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 SUB COMMITTEE
TUESDAY, 7 MARCH 2023

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 5 - 8)*

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

For Decision:

6. Third Sector Grants 2023-24 - Additional Applications
(Pages 9 - 12)

7. Miscellaneous Grant Fund Application *(Pages 13 - 18)*

8. Community Councils Minor Projects Scheme *(Pages 19 - 24)*

9. Rate Relief for Charities and Non-profit Making Organisations
(Pages 25 - 34)

For Information:

10. Cyber Security Strategy 2023 Update *(Pages 35 - 60)*

11. Urgent Items
Any urgent items (whether public or exempt), at the discretion of the Chairperson pursuant to Statutory Instrument 2001 No 2290 (as amended)

12. Access to Meetings - Exclusion of the Public *(Pages 61 - 66)*
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

For Decision:

13. Write Off Of Business Rates (Exempt Under Paragraph 14)
(Pages 67 - 76)

14. Write Off Of Council Tax (Exempt under Paragraph 14)
(Pages 77 - 92)

K.Jones
Chief Executive

Civic Centre
Port Talbot **1 March 2023**

Cabinet (Policy and Resources) Sub Committee Members:

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

This page is intentionally left blank

EXECUTIVE DECISION RECORD

24 JANUARY 2023

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

Cabinet Members:

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

Officers in Attendance:

C.Griffiths, H.Jones, H.Lewis, C.John and T.Davies

Scrutiny Chair: Councillor P.Rogers

---

1. **APPOINTMENT OF CHAIRPERSON**

Agreed that Councillor S.K.Hunt (Leader of Council) 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**

The Minutes from the meeting of 15 November, 2022, were agreed.

5. **FORWARD WORK PROGRAMME 2022/23**

The Forward Work Programme 2022/23, was noted.

6. **MISCELLANEOUS GRANT FUND APPLICATION**

Members noted that the acronym 'CIC' stood for 'Community Interest Company'. The Chief Finance Officer would circulate the Miscellaneous Grants Policy to Members outside of the meeting.

Decision:

That the Trustees of Jones CIC be granted £9,350 per annum towards the cost of the rent of £9,845 pa in relation to the lease of Playing Fields and Recreational Areas at Evans Bevan Playing Field, Baglan Port Talbot Cross for use as a Community Centre (Cross Community Centre).

Reason for Decision:

To decide on the amount of financial support in respect of the grant application received.

Implementation of Decision:

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

7. **ANTI-FRAUD CORRUPTION STRATEGY**

Officers explained that the numbering in the circulated Policy was incorrect, and should flow from 1.1 to 1.2 to 1.3 and so on.

Decision:

That the report be noted.

8. **ACCESS TO MEETINGS - EXCLUSION OF THE PUBLIC**

Decision:

That the public be excluded from the meeting during consideration of the following items of business on the grounds that it involved the likely disclosure of exempt information as set out in Paragraph 14 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.

9. **COUNCIL TAX WRITE OFFS**

Decision:

That approval be granted to write off the amounts of Council Tax, as detailed in the private circulated report.

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.

10. **GLAMORGAN FURTHER EDUCATION TRUST FUND**

Decisions:

1. That the applications for awards, as detailed in Appendix B to the private circulated report, made out of the Glamorgan Further Education Trust Fund for the academic year 2022/2023, to eligible applications received on or before the closing date, be approved.

2. That payments to those applicants for whom continuing support from the Glamorgan is needed, as detailed in the private circulated report, be approved.

Reason for Decisions:

To provide appropriate financial support for students who would otherwise suffer hardship.

Implementation of Decisions:

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

11. **THE HAROLD AND JOYCE CHARLES TRUST**

Decisions:

1. That the applications for awards, as detailed in Appendix B of the private circulated report, made out of the Harold and Joyce Charles Fund for the academic year 2022/2023 to eligible applications received on or before the closing date, be approved.

2. That payments to those applicants for whom continuing support from the Harold and Joyce Charles Fund has already been approved, as detailed within the private circulated report, be approved.

Reason for Decisions:

To provide appropriate financial support for students who would otherwise suffer hardship.

Implementation of Decisions:

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

CHAIRPERSON

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

7th March 2023

Report of the Chief Finance Officer – Huw Jones

Matter for: Decision

Wards Affected: All Wards

Third Sector Grant Funding – Additional applications for funding

Purpose of Report

To ask Members to consider additional applications for a third sector grant received after the official closing date and to seek approval on the award of grants to these organisations as set out in Appendix 1.

