CABINET – 21ST MAY 2025

SUBJECT: **INFORMATION GOVERNANCE AND CYBER SECURITY UPDATE**

REPORT BY: **EXECUTIVE DIRECTOR FOR CORPORATE AND REGENERATION**

1. PURPOSE OF REPORT

1.1 The purpose of this report is to provide Cabinet with a status update in relation to Information Governance and Cyber Security.

1.2 This update relates to:

The Council's approach to Information Governance and specifically in relation to Access, Risk, Records Management and Corporate Complaints.

The Council's Cyber Security Strategy ('Strategy') and Associated Action Plan, which were formally endorsed by Cabinet on 30 November 2022 and implemented in December 2022.

2. SUMMARY

2.1 The report summaries the Council's approach to Information Governance and provides an overview of the separate disciplines associated with the Corporate Information Governance Unit, namely, Information Access, Information Risk, Records Management and recently added Corporate Complaints.

2.2 Provides quarterly statistics for calendar year 2024 in relation to:

- Freedom of Information Requests.
- Environmental Information Regulations Requests.
- Data Subject Rights Requests.
- Data Breach Incidents/ Complaints.

2.3 Highlights continuation of the positive work being progressed in relation to Cyber Security in accordance with the agreed Strategy and Action Plan. Successes include:

- Securing PSN Accreditation in 2024.
- Microsoft Secure Score in excess of 90%.
- Passwords.
- 98.7% of staff up to date with Matobo Cyber Ninja Training.

- Continued collaborative approach across the Council and the wider UK and Welsh Public Sector.

3. RECOMMENDATIONS

3.1 To note the status update and the progress made in relation to Information Governance and Cyber Security.

4. REASONS FOR THE RECOMMENDATIONS

4.1 To ensure that the Council is continuously monitoring and improving its Information Governance and Cyber Security arrangements.

5. THE REPORT

INFORMATION GOVERNANCE

5.1 The Corporate Information Governance Unit ('CIGU') assists the Council with managing our obligations in respect of handling information, including compliance with the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR'), the UK General Data Protection regulations 2018 ('GDPR'), the Data Protection Act 2018 and Records Management requirements.

5.2 CIGU has recently taken over responsibility, from Legal Services, for the Corporate complaints telephone line for the public, and the logging and distribution of complaints, using the newly implemented complaints system. The Council's Governance and Audit Committee receive reports on Corporate complaints, including statistics, twice a year.

5.3 The Council's current Information Governance Work Programme builds on previous efforts to comply with audit recommendations and reflects current requirements to have better knowledge of the information held within the Council and how it is used. As part of this work programme, Information Governance Stewards who are Council wide are working on mitigating information risks and encouraging greater use of information assets to support the work of the Senior Information Risk Owner ('SIRO').

5.4 The CIGU consists of the following areas:

INFORMATION ACCESS

5.5 This area deals with our obligations under the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and requests for data subjects rights, including the right of access, under the UK General Data Protection Regulations 2018 ('GDPR'). This is achieved through:

- Maintaining a suite of policies, guidance and compliant response templates.
- Providing a central point of contact for requestors to contact the Council to make a request.

- Logging and distributing requests to the relevant service areas.
- Managing a central log of all requests received together with legal compliance dates.
- Applying exemptions to the right of access, where applicable, with Legal Services colleagues ('Exemption Panel').
- Compliance checking all responses to requests.
- Maintaining the Publication Scheme (list of publicly available information which we are required to publish under FOIA).
- Dealing with requests for a review of the outcome of a request (complaints).
- Dealing with queries and investigations from the Information Commissioners Office ('ICO') in relation to information requests.

5.6 This is an extremely busy area with typically around 1500 requests per year. The majority of requests received are under the FOIA or EIR legislation that gives public authorities (like the Council) 20 working days to respond, which may be extended in certain circumstances. While the FOIA provides a general right of access to recorded information and EIR provides a right of access specifically to Environmental Information, as these two access rights are very similar for statistical purposes, staff do not differentiate between FOIA and EIR.

5.7 Statistics for FOIA / EIR requests for 2024 are detailed