of an asset.

OUR APPROACH

To mitigate the multiple threats, we face and safeguard our interests, we need a strategic approach that underpins our collective and individual actions in the digital domain over the next three years. This will include:

- Foster a culture of empowerment, accountability and continuous improvement.
- Prioritising information assets and processes with our councils and customers, maintaining a register and conducting regular reviews including data retention policies.
- Ensuring adequate plans are in place to recover and quickly identify exposure.
- A council wide risk management framework to help build a risk aware culture within each of the councils, ensuring staff understand how to identify and manage risks.
- Cyber Awareness training and principles to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.

The diagram below shows the continual cycle for protecting the councils and its customers for cyber-attacks:

To further enhance the maturity and capability of the service we will be building a Cyber Security team within the Shared Service, this will focus on the delivering the technical controls and guidance to the councils and customers of the Shared Service. This will be led by a new role the Chief Information Security Officer. April 2021 will see a new Target Operating Model start which will ensure that focus is given to the maturity and capacity of the council's defences.

IMPLEMENTATION PLAN

To adapt to the changing landscape and achieve our vision we will align with the National Cyber Security Strategy's approach to defend our, residents, councils and customers and deter our adversaries and to develop our capabilities.

It is recognised that each partner and council will be at different levels of maturity and capacity therefore STS has developed a 5-year (2021-2026) Technology Roadmap in which it will invest a significant number in cyber protections, look for opportunities where we can share, build and grow together but also react to different levels of risk appetite.

DEFEND

STS will have the means to defend against evolving cyber threats, to respond effectively to incidents, and to ensure networks, data and systems are protected and resilient. It includes helping our residents, businesses and partners in gaining the knowledge and ability to defend themselves.

Actions:

- Implementing daily firewalls and scanning services.
- Continue to email hygiene for all partners and enable Attack Targeted Prevention.
- Improve threat correlation and reporting services.
- Ensure vulnerability and patch management is kept up to date.
- Ensuring that Cyber Security is considered in any procurement of solutions.
- Work with councils and customers to ensure websites and line of business systems are kept secure.
- Continue with a 3rd party Security Operations Centre partner to give us the assurance and protection of our systems, using dynamic and Artificial Intelligence (AI) from across the global to identify immediate threats.
- Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes, e.g. Web Check – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils. This is free to use and available to all public sector organisations.
- Identify an STS Red team to be able to respond to incidents and have relationships in place with government agencies and cyber specialists.
- Ensuring that we carryout regular backups and recovery exercises
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN) and the Health and Social Care Network.
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting.
- Comply with The Minimum Cyber Security Standard
- Comply with Data Protection Act 2018 (including the Applied General Data Protection Regulation EU679/2016) and the Freedom of Information Act 2000
- Comply with Section 224 of Local Government Act 1972
- Work towards ISO27001.
- Comply with Access to Health Record Act 1990 and Access to Personal Files Act 1987
- Comply with PCI-DSS requirements for taking electronic payments.

DETER

Our councils and customers will be a desirable target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action against us.

Actions:

- Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
- Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.
- Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts.
- Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high complexity and introduce multi-factor authentication.
- Use of Malware prevention and ensure air gaps or immutable storage.
- Ensure removable media is encrypted to the last levels controls.
- Improve micro segmentation of the network to avoid attackers crossing the network.
- Secure configuration to avoid access to critical information and enabling attackers.
- Introduce cyber awareness and training for users to help detect, deter and defend against the cyber threats.

DEVELOP

This includes developing a co-ordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.

Actions:

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud
- Process, procedures and controls to manage changes in cyber threat level and vulnerabilities
- Managing vulnerabilities that may allow an attacker to gain access to critical systems
- Operation of the council's penetration testing programme; and Cyber-incident response
- Introducing training for staff and elected members
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities
- Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive)

- Develop a network of sharing with other councils and customers, collaborate and learn from each other, harness networks such as London Office of Technology and Innovation, London CIO council, WARP, IGfL and ISfL.

REACT

STS will ensure that we have the sufficient controls in place to respond to an attack and furthermore have the organisational channels and processes to make efficient decisions further protecting our data and limiting any scope of an attacker.

We have third parties proactively monitoring our environment disabling any potential threats and locking down resources which are identified as a risk.

SUCCESS FACTORS

Throughout this period of challenging transformation, the councils have committed to delivering robust information security measures to protect our data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

To continue to provide assurance on the effectiveness and robustness of STS's arrangements for IT security, we will:

- Develop appropriate cyber security governance processes
- Develop a Cyber Risk Management Framework
- Develop policies/procedures to review access on a regular basis
- Create a cyber-specific Business Continuity Management Plan and/or Incident Plan to include emergency planning for cyber attack
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents shall be recorded regardless of the need to report them
- Set up a Playbook to have test incidents on a regular basis; to ensure reaction to incidents where an incident is triggered
- Create standard test plans with security testing as a standard
- Reconcile current systems in place and last times these were reviewed (build into Enterprise Architecture)
- Review vendor management – process of assessments of third parties
- Explore Active Cyber Defence tools and new technologies to ensure partners have the best solutions to match to threats
- Apply the governments cyber security guidance – 10 Steps to Cyber Security
- Provide relevant cyber security training for staff and elected members
- Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises
- Comply with the Governments Public Sector Network (PSN) Code of Connection and Payment Card Industry (PCI) standards; a minimum requirement for all systems used, audit trails, deletion of data etc.
- Protect enterprise technology by working with specialist partners to develop model architecture and review audit logs to reduce chances of threats

ROLES AND RESPONSIBILITIES

Information Governance and Policy will remain the responsibility of the councils and customers and the Shared Service will work with those teams to ensure that shared understanding and collaboration is met.

Effective cyber security governance in STS is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)
A nominated Senior Information Risk Owner (SIRO) is responsible for the governance of cyber security and information risk within the Council. This includes ensuring that information governance risk is managed in accordance with GDPR.

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.

Joint Committee (JC)
The Joint Committee is made up of the lead councillors for IT. The Joint Committee will sponsor the Cyber Security Strategy and oversee the strategic framework through which the council governs its information resources and in turn agree and receive updates on implementation of the Cyber Security Strategy.

Joint Management Board (JMB)
The Joint Management Board is responsible for the strategic direction of the shared service and is made up of the executive directors from each council and the Managing Director of the shared service. This board is responsible for holding the shared service to account on the delivery of its obligations in turn the protection of its data and systems.

Operational Management Board (OMB)
The Operational Management Board is responsible for the day-to-day tracking of tasks and deliverables, this board will allocates resources and funds necessary to deliver the protection to the councils and its customers. The board is made up of Heads of IT from each council and the Senior Leadership Team of the shared service.

Information Governance Group (IGG)
The IGG is comprised of senior representatives from each council area. The group are responsible for overseeing the delivery of the Cyber Security Strategy and monitoring its effectiveness.

Technical Design Authority (TDA)
The Technical Design Authority (TDA) make decisions regarding technical implementations for projects. This includes ensuring that cyber security implications are properly considered.

Information Asset Owners (IAO)
Information Asset Owners are responsible for all processing of personal data within their business area.

All council officers
It is the responsibility of all officers to comply with the standards set out in this Cyber Security Strategy