Executive Summary

Cabinet approved a schedule of third sector grants at their meeting on 30th November 2022.

Following that meeting officers were approached by the following organisations Citizens Advice Swansea Neath Port Talbot and NPT Shopmobility who had inadvertently failed to submit their applications for funding by the deadline for applications; and were therefore not considered for funding at that time.

This report requests that Members consider awarding grants to the strategic partners Citizens Advice Swansea Neath Port Talbot and NPT Shopmobility.

Assessment of Grant Application

The applications from Citizens Advice Swansea Neath Port Talbot and NPT Shopmobility have been assessed in line with all other applications received.

Based on the assessment Officers are proposing that a grant of £90,000 be awarded to Citizens Advice Swansea Neath Port Talbot and £47,000 be awarded to NPT Shopmobility for 2023/2024 as detailed in Appendix 1.

Financial Appraisal

There are additional resources forecast to be carried forward from 2022/23 to fund grant awards of £137,000.

Integrated Impact Assessment

An Equality Impact Assessment was completed as part of the initial development of the Grant Scheme in 2016 and a further Integrated Impact Assessment was completed as part of the changes to the Scheme in 2018. The Scheme was reviewed further in July 2022 with only minor amendments made.

Valleys Communities Impact

The applicants will be providing services to those living in valley communities.

Workforce Impact

There is no workforce impact.

Legal Impact

The grant recipients will be required to sign a Grant Agreement.

Risk Management

The successful grant recipients will assist the Council to provide important services within the County Borough.

Consultation

There is no requirement for external consultation on this item.

Recommendation

It is recommended that Members:

- Confirm the amount of grant payable to each Strategic Partner as set out in Appendix 1

Reason for Proposed Decision

To approve grants to a third sector organisations in line with the Council's Scheme.

Implementation of Decision

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

Appendices

Appendix 1

List of Background Papers

The Neath Port Talbot Third Sector Grant Funding Scheme.

Officer Contact

Huw Jones, Chief Finance Officer
Email: h.jones@npt.gov.uk

Caryn Furlow-Harris, Strategic Manager – Policy & Executive Support

Email: c.furlow@npt.gov.uk

Louise McAndrew, Corporate Strategic Planning & Governance Officer

Email: l.mcandrew@npt.gov.uk

APPENDIX 1

Grant Award to Third Party Strategic Partner Organisations 2023/24	2023/24 Year 1	2024/25 Year 2	2025/26 Year 3
Citizens Advice Swansea Neath Port Talbot	£90,000	£94,879	£98,674
NPT Shopmobility	£47,000	£51,480	£51,480
Total	**£137,000**	**£146,480**	**£150,154**

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

7 MARCH 2023

REPORT OF THE CHIEF FINANCE OFFICER – HUW JONES

Matters for Decision

Wards Affected: Pontardawe

Report Title – Miscellaneous Grant Fund Application

Purpose of the Report:

1. To seek Member approval in relation to grant application received at Appendix 1 attached. It should be noted that this application was reported to the Cabinet (Policy and Resources) Sub Committee on the 24th January 2023, however, the incorrect ward and premises i.e Baglan Ward and Evans Bevan Playing Fields was reported. This is correctly reported now as Pontardawe ward and the premises referred to is Cross Community Centre High Street Pontardawe.

Background and Financial Impacts

2. The Council has a Miscellaneous Grants Scheme to support individual applications for grants in line with the criteria set out below:-

Existing Policy Statement

a) Each application will be considered on its merits.
b) The Committee will only approve applications for financial assistance from voluntary or charitable organisations which are manifestly committed to voluntary endeavours of a local nature. This will not preclude the consideration of applications where the disposal of funds is outside the area but still provides significant benefits for the people from the Neath Port Talbot area.
c) No applications will be considered from religious bodies except relating to church halls and other premises where there is significant community use of the property for non-religious activities.
d) No applications will be considered from other public funded bodies such as community councils, hospital trusts, etc. or where the benefit may be in lieu of their contributions such as appeals for hospital equipment.
e) Applications from individuals may be considered where both the person and the community derive a benefit.
f) No grants will be made to any individual or organisation whose prime purpose is to distribute their funds to other charitable bodies.

Integrated Impact Assessment

3. There are no impacts in respect of the obligations to the Council under the Equality Act 2010, the Welsh Language Standards (No 1) Regulations 2015, the Environment (Wales) Act 2016 and support via this grant provides generally a positive impact in respect of the Wellbeing and Future Generations (Wales) Act 2015.

