Neath Port Talbot
Castell-nedd Port Talbot
County Borough Council Cyngor Bwrdeistref Sirol

AGENDA

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

IMMEDIATELY FOLLOWING CABINET (POLICY AND RESOURCES) SCRUTINY COMMITTEE
TUESDAY, 9 APRIL 2024

MULTI-LOCATION MEETING – COUNCIL CHAMBER PORT TALBOT AND MICROSOFT TEAMS

ALL MOBILE TELEPHONES TO BE SWITCHED TO SILENT FOR THE DURATION OF THE MEETING

Webcasting/Hybrid Meetings:
This meeting may be filmed for live or subsequent broadcast via the Council's Internet Site. By participating you are consenting to be filmed and the possible use of those images and sound recordings for webcasting and/or training purposes.

Part 1

1. Appointment of Chairperson

2. Chairpersons Announcement/s

3. Declarations of Interest

4. Minutes of Previous Meeting *(Pages 3 - 4)*

5. Public Question Time
Questions must be submitted in writing to Democratic Services – democratic.services@npt.gov.uk – no later than two working days prior to the meeting. Questions must relate to items on the agenda. Questions will be dealt with in a 10 minute period.

Matter/s for Decision:

6. Council Tax and Business Rates Court Costs 2024-2025
(Pages 5 - 8)

7. Neath Port Talbot Cyber Security Strategy Update 2024
(Pages 9 - 36)

8. Urgent Items
Any urgent items (whether public or exempt) at the discretion of the Chairperson pursuant to Regulation 5(4)(b) of Statutory Instrument 2001 No. 2290 (as amended).

9. Access to Meetings - Exclusion of the Public *(Pages 37 - 42)*
To resolve to exclude the public for the following items pursuant to Regulation 4 (3) and (5) of Statutory Instrument 2001 No. 2290 and the relevant exempt paragraphs of Part 4 of Schedule 12A to the Local Government Act 1972.

Part 2

Matter/s for Decision:

10. Write off of Debts (Exempt Under Paragraph 14) *(Pages 43 - 52)*

K.Jones
Chief Executive

Civic Centre
Port Talbot

3 April 2024

Cabinet (Policy and Resources) Sub Committee Members:

Councillors. S.K.Hunt, S.A.Knoyle and A.Llewelyn

EXECUTIVE DECISION RECORD

20 FEBRUARY 2024

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

Cabinet Members:

Councillors: S.K.Hunt (Chairperson), S.A.Knoyle and A.Llewelyn

Officers in Attendance:

N.Daniel, H.Jones, A.Thomas and T.Davies

Scrutiny Chair: Councillor C.Jordan

---

1. APPOINTMENT OF CHAIRPERSON

Agreed that Councillor S.K.Hunt be appointed Chairperson for the meeting.

2. CHAIRPERSONS ANNOUNCEMENT/S

The Chair welcomed all to the meeting.

3. DECLARATIONS OF INTEREST

No declarations of interest were received.

4. MINUTES OF PREVIOUS MEETING

That the minutes of the previous meeting, held on 9 January 2024, be approved.

5. PUBLIC QUESTION TIME

No Public Questions were received.

6. ACCESS TO MEETINGS - EXCLUSION OF THE PUBLIC

RESOLVED: That pursuant to Regulation 4 (3) and (5) of Statutory Instrument 2001 No. 2290, the public be excluded for the following item of business which involved the likely disclosure of exempt information as defined in Paragraph 14 of Part 4 of Schedule 12A of the Local Government Act 1972.

7. DEBTOR WRITE OFFS
8.

Decision:

That the Debtor Write Offs, as detailed in the Private, circulated report, be approved.

Reason for Decision:

To enable the Council to write off irrecoverable accounts.

Implementation of Decision:

The decision will be implemented after the three day call in period.

CHAIRPERSON

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

Neath Port Talbot Council

Cabinet (Policy and Resources) Sub Committee

REPORT OF THE CHIEF FINANCE OFFICER – H.Jones

9th April 2024

MATTERS FOR DECISION:

Council Tax and Business Rates Court Costs 2024/2025

WARDS AFFECTED:

All

1 Purpose of Report

To determine the level of costs to be recovered from council taxpayers and business rates payers in respect of the issue of summonses and the granting by the Magistrates of liability orders.

2 Background

The Council Tax (Administration & Enforcement) Regulations and the Non Domestic Rating (Collection & Enforcement) Regulations 1989 allow the council to levy an additional fee which is equal to the amount of costs reasonably incurred in making an application for a Liability Order through the Magistrates. Reasonable costs are not defined in the regulations, but should reflect the cost to the Council of the processes undertaken in obtaining the Liability Order. The costs are capped at £70 in legislation.

The Council Tax costs charged have not increased since 2018, they currently stand at –

On the issue of a summons	£44.00
On the granting of a liability order	£19.00

The Business Rates costs are currently at the maximum level of £70.00 which are split as follows –

On the issue of a summons	£41.00
On the granting of a liability order	£29.00

3 Proposed Costs

It is proposed that the Business Rates costs remain unchanged as detailed above.