Valleys Communities Impacts

4. Applications for grant are available to voluntary and charitable organisations across the county borough.

Workforce Impacts

5. There are no workforce impacts.

Legal Impacts

6. Grants are provided in line with the approved scheme criteria.

Risk Management Impacts

7. All grant applications are considered on their own merit and in line with the approved scheme criteria.

Consultation

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

Recommendation

9. It is recommended that Members approve the application set out in Appendix 1 to this report.

Reason for Proposed Decision

10. To decide on the amount of financial support in respect of the grant application received.

Implementation of Decision

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

Appendices

12. Appendix 1 – Schedule of grant application.

List of Background Papers

13. Grant Application

Officer Contact

Mr. Huw Jones – Chief Finance Officer
Email: h.jones@npt.gov.uk

APPENDIX 1

SCHEDULE OF GRANT APPLICATIONS

Applicant	Purpose	Amount Request/Cost of "Project"	Previous Support	Comments
Jones Community CIC	The Trustees of Jones Community CIC have applied for grant assistance in relation to the lease of Cross Community Centre High Street Pontardawe	Grant towards the cost of rent of £9,845 pa which is increasing from £8,950 pa	P&R board 19/02/2015 approved 100% grant assistance in the amount of £8,950 pa	Proposed that a grant of £9,350 per annum be offered which is the equivalent of c95% of the new rent.

This page is intentionally left blank

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB COMMITTEE

7 MARCH 2023

REPORT OF THE CHIEF FINANCE OFFICER – HUW JONES

Matter for Decision

Wards Affected – Cimla and Pelenna

Report Title – Community Councils Minor Projects Scheme – Application from Pelenna Community Council

Purpose of Report

1. To seek Members' approval to provide a grant to Pelenna Community Council under the Council's Community Councils Minor Projects Scheme.

Background

2. Neath Port Talbot Council has approved a Community Council Minor Projects Grants Scheme in order to assist Community Councils in undertaking minor capital projects. Approved grants are required to be claimed within two years of approval.

   The Council has received an application for grant aid under the above mentioned scheme from Pelenna Community Council.

   This application is for grant assistance towards the cost of works for redeveloping and improving the provision currently on offer at the play area on Johns Terrace, Tonmawr. Play equipment to be installed includes both Junior and Toddler Multi-Play Units, inclusive nest, pod and tango swings and a Play End Wall complete with anti-

slip textured rubber play surfacing and court markings for football and basketball. The funding will also cover the cost of infrastructure such as self-closing gates, benches, a picnic table, litter bin and bow top fencing.

“Our vision is to create an outdoor hub which offers the most generous arrangements for public enjoyment, regardless of age”

Annual inspection of the play equipment will be carried out by an Independent Service Engineer from RoSPA. The Community Council have committed to the cost of insuring, maintaining and inspecting the Park for the foreseeable future - this will guarantee future sustainability and that this asset remains viable for many years to come,

The new equipment will conform to the relevant safety standards. There are extended warrantees on the equipment and safety surfacing, integrity of the installations, etc. As such, we expect very little in the way of maintenance in the immediate subsequent years.

The project aligns closely to two of the four NPTCBC Corporate Plan 2022-2027 outcomes:-

1. **To ensure our local environment, culture and heritage can be enjoyed by future generations:**

   There are currently no intergenerational, doorstep activities for the community of Pelenna outside of the playing of rugby. As a Community Council we feel it is our duty to provide facilities that are not just enjoyable for residents to use, but that guarantee longevity for future generations. The equipment to be installed and the play end wall will be of robust construction, it will serve the community for many years to come.

2. **To ensure all our communities are thriving and sustainable:**

   The community of Pelenna has lost much in recent years including two Primary Schools and ‘Tonmawr 2000’, which was the only indoor sports facility. There are two Community Centres, two rugby clubs and two shops – there are currently no play amenities of the type intended in this project proposal. The new facility would provide opportunities for our residents to thrive;

enjoying a better quality of life, making the most of the outdoors, and making the area more attractive and vibrant.

The proposal will imbibe a greater sense of community pride and spirit. Residents have been involved in the design of the play area and we know, through consultation, that this project is very close to their hearts.

3. The estimated cost of the works overall is £110,000 plus recoverable VAT.

4. The balance of the project costs will be financed as follows:-

The £14,000 requested from the Community Minor Projects grant would be used as match funding towards an application to the Pen y Cymoedd Wind Farm 'Vision' Fund, valued at £91,570. The remaining £4,430 will be contributed from Pelenna Community Council reserves (agreed at the Full Council Meeting on 07.11.22).

Proposal and Financial Impact

5. The application from Pelenna Community Council complies with the conditions of grant and is entitled to grant support at 70% up to a maximum of £14,000 in accordance with the Minor Projects Grants Scheme and payment be made on receipt of paid invoices together with a copy bank statement.

Integrated Impact Assessment

6. There are no impacts in respect of the obligations to the Council under the Equality Act 2010, the Welsh Language Standards (No 1) Regulations 2015, the Environment (Wales) Act 2016 and support via this grant is a positive impact in respect of the Wellbeing and Future Generations (Wales) Act 2015.

Valleys Communities Impacts

7. Applications for grant are available to Community Councils across the county borough.

Workforce Impacts

8. There are no workforce impacts.

Legal Impacts

9. Grants are provided in line with the approved scheme criteria.

Risk Management Impacts

10. All grant applications are considered on their own merit and in line with the approved scheme criteria.

Consultation

11. There is no requirement under the Constitution for external consultation on this item.

Recommendation

12. It is recommended that Members approve a grant of 70% of actual costs up to a maximum of £14,000 to Pelenna Community Council.

Reason for Proposed Decision

13. The decision is in compliance with the approved policy and to enable community improvements.

Implementation of Decision

14. The decision is proposed for implementation after the 3 day call-in period.

List of Background Papers

15. Application from Pelenna Community Council.

Officer Contact

16. Mr. H. Jones. – Chief Finance Officer
Tel. 01639 763575
email: h.jones@neath-porttalbot.gov.uk

This page is intentionally left blank

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET FINANCE SUB COMMITTEE

7th MARCH 2023

REPORT OF CHIEF FINANCE OFFICER –

HUW JONES

Matter for Decision

Wards Affected: All

Rate Relief for Charities and Non-profit Making Organisations

Purpose of the Report:

1. To This report recommends a scheme of rate relief for charities and non-profit making organisations for the period 1st April, 2024 to 31st March, 2029.

Background

2. The Local Government Finance Act 1988 provides rate relief from rates may be granted as follows:

(a) Mandatory Relief (80%)

Where a property is occupied by a charity and is used wholly or mainly for charitable purposes, and for community amateur sports clubs (as registered with HMRC).

(b) “Top Up” Discretionary Relief (up to 20%)

Where mandatory relief has been granted, an authority has the discretion to grant up to a further 20% relief.

(c) Discretionary Relief (up to 100%)

Where a property is occupied by an organisation which is not established or conducted for profit and whose objects are charitable, philanthropic, religious, or concerned with education, social welfare, science, literature or fine arts.

(d) Discretionary Relief (up to 100%)

Where a property is occupied by an organisation which is not established or conducted for profit and the property is wholly or mainly used for the purpose of recreation.

3. The cost of mandatory relief is met by the non-domestic rate pool. The cost of discretionary relief is shared between the pool and the local authority, as follows:

"Top up" of Mandatory Relief

25% is met by the pool;
75% is met by the local authority

Other

90% is met by the pool;
10% is met by the local authority

4. The current criteria for granting discretionary relief were agreed at the Cabinet Board meeting of 12th May 2021.

Criteria for Discretionary Rate Relief

5. The following are the current criteria for discretionary relief:

(a) that each application be treated on its merits;
(b) that the following general guidelines are met:

- membership of the organisation must normally be open to all sections of the community, and membership rates must not be set at a level which excludes the general community;

- it is accepted that reasonable restrictions may be placed on membership in relation to, for example, ability in a sport,

achievement of a standard in the field covered by the organisation, or where the capacity of the facility is limited;

- favourable consideration will be given to applications from organisations whose objectives are in line with the authority's 'Well Being Objectives';

- top up relief will not normally be granted to charity shops or housing associations;

- top up relief will only be granted to an outreach facility provided by a college in a deprived ward, subject to excluding those wards within the main population centres;

- rate relief will not be granted in respect of any area of an organisation's premises which are operated as a licensed bar and ancillary areas (e.g. cellars).

(c) that, having regard to the guidelines at (b) above, the types of organisation listed below in (e), will be granted 20% top up discretionary relief or 100% only relief, as appropriate.

(d) that having regard to the guidelines at (b) above, all other applications be treated on their merits.