It is proposed that the Council Tax costs increase as detailed below –

On the issue of a summons	£45.00
On the granting of a liability order	£20.00

4. Financial Impact

No impact.

5. Integrated Impact Assessment

There is no requirement to undertake an integrated impact assessment.

6. Valleys Communities Impacts

No impact.

7. Workforce Impacts

No Impact.

8. Legal Impact

No impact.

9. Risk Management Impact

No Impact.

10. Consultation

This item is not subject to external consultation.

11. Recommendations

It is recommended that the costs charged in relation to court action in the recovery of Council Tax and Business Rates are for 2024/25 are as follows –

Council Tax	
On the issue of a summons	£45.00
On the granting of a liability order	£20.00

Business Rates	
On the issue of a summons	£41.00
On the granting of a liability order	£29.00

12. Reason for proposed decision

To allow for the relevant costs be to charge in the issuing of a summons and obtaining a liability order.

13. Implementation of Decision

The decision is proposed for implementation after the three day call in period.

14. Appendices

None

15. Background Papers

The Council Tax (Administration & Enforcement) Regulations and the Non Domestic Rating (Collection & Enforcement) Regulations 1989

16. Officer Contact

Mr Huw Jones – Chief Finance Officer
E-mail: h.jones@npt.gov.uk

Mrs Ann Hinder –Principal Council Tax Officer

E-mail: a.hinder@npt.gov.uk

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB-COMMITTEE

9 April 2024

Report of the Chief Digital Officer – C.Owen

Matter for Decision

Wards Affected: All Wards

Neath Port Talbot Cyber Security Strategy Update 2024

Purpose of the Report:

1. To provide Policy and Resources Sub-Committee Members with an update on the implementation of the Neath Port Talbot Council's Cyber Security Strategy and to seek their continued support.

Executive Summary:

2. The NPT Cyber Security Strategy has been developed to support council's approach to protecting its information systems, the data held within them, and the services they provided from unauthorised access, harm or misuse - a copy of the strategy is attached at Appendix 1.

3. This report provides an update on the actions taken in the second year of the multi-year cyber security action plan, which underpins the delivery of the strategy. An updated copy of the action plan is attached at Appendix 2.

Background

4. Since the approval by Members of our council's Cyber Security Strategy in January 2022, the world of cyber security has continued to evolve at pace.

5. The global cyber threat has continued to grow since our last report in March 2023, with most incidents (89%) still containing a human element. This

includes people being involved either via ‘Social Engineering’, ‘Privilege Misuse’ or the use of stolen credentials.

6. Financial gain remains the overwhelming motivation (globally 95% of all attacks). Ransomware continues to be the most prevalent goal of cyber criminals to extort money from organisations of all sizes and in all industries.

7. With the ongoing Ukraine war, the Israel / Hamas conflict, and the developing attacks on shipping in the Red Sea, there has been a continued spike in cyber activity in the war zones and against the allies of Ukraine and Israel.

8. Some hopeful news is the International Committee of the Red Cross (ICRC) has, for the first time, published rules of engagement for civilian hackers involved in conflicts. The eight rules include bans on attacks on hospitals, hacking tools that spread uncontrollably and threats that engender terror among civilians.

9. For the last year the United Kingdom has seen a continuation of high-profile attacks totalling 2005, this is the highest number ever reported to National Cyber Security Centre (NCSC) a year-on-year increase of 64%.

10. This number includes attacks on Critical National Infrastructure including water companies, power generation centres, and internet connectivity providers.

11. In the public service arena, Canterbury, Dover, and Thanet councils, with a combined population of almost 500,000 residents were jointly investigating an unspecified “cyber incident” that had caused major disruption in January 2024 to council tax payments and online forms. Investigations are ongoing.

12. Whilst NPT council has not been hit by a major cyber incident, there remains an ever-present threat of phishing attempts and other malicious actions against the council.

13. In July 23 the council’s ‘Any Connect Portal’ was subject to a combination of brute force and password spraying attack. This attack attempted to gain unauthorised access to the network, by attempting various combinations of user account names and passwords.

14. The attack was detected within the logs and as an initial precaution access to the portal(s) was disabled whilst the situation was assessed.

15. Counter measures were then implemented to block the source of the attack and further steps taken to help block similar such attacks in the future.

What are we doing to protect our Digital Services?

16. The councils new Digital Data and Technology Strategy was approved by Council in July 2023, with clearly defined themes, aims, and objectives, ensuring a golden thread of cyber security throughout.

17. The Welsh Government has published its Cyber Action Plan for Wales. The plan is a high-level document and officers can confirm that both the council's digital strategy and cyber security strategy align closely to its objectives.

18. The Cyber Resilience Centre for Wales (WCRC) and Welsh Government have teamed up to launch a new, free initiative for the Welsh social care sector that offers organisations the chance to receive cyber security training. Members have benefitted directly, attending the award-winning Cyber Ninjas for councillors training, increasing their understanding and awareness. We have been liaising with WCRC to ensure we leverage their content and experience where possible.

19. Throughout the year our information governance team have been running information campaigns from cyber security awareness month (with daily and weekly themed communications) to cyber security holiday awareness events (highlighting festive scams and phishing tips and tricks).