(e) the organisations referred to in (c) above are:

- youth organisations (such as youth clubs, scouts and guide groups)
- OAP associations
- Gardening / horticultural societies
- Mental Health Associations
- Musical / theatrical groups
- Community associations
- Organisations concerned with education and training
- Sporting organisations
- Organisations concerned with voluntary and community services
- Organisations concerned with promoting economic development
- Citizens' Advice
- Organisations concerned with better health and well being
- Organisations concerned with the welfare of young people

Financial Impact

6. The current scheme provides financial support to 290 properties and is operated in line with Welsh Government proposals. However should the Welsh Government scheme change with regards to the 80% mandatory relief or any other relief element, it will require us to reconsider our scheme based on the changes.

   Current position in 2022/23 i.e. relief already provided to known organisations:

   - 81 accounts receive discretionary rate relief costing the authority £35,859.24

   - 209 accounts received mandatory and discretionary rates relief costing the authority £189,551.43

   - Total cost to the authority is £225,410.67

Integrated Impact Assessment

7. The first stage assessment, attached at Appendix 1, has indicated that a more in-depth assessment is not required.

Valley Communities Impacts

8. No implications.

Workforce impacts

9. All 290 accounts will be required to reapply for the relief which will need to be authorise by the Chief Finance Officer. Staff will need to deal with the associated workload.

Legal impact

10. There are no legal impacts arising from this report.

Risk management

11. There are no risk management issues arising from this report.

Consultation

12. There is no requirement under the Constitution for external consultation on this item.

Recommendations

13. That the current scheme of rate relief for charities and non-profit organisations be extended to 31st March 2029.

Reason for proposed decision

14. To enable the Council to provide discretionary rates relief to ratepayers to the 31st March 2029.

Implementation of decision

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

Appendices

16. Appendix 1 – First Stage Integrated Impact Assessment

List of background papers

17. Local Government Finance Act 1988.

Officer contact

18. Mrs Ann Hinder- Principal Council Tax Officer
E-mail: a.hinder@npt.gov.uk

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

Impact Assessment - First Stage

1. Details of the initiative

Initiative description and summary: To Approve The NNDR Discretionary Relief Scheme - 01.04.24 to 31.03.2029
Service Area: Revenues
Directorate: Chief Executives

2. Does the initiative affect:

	Yes	No
Service users		√
Staff		√
Wider community	√	
Internal administrative process only		√

3. Does the initiative impact on people because of their:

	Yes	No	None/ Negligible	Don't Know	Impact H/M/L	Reasons for your decision (including evidence)/How might it impact?
Age		√				
Disability		√				
Gender Reassignment		√				
Marriage/Civil Partnership		√				
Pregnancy/Maternity		√				
Race		√				
Religion/Belief		√				
Sex		√				
Sexual orientation		√				

4. Does the initiative impact on:

	Yes	No	None/ Negligible	Don't know	Impact H/M/L	Reasons for your decision (including evidence used) / How might it impact?
People's opportunities to use the Welsh language		√				
Treating the Welsh language no less favourably than English		√				

5. Does the initiative impact on biodiversity:

	Yes	No	None/ Negligible	Don't know	Impact H/M/L	Reasons for your decision (including evidence) / How might it impact?
To maintain and enhance biodiversity		√				
To promote the resilience of ecosystems, i.e. supporting		√				

protection of the wider environment, such as air quality, flood alleviation, etc.						

6. Does the initiative embrace the sustainable development principle (5 ways of working):

	Yes	No	Details
Long term - how the initiative supports the long term well-being of people	✓		Will support organisations that provide services to the public as outlined in the report.
Integration - how the initiative impacts upon our wellbeing objectives	✓		Will support organisations that provide services to the public as outlined in the report.
Involvement - how people have been involved in developing the initiative			N/A
Collaboration - how we have worked with other services/organisations to find shared sustainable solutions			N/A
Prevention - how the initiative will prevent problems occurring or getting worse			N/A

7. Declaration - based on above assessment (tick as appropriate):

A full impact assessment (second stage) **is not** required	✓
Reasons for this conclusion	
A full impact assessment is not required as this relates to the implementation of a scheme as prescribed by the 1988 Local Government Finance Act.	
A full impact assessment (second stage) **is** required	
Reasons for this conclusion	

	Name	Position	Date
Completed by	Ann Hinder	Principal Council Tax Officer	11/01/2023
Signed off by	Huw Jones	Chief Finance Officer	11/01/2023

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

CABINET (POLICY AND RESOURCES) SUB-COMMITTEE

7 March 2023

Report of the Chief Digital Officer – Chris Owen

Matter for Information

Wards Affected: All Wards

Neath Port Talbot Cyber Security Strategy Update 2023

Purpose of the Report:

1. To provide Members with an update on the Neath Port Talbot Council's Cyber Security Strategy.

Executive Summary:

2. The Neath Port Talbot County Borough Council (NPTCBC) Cyber Security Strategy has been developed to outline the council's approach to protecting our information systems; the data held within them; and the services they provide, from unauthorised access, harm or misuse. A copy of the strategy is attached at Appendix 1.