20. We have updated the council's password policy ensuring we adopt a policy that strikes a balance between strong security, usability, and industry best practice compliance. The policy has been rolled out and communicated across the council with no service effecting issues.

21. Digital Services have developed comprehensive cyber playbooks (CSOP – Cyber Standard Operating Procedure), which outline the steps the council will take in the event of a cyber-incident. The playbooks cover several specific cyber threats and provide incident managers and stakeholders with a consistent approach to follow when remediating an incident.

22. It is intended to create a working group to review and update the existing playbooks to ensure that they continue to be fit for purpose and to identify if any additional playbooks are required as new threats emerge.

23. The present Cyber Security Strategy action plan has been updated and can be seen in Appendix 2 showing our progress to date. In 2024 Digital

Services plans to review and update the Cyber Security Strategy against the council's Digital Strategy and the global cyber landscape. This review will ensure that the Cyber Strategy remains fit for purpose, providing the Council with a firm foundation to continue building its cyber defences.

What else are we planning to do?

24. As part of our ongoing Cyber Security Strategy, we are currently in the process of implementing an Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS). These systems will constantly monitor and survey the council network to actively identify potential security incidents, stop those incidents, and alert Digital Services staff to undertake further action where necessary.

25. The automation provided by an IDS/IPS solution is a lot more efficient than trying to carry out the processes manually. It provides an additional layer of security and is essential to meet compliance requirements, enhanced incident handling, and increase network visibility.

26. Utilising the benefits of an IDS/IPS including early threat detection, compliance support, enhanced incident handling, and network visibility significantly improves the council's position. With an IDS/IPS being recognised as a vital tool in helping an organisation protect their networks and sensitive data in today's digital landscape, where cyber threats are ever-increasing and growing more sophisticated by the day.

27. The Welsh Security Operations Centre (Cymru SOC) will provide a protective, virtual 24/7/365 "cyber umbrella" over the Authority, bringing additional cyber resilience, protecting against threats, sharing intelligence feeds on threats, and feeding that intelligence to and from the NCSC. We continue to engage with the Welsh Government Cyber Resilience team on the project. Connectivity with the future SOC is an important requirement of the current Security Event and Incident Management (SIEM) project.

28. Throughout this year the team will be developing a council wide cyber awareness program. This program will take advantage of Welsh Government, Socitm, WARP (Warning, Advice and Reporting Point), and other public sector organisations content and training augmented by home grown content that will provide a platform for ongoing employee education. This will go some way to mitigating the 89% of the human involvement in all cyber incidents.

Summary

29. Whilst the cyber treat landscape continues to evolve and grow year-on-year, the activities highlighted above both completed and planned provide the council with a sound approach to its defence.

30. The key factor for the coming year will be the introduction of the Cymru SOC. This will be the keystone to the future of the Welsh Governments Cyber standards and play a pivotal role in how the council manages cyber security going forward.

Financial Impacts:

31. There are no financial impacts associated with this report.

Integrated Impact Assessment:

32. There is no requirement to undertake an Integrated Impact Assessment.

Valleys Communities Impacts:

33. There are no valley communities impacts associated with this report.

Workforce Impacts:

34. There are no workforce impacts associated with this report.

Legal Impacts:

35. There are no legal impacts associated with this report.

Risk Management Impacts:

36. There are no risk management impacts associated with this report.

Consultation:

37. There is no requirement for external consultation on this item.

Recommendations:

38. Members continue their support for the Neath Port Talbot Council Cyber Security Strategy and action plan as set out in Appendix 1 and Appendix 2.

Appendices:

Appendix 1 - NPT Cyber Security Strategy
Appendix 2 - NPT Cyber Security Action Plan Update 2024

List of background papers: None

Officer Contact:

Chris Owen
Chief Digital Officer
Tel: 01639 686217
c.m.owen@npt.gov.uk

Alan Tottman
Head of Digital Strategy and Governance
a.tottman@npt.gov.uk

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NPTCBC

Cyber Security Strategy

Version: 2.0
Publish Date: December 2021
Review Date: December 2023
Next Review: December 2024
Owner: Chief Digital Officer

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

Table of contents

1. Introduction

We live in a world characterised by interconnecting data, constantly evolving and empowering us to make better informed decisions. Information and data are vital to every part of the work of a Local Authority. As we deliver against the objectives in our Smart & Connected Digital Strategy, we are transforming the way we work and how our residents, business and wider stakeholders access information and services. As a result, we need increasingly robust security measures to protect against cyber threats.

Across the world, cyber-attacks are growing more frequent and sophisticated. Public sector organisations are not immune to the rise in cyber incidents and when they succeed, the damage can be life-altering, with severe personal, economic and social consequences.

This Cyber Security Strategy sets out Neath Port Talbot County Borough Council's approach to protecting our information systems, the data held within them, and the services they provide from unauthorised access, harm or misuse. This ensures the services we provide are secure and our residents, businesses and wider stakeholders can safely interact with us. It requires a balance of embracing digital opportunities, including making information more widely available and accessible, whilst ensuring that the right levels of protection are in place.

In order to obtain strong cyber security, the Council must ensure it promotes a comprehensive risk-based approach to cyber security, which is integrated across personnel, technical security, information assurance and physical security which strategically encompasses Information Security, Assurance, Resilience and Governance.

This approach is in line with the HMG Cyber Security standard, the Public Services Network (PSN) code of connection and National Cyber Security Strategy of 'Defend, Deter, Develop'.

2. Purpose and scope of the strategy

The purpose of this strategy is to give assurance to residents, businesses and other stakeholders of the Council's commitment to delivering robust information security measures to protect resident and stakeholder 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. The strategy supports delivery of the wider Digital Strategy by providing a framework for the Council to securely harness the benefits of digital services for the benefit of all stakeholders.

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.

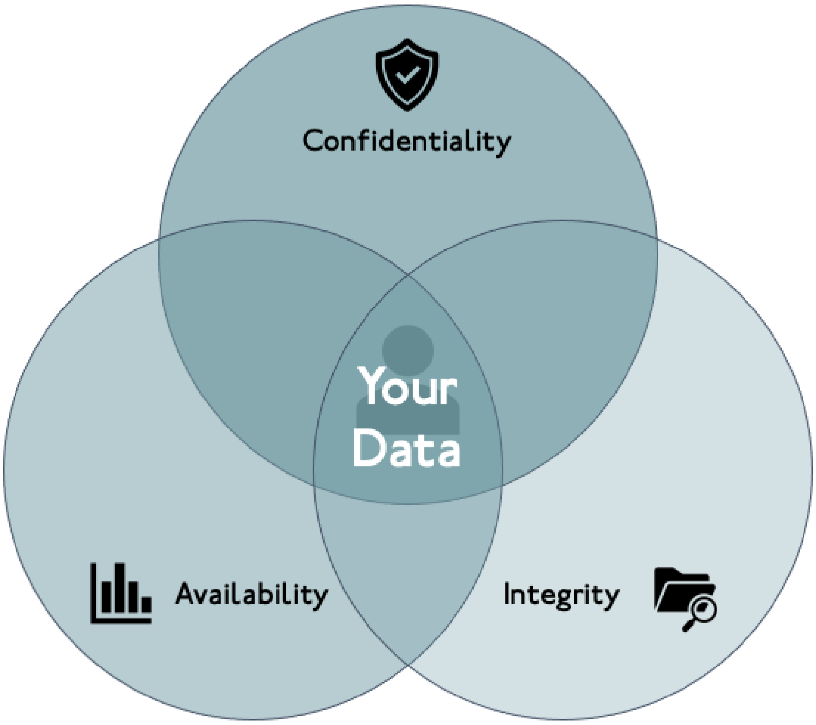
This strategy is intended to cover all partners and customers, the data on the systems we are responsible for and the services they help provide. The recommendations in this strategy will be embedded in all areas of new and emerging technologies which we implement. It will also set out the best practices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

The strategy will sit alongside other Council strategies such as the Information Governance Strategy and is supported by a suite of operational policies (Acceptable usage policy, Information Security Policy, IT Security Policy, Removable Media Policy, Mobile Device Policy and Information Security Breach Policy) and Incident Response Playbooks (Denial of Service, Phishing, Malware etc.)

3. 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 unauthorised copying of 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.

It is important because, in order to effectively deliver services, we all process and store large amounts of data on computers and other devices, with a significant portion of this data being classified as sensitive information. It will also include financial, personal and other types of information, 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. 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 also crucial in ensuring our services continue to operate. It is a core element of building and keeping our stakeholders trust. A cyber-attack would potentially have very serious consequences in terms of disruption to our services (many of which serve some of our most vulnerable residents), the Council's reputation and impact to our financial position.