3. To underpin the delivery and continuous review of the strategy, a multi-year Cyber Security Action Plan has been developed. A 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. Globally healthcare, government systems and critical national infrastructure continue to be a key target, with the goal of using ransomware to extort monies from their victims.

5. Following the commencement of the war in Ukraine, there has been an increase in nefarious cyber activity in the war zone that has spilt over into the rest of the world.

6. For example, the biggest ever recorded denial of Service attack on Google's infrastructure was a co-ordinated attack from 130 countries, which peaked at 46 million attacks a second[1].

7. In last year alone, the United Kingdom has experienced 63 critical national infrastructure incidents[2]. Closer to home has been the recent cyber-attack on Neath Port Talbot College in December which has caused significant disruption and is still under investigation.

8. 82% of attacks involve a human interaction, with the remainder predominantly through compromised partner organisations. Of these attacks, 85% involve users opening infected email attachments, clicking on unsolicited internet links and compromised accounts through insufficient password strength[3].

9. In order to achieve strong cyber security, the council must continue to ensure it promotes a comprehensive risk-based approach, which is integrated across personnel, technical security, information assurance and physical security. It must

[1] ZDNET.com
[2] National Cyber Security Centre
[3] Verison.com

strategically encompass Information Security, Assurance, Resilience and Governance.

10. To mitigate the growing threat to the council, Digital Services has developed the Cyber Security Action Plan with the following key actions for 2022/23:

- Introduction of the innovative new Targeted Operating Model (TOM) – Aligning digital services activities with the TOM structure to provide a clear concise approach to continuous improvement.

- Through new governance arrangements we have established teams to assess and mitigate risks - Define mandatory training requirements and identify and compile performance measures.

- Policies / procedures – As part of the action plan, key policies and procedures have been identified and are being progressed.

- Plans / Playbooks - The Cyber Incident Response Plan and incident playbooks are under review, and where applicable will be updated to align with Council needs, Government & Industry best practice and adapt to the changing threat landscape.

- Infrastructure updates – Migrating to Microsoft Intune as the Authority's Mobile Device Management (MDM) solution, implementation of additional anti-ransomware tools, user access protection systems and commitment to continuous improvement of network security devices.

- Alignment with wider Government guidance – Monitoring advice and guidance from the Welsh and UK Governments, such as the '10 Steps to Cyber Security' issued by the National Cyber Security Centre.

- Roles and responsibilities – the key roles / groups identified in 2022 to deliver the strategy have now been set up and appointed.

11. The action plan will be used as a tool to measure continuous progress, whilst also allowing us to respond to meet the ever-changing challenges that we face.

12. Please refer to Appendix 2 – Cyber Security Action Plan for further information on progress across each key area.

Financial Impacts:

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

Integrated Impact Assessment:

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

Valleys Communities Impacts:

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

Workforce Impacts:

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

Legal Impacts:

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

Risk Management Impacts:

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

Consultation:

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

Recommendation:

20. It is recommended that Members continue to 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

List of background papers: None

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

Appendix 1 – Cyber Security Strategy V2.0

NPT Cyber Security Strategy V2.0 Final.pd

Appendix 2 – Cyber Security Action Plan

NPT Cyber Security Action Plan Update - .

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

NPTCBC

Cyber Security Strategy

Version: 2.0
Publish Date: December 2021
Review Date: December 2022
Next Review: December 2023
Owner: Chief Digital Officer