4. The challenge we face as a Council

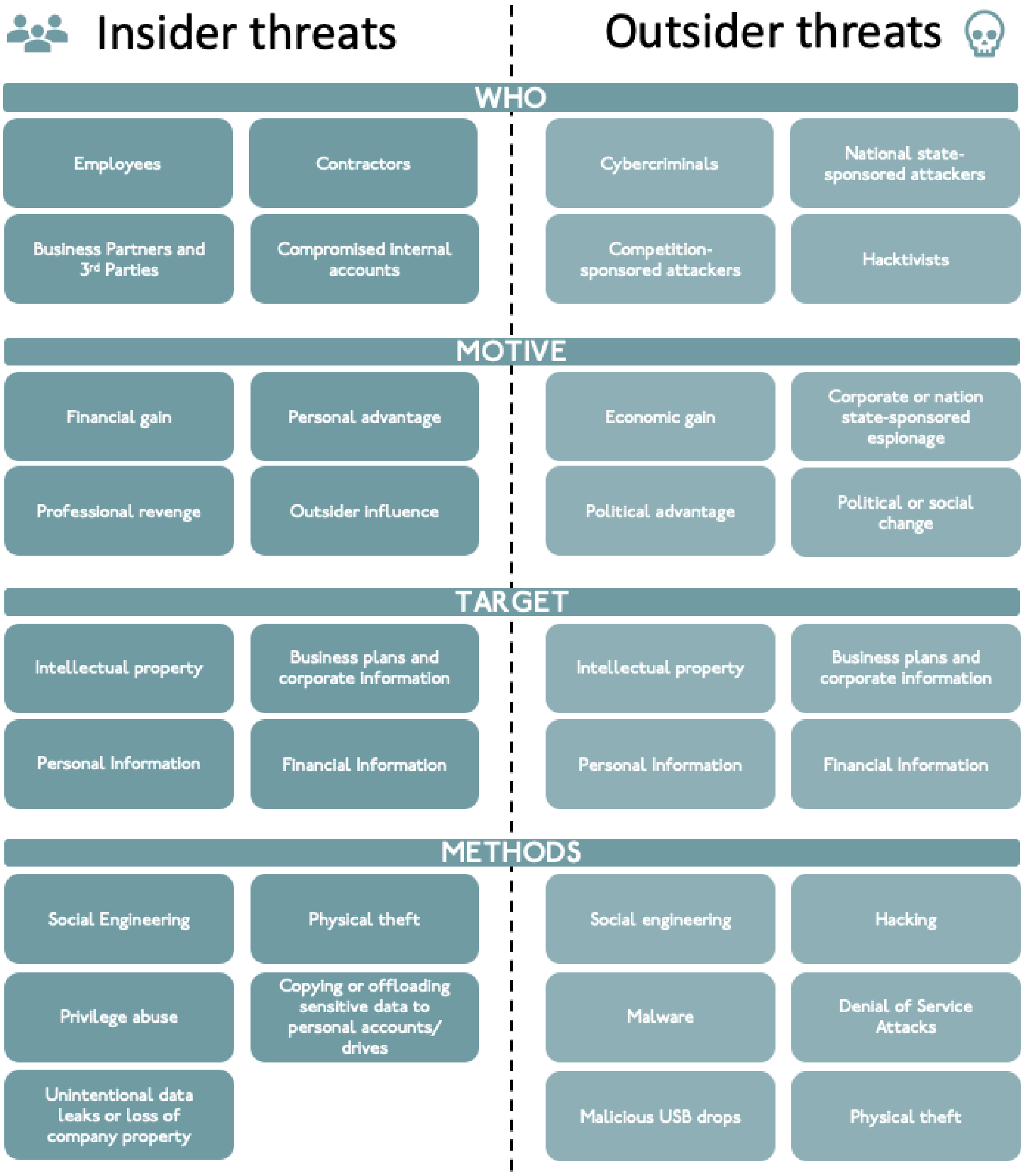
We are using an increasing range of technology, from 'apps' and 'the cloud', to different devices and 'gadgets'. Much of our business is online - corresponding with residents and local businesses, carrying out case work, and reviewing reports and papers for Council meetings.

This direction of travel is expected to continue and accelerate; making effective cyber security ever more crucial in protecting against new types of threats, risks and vulnerabilities.

Threats - A threat if left unchecked, could disrupt the day-to-day operations of the Council, and the delivery of local public services.

Types of Threats

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



Insider threats		Outsider threats	
WHO			
Employees	Contractors	Cybercriminals	National state-sponsored attackers
Business Partners and 3rd Parties	Compromised internal accounts	Competition-sponsored attackers	Hacktivists
MOTIVE			
Financial gain	Personal advantage	Economic gain	Corporate or nation state-sponsored espionage
Professional revenge	Outsider influence	Political advantage	Political or social change
TARGET			
Intellectual property	Business plans and corporate information	Intellectual property	Business plans and corporate information
Personal Information	Financial Information	Personal Information	Financial Information
METHODS			
Social Engineering	Physical theft	Social engineering	Hacking
Privilege abuse	Copying or offloading sensitive data to personal accounts/ drives	Malware	Denial of Service Attacks
Unintentional data leaks or loss of company property		Malicious USB drops	Physical theft

Cyber Criminals and Cyber Crime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either 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.

We have already developed Cyber Incident Playbooks for each of these situations.

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 (DDoS) 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.

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

We must ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.

Training and Skills

It is crucial that all employees have a fundamental awareness of cyber security. Accountable managers are responsible for ensuring all their employees have completed the appropriate training.

Assets

We regularly review the value of all assets across the Council in line with legislative requirements, to ensure that the appropriate levels of protection are placed around those digital and physical assets. Our assets include:

- Data
- Services
- Infrastructure

Risks

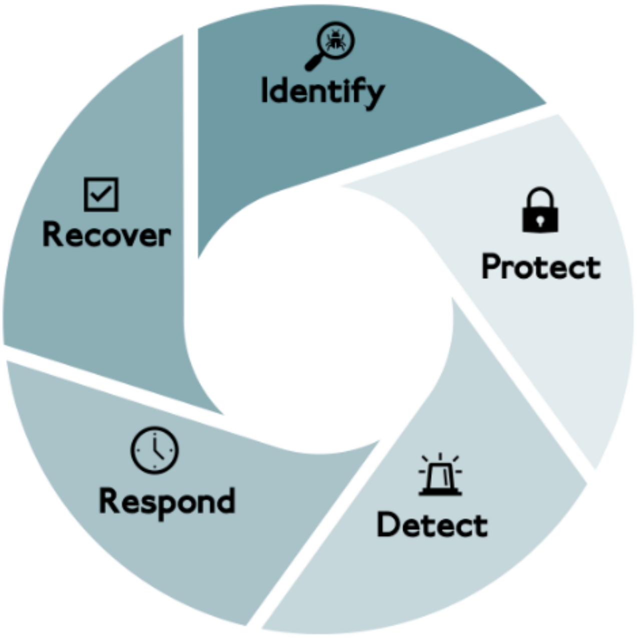
Cyber Risk Management is a fundamental part of the broader risk management. It ensures cyber security challenges are fully identified across the Council and appropriate action is carried out to mitigate the risk, but also to develop effective recovery and containment procedures in the event of an incident.

5. Our approach, principles and priorities

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

- Fostering a culture of empowerment, accountability and continuous improvement.
- Prioritising information assets and processes, maintaining appropriate records and policies and conducting regular reviews including data retention policies.
- Ensuring adequate procedures and plans are in place to recover and quickly identify exposure.
- Embedding a Council wide risk management framework to help build a risk aware culture, ensuring staff understand how to identify and manage risks.
- Delivering Information Security 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 Council and its service users from cyber-attacks:



Identify

- Identify and catalogue sensitive information and key operational services.
- Understand and manage user access to key operational services.
- Review through Information and Cyber Security Governance Processes.

Protect

- Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems.
- Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.
- High privileged accounts shall not be vulnerable to common cyber-attacks.

Detect

- Steps are taken to detect cyber-attacks.
- Monitor key areas and activities.

Respond

- A rapid response to incidents.
- A defined, planned and tested response to security incidents that impact personal, sensitive or confidential information, leveraging a multi-disciplinary response team.

Recover

- Identification and testing of contingency mechanisms to ensure critical service delivery continues.
- Restoration of services to normal operation.
- Lessons learned fed back into the process.

6. 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 the Council, residents, businesses and wider stakeholders, deterring potential threats and developing our capabilities – Defend, Deter and Develop.

Defend

The Council will further develop 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:

- Maintaining firewalls and scanning services.
- Continue to develop end-point protection (Anti-Virus, USB Encryption and MDM).
- 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.
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN).
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting.

Deter

The Council will be a hard target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action against the Council.

Actions:

- **Governance**
  - Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
  - Review (update where appropriate) policies and procedures.

- **Technology and information**
    - Ongoing review of network security.
    - 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.
    - Malware prevention.
    - Removable media controls.
    - Secure by design configuration.
- Review and update plans and guidance.
- Training or educating users to help detect, deter and defend against the cyber threats.

Develop

The Council will continually develop this innovative cyber security strategy to address the risks faced by our residents, businesses and wider stakeholders.

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.
- 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.

- Develop a network of sharing with other Councils, collaborate and learn from each other, harness networks such as, WARP and CiSP.

7. Critical Success Factors

Throughout this period of challenging transformation, the Council has committed to delivering robust information security measures to protect residents and stakeholder 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 the Council's arrangements for information security, the Council will:

- Develop appropriate cyber security governance processes.
- Develop a Council wide Cyber Risk Management Framework.
- Develop policies/procedures to review access on a regular basis.
- Create a cyber-specific Business Continuity Management Plan and/or review our 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 we have the best solutions to match to threats.
- Apply the Government's 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.

8. Cyber Security Governance - Roles and Responsibilities

Effective cyber security governance at the Council is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO), is the Chief Digital Officer. The 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 legal requirements.

However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all users having a role to play.

Corporate Director's Group (CDG)

CDG will take an overview of the Cyber Security Strategy via regular updates from the SIRO, where progress and risks are reported.

Corporate Governance Group

The Corporate Governance Group will have reporting and monitoring oversight of Cyber Security threats that have been experienced across the Council. They will also deal with any Cyber Security escalation matters.

Information Security Group (ISG)

The group is comprised of senior representatives from each service area. The group are responsible for overseeing the delivery of the Information, Cyber Security and related Strategies and monitoring their effectiveness.

Data Protection Officer (DPO)

The Council's Data Protection Office (DPO), is the Head of Legal and Democratic Services. The DPO leads on overseeing the Council's implementation of data protection legislation (UK GDPR and the Data Protection Act 2018). They take an assurance view that progress is being made in adoption and implementation of the Cyber Security Strategy, and commission the undertaking of Audits of Information Security as appropriate.

Security and Operations Team

The Security team will lead on the implementation of the Cyber Security Strategy, preparing regular feedback and updates not only on progress regarding implementation of the tasks identified but also provide an informed view of the threat landscape overall.

Information Governance Team

The Information Governance team will lead on information security incident investigations that are not serious cyber security incidents which are dealt with under the cyber incidence response plan and hold the corporate information security incident register.

The team will be part of all initiatives to provide information security, data protection and information management advice and recommendations ensuring that potential issues are identified and escalated to the relevant area.

Information Asset Owners

Information Asset Owners are responsible for all processing of personal data within their business unit/service area. They are identified by the Information Governance team.

All Council staff / users and Elected Members

It is the responsibility of all staff / users and Elected Members to comply with the standards set out in this Cyber Security Strategy and within supporting Policies, such as, but not limited to Members ICT Scheme, Information Security and Acceptable Usage Policy.

Appendix A: Standards

Information Security Management within Neath Port Talbot County Borough Council will comply with appropriate standards. These include the Governments' Cyber Essentials certification for Cyber Security, the Public Services Network Code of Connection and PCI DSS.

The standard specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the Council's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of the Council.

Appendix B: NCSC: 10 Steps to Cyber Security

Risk Management Regime

Embed an appropriate risk management regime following standards, across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Secure configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

Network security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many 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, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

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 should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

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 can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

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. You should identify recognised sources (internal or external) of specialist incident management expertise.

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 your 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.

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 you 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.

Removable media controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

Home and mobile working

Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 1	Defend / Technology	Maintain firewall and scanning services.	100%	Apr-23		Jan-23	
AP - 2	Defend / Technology	Maintenance of end-point protection for devices – Anti Virus, USB Encryption and Mobile Device Management.	67%	Estimated End 2024			
AP - 3	Defend / Technology	Undertake Cyber Security Health Checks and Penetration Testing.	67%	Sep-23	Dec-24		On further investigation a wider scope assessment is to be undertaken which has increased the completion date to December 2024
AP - 4	Defend / Technology	Utilisation of the National Cyber Security Centre tools. WebCheck and Mail Check.	75%	Nov-23	Nov-23		CF to check with RF and make the change if not done already.
AP - 5	Defend / Governance	Meet compliance regimes which require good Cyber Hygiene (Public Service Network Code of Connection, Cyber Essentials).	83%	Apr-24	Mid 2025		Due to delays in other elements of work this is beginging in April 2024, and is expected to run into 2025 and will be embedded into our rolling program of infrastructure modernisation.
AP - 6	Defend / Governance	Be an active member of the public sector cyber security community. Participation in the Cyber Security Information Sharing Partnership (CiSP) and Wales Local Authority Warning, Advice and Reporting Point.	100%	May-23		23-May	
	Deter / Technology	Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions.	25%	End of 2023	Dec-24		The development and management of polices has transition into business as usual work and as a result is no longer part of the Cyber Security Action Plan.

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 1	Deter / Technology	Reconcile current systems in place and last times these were reviewed.	25%	Mar-24	late 2024		Resource commitments have resulted in this being moved to late 2024.
AP - 2	Deter / Technology	Protect enterprise technology by working with specialist partners to develop model architecture.	100%	Apr-23		23-Apr	
AP - 3	Deter / Technology	Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services.	50%	Mid 2024			Resource commitments have resulted in this being moved to late 2024.
AP - 4	Deter / Governance	Embed the Secure by Design principle throughout.	100%	Apr-23		23-Oct	
AP - 5	Deter / Governance	Review vendor management to address supply chain risk.	50%	Mid 2024	late 2024		Resource commitments have resulted in this being moved to late 2024.
AP - 6	Deter / Governance	Review (update where appropriate) policies and procedures.	13%	Mid 2024	Dec-24		The development and management of polices has transition into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 7	Develop / Technology	Explore Active Cyber Defence tools and new technologies to ensure we have the best solutions to match to threats.	50%	On hold pending WG SOC review			The main pieces of work are waiting on WG. In the meantime we have started implementation of IDS/IPS and a local Security Incident and Event Monitoring system.

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 8	Develop / Technology	Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.	33%	Pending WG direction			WLGA Cyber Resilience workshop taking place on 14/03/2024. WG events waiting on further information from WG.
AP - 9	Develop / Governance	Provide relevant cyber security training for staff and elected members to help detect, deter and defend against the cyber threats.	86%	Feb-24	Apr-24		In process to be completed by end of April 2024.
AP - 10	Develop / Governance	Develop and maintain a risk management framework, internal controls and governance mechanisms. Process, procedures and controls to manage changes in cyber threat level and vulnerabilities.	25%	End of 2023	late 2024		Current Risk Management approach utilises the corporate Risk Management framework which is undergoing modification. Intention to dovetail into this for completion by end of 2024.
AP - 11	Develop / Governance	Aligned with best practice, develop a minimum requirement for all systems used, audit trails, deletion of data etc.	50%	May-23	Apr-24		With the extraordinary changes in global digital landscape (AI) and these needing to be reflected in the process, the completion will be the end of April 2024
AP - 12	Develop / Governance	Develop a communication plan in the event of an incident, which includes notifying the senior accountable individuals, the communication team, statutory notification bodies and relevant external organisation and law enforcement as applicable.	100%	Oct-23		Nov-23	
AP - 13	Develop / Governance	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.	100%	Delivered		Aug-23	

Action Plan - Cyber Security Strategy

ID	Area	Observation	% Complete	Expected Completion Date	Revised Completion Date	Actual Completion Date	Notes
AP - 14	Develop - Governance	Create a cyber-specific Business Continuity Management Plan and/or review our Incident Plan to include emergency planning for cyber-attack.	100%	End of 2023		Dec-23	The development and management of business continuity plans has transitioned into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 15	Defend / Technology	Maintain firewall and scanning services.	0%	Aug-23	Pending WG direction		The main pieces of work are waiting on WG. In the meantime we have started implementation of IDS/IPS and a local Security Incident and Event Monitoring system.
AP - 16	Defend / Technology	Maintain firewall and AD scanning.	100%	Apr-24		Feb-24	The management of AD scanning has transitioned into business as usual work and as a result is no longer part of the Cyber Security Action Plan.
AP - 17	Develop - Governance	AI Strategy - New, added April 2024	0%	Mid-Late 25 ***(NEW)***			Mid-late 2025

Agenda Item 9

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

Report of the Head of Legal and Democratic Services

Cabinet (Policy and Resources) Sub Committee – Tuesday, 9 April 2024

ACCESS TO MEETINGS/EXCLUSION OF THE PUBLIC

Purpose:	To consider whether the Public should be excluded from the following items of business.
Item (s):	Item 11 – Write Offs of Debt
Recommendation(s):	That the public be excluded from the meeting during consideration of the following item(s) of business on the grounds that it/they involve(s) the likely disclosure of exempt information as set out in the Paragraphs listed below of Schedule 12A of the Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) (Wales) Order 2007 subject to the Public Interest Test (where appropriate) being applied.
Relevant Paragraph(s):	14

1. Purpose of Report

To enable Members to consider whether the public should be excluded from the meeting in relation to the item(s) listed above.

Section 100A (4) of the Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) (Wales)

Order 2007, allows a Principal Council to pass a resolution excluding the public from a meeting during an item of business.

Such a resolution is dependant on whether it is likely, in view of the nature of the business to be transacted or the nature of the proceedings that if members of the public were present during that item there would be disclosure to them of exempt information, as defined in section 100I of the Local Government Act 1972.

2. Exclusion of the Public/Public Interest Test

In order to comply with the above mentioned legislation, Members will be requested to exclude the public from the meeting during consideration of the item(s) of business identified in the recommendation(s) to the report on the grounds that it/they involve(s) the likely disclosure of exempt information as set out in the Exclusion Paragraphs of Schedule 12A of the Local Government Act 1972 as amended by the Local Government (Access to Information) (Variation) (Wales) Order 2007.

Information which falls within paragraphs 12 to 15, 17 and 18 of Schedule 12A of the Local Government Act 1972 as amended is exempt information if and so long as in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

The specific Exclusion Paragraphs and the Public Interest Tests to be applied are listed in Appendix A.

Where paragraph 16 of the Schedule 12A applies there is no public interest test. Members are able to consider whether they wish to waive their legal privilege in the information, however, given that this may place the Council in a position of risk, it is not something that should be done as a matter of routine.

3. Financial Implications

Not applicable

4. Integrated Impact Assessment

Not applicable

5. Valleys Communities Impact

Not applicable

6. Workforce Impact

Not applicable.

7. Legal Implications

The legislative provisions are set out in the report.

Members must consider with regard to each item of business the following matters.

(a) Whether in relation to that item of business the information is capable of being exempt information, because it falls into one of the paragraphs set out in Schedule 12A of the Local Government Act 1972 as amended and reproduced in Appendix A to this report.

and either

(b) If the information does fall within one or more of paragraphs 12 to 15, 17 and 18 of Schedule 12A of the Local Government Act 1972 as amended, the public interest test in maintaining the exemption outweighs the public interest in disclosing the information; or

(c) if the information falls within the paragraph 16 of Schedule 12A of the Local Government Act 1972 in considering whether to exclude the public members are not required to apply the public interest test by must consider whether they wish to waive their privilege in relation to that item for any reason.

8. Risk Management

To allow Members to consider risk associated with exempt information.

9. Recommendation(s)

As detailed at the start of the report.

10. Reason for Proposed Decision(s):

To ensure that all items are considered in the appropriate manner.

11. Implementation of Decision(s):

The decision(s) will be implemented immediately.

12. List of Background Papers:

Schedule 12A of the Local Government Act 1972

13. Appendices:

Appendix A – List of Exemptions

Appendix A

NO	Relevant Paragraphs in Schedule 12A
12	Information relating to a particular individual
13	Information which is likely to reveal the identity of an individual
14	Information relating to the financial or business affairs of any particular person (including the authority holding that information).
15	Information relating to any consultations or negotiations, or contemplated consultations or negotiations in connection with any labour relations matter arising between the authority or a Minister of the Crown and employees of, or office holders under, the authority
16	Information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.
17	Information which reveals that the authority proposes: • To give under any enactment a notice under or by virtue of which requirements are imposed on a person, or • To make an order or direction under any enactment.
18	Information relating to any action taken or to be taken in connection with the prevention, investigation or prosecution of crime.

This page is intentionally left blank

By virtue of paragraph(s) 14 of Part 4 of Schedule 12A
of the Local Government Act 1972.

Agenda Item 10

Document is Restricted

This page is intentionally left blank