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

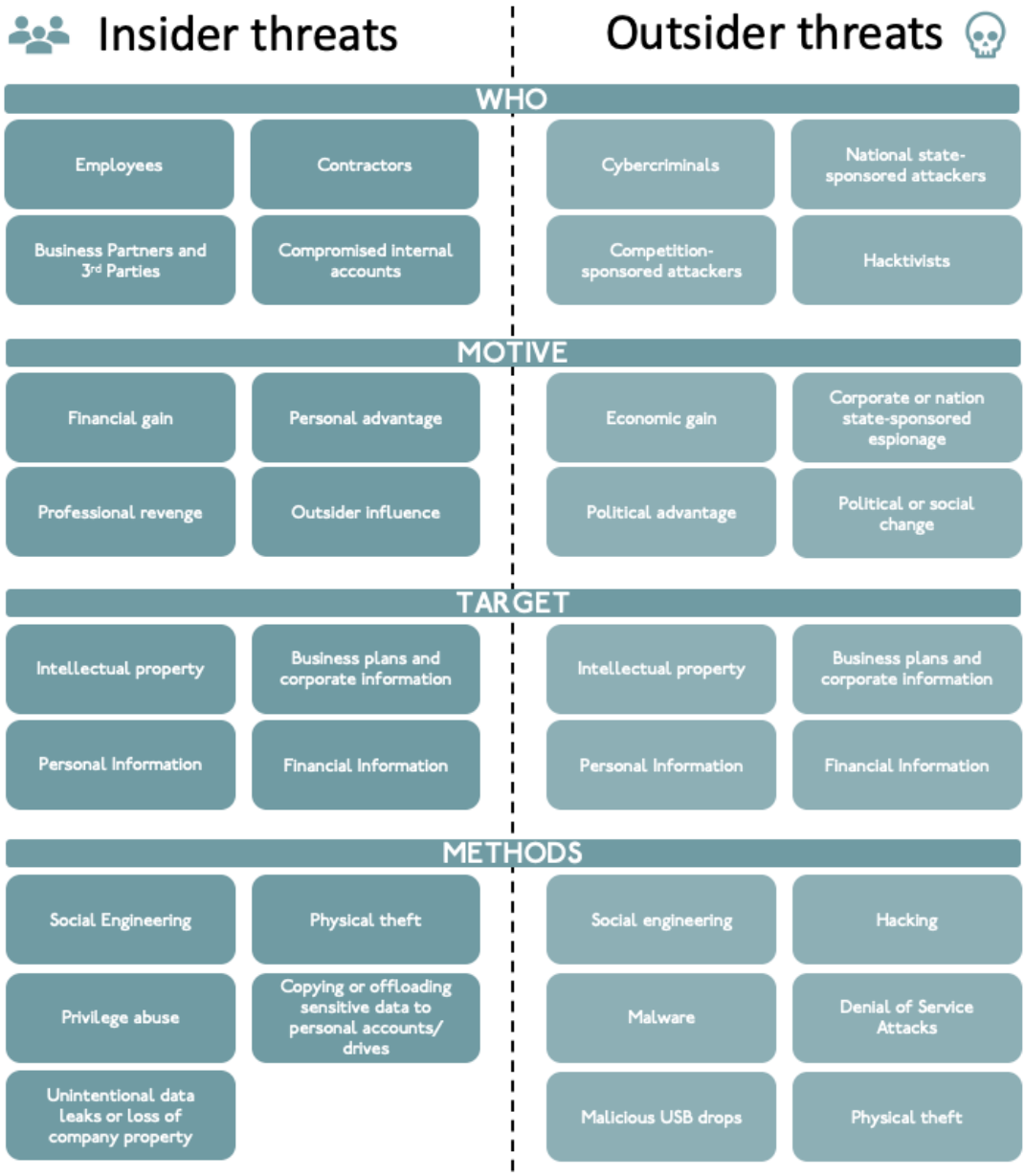
We are using an increasing range of technology, from 'apps' and 'the cloud', to different devices and 'gadgets'. Much of our business is online - corresponding with residents and local businesses, carrying out case work, and reviewing reports and papers for Council meetings.

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:



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 Update January 2023

ID	Area	Observation	Action - quick win	Action - longer term	% Complete
AP - 1	Defend / Technology	Maintain firewall and scanning services.	Maintenance of current infrastructure and services.	Migration to virtual firewall to enhance functionality and management.	67%
AP - 2	Defend / Technology	Maintenance of end-point protection for devices – Anti Virus, USB Encryption and Mobile Device Management.	Maintenance of current endpoint protection.	Consolodation of endpoint protections as part of planned move to enhanced Microsoft licencing	50%
AP - 3	Defend / Technology	Undertake Cyber Security Health Checks and Penetration Testing.	Maintain the programme of quaterly vulnerability scans of the server suite and rolling programme of workstation scans.	Establish schedule of independent health checks.	33%
AP - 4	Defend / Technology	Utilisation of the National Cyber Security Centre tools. WebCheck and Mail Check.	Migration to MyNCSC platform and configuration of services	Exploitation of enhanced features available within MyNCSC	67%
AP - 5	Defend / Governance	Meet compliance regimes which require good Cyber Hygiene (Public Service Network Code of Connection, Cyber Essentials).	Maintain current compliance with Public Service Network and Cyber Essentails.	Development work to move to Gov.Pay platform to harmonise payment processing on secure government platform. Extension of current Cyber Essentials into Cyber Essentials Plus and Cyber Essentials Governance	33%
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.	Expansion of Welsh WARP membership to include relevant internal stakeholders	Active presence in wider cyber community events	67%
AP - 7	Deter / Technology	Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions.	Identification and remediation of less secure authentication. Expansion of seperation of duties - privileged accounts used solely for adminstrative functions	Review of standard accounts with enhanced privieges.	50%
AP - 8	Deter / Technology	Reconcile current systems in place and last times these were reviewed.	Identiy high risk systems and undertake a scoping review to provide an interim assessment.	Scheduled annual review of existing systems to be setup and ongoing identification and creation of new guidance.	25%
AP - 9	Deter / Technology	Protect enterprise technology by working with specialist partners to develop model architecture.		Where necessary engage consultants with specialist expertise to advise on specific areas while internal capacity is being developed	0%
AP - 10	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.	Implemented as a requirement in all new systems	Review of existing systems to identify where MFA is not in place but can be in order to address these.	50%
AP - 11	Deter / Governance	Embed the Secure by Design principle throughout.	Regular Digital Team 'Stand Ups' raising awareness of workstreams and providing a coherent approach to bridge until Solutions Board in place.	Full initiation of Solutions Board to ensure all development follows the Target Operating Model, including Secure by Design and Privacy by Design	50%
AP - 12	Deter / Governance	Review vendor management to address supply chain risk.	Refine current process of System Assessments and IG processes for Third Party management.	Development of NPT Supply Chain Strategy and associated policy and process/procedure.	50%
AP - 13	Deter / Governance	Review (update where appropriate) policies and procedures.	Body of work required to review and update (new posts filled etc)	Scheduled annual review to be setup	33%
AP - 14	Develop / Technology	Explore Active Cyber Defence tools and new technologies to ensure we have the best solutions to match to threats.	Adopt Protected DNS toolkit and EmailCheck into current suite of Active Cyber Defence Tools.	Identify and test further ACDT with a view to implementing into the digital estate.	50%
AP - 15	Develop / Technology	Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises.	Engage in funded "Excercise in a box" opportunity.	Develop a scheduled programme of internal exercises.	33%

ID	Area	Observation	Action - quick win	Action - longer term	% Complete
AP - 16	Develop / Governance	Provide relevant cyber security training for staff and elected members to help detect, deter and defend against the cyber threats.	Report on current statistics of staff e-learning compliance. Awareness of Member e-learning to be raised and completion reported on. High Risk areas to be identified and proactively added to training cycle to address any gaps.	Regular reporting process put in place to collect and report on training compliance levels.	71%
AP - 17	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.	Formalise current processes which provide security governance.	Gap analysis leading to implementation of an Information Security Management System.	25%
AP - 18	Develop / Governance	Aligned with best practice, develop a minimum requirement for all systems used, audit trails, deletion of data etc.	Utilise current critera for System Assessments and IG processes to create a baseline set of requirements.	Develop a standalone internal minimum requirements standard to form part of suite of standards within the Information Security Management System.	50%
AP - 19	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.	Utilise RACI Matrix from Cyber Incident Response Plan to inform interim communications plan alongs side exisitng reporting mechanisms for statutory bodies.	Expand interim communication plan to include other existing communication plans to formalised cyber incident communication plan.	67%
AP - 20	Develop / Governance	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities.	Incident Response Plan is in place. Review and update of current incident playbooks.	Annual Review of Cyber Incident Response Plan.	100%
AP - 21	Develop - Governance	Create a cyber-specific Business Continuity Management Plan and/or review our Incident Plan to include emergency planning for cyber-attack.	Inclusion of cyber in current Business Continuity Management Plan	Develop separate Cyber Business Continuity Management Plan	50%

Cyngor Castell-nedd Port Talbot
Neath Port Talbot Council

Report of the Head of Legal and Democratic Services

Cabinet (Policy and Resources) Sub Committee Cabinet Board – Tuesday, 7 March 2023

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 12 – Write Off of Business Rates Item 13 – Write Off of Council Tax
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

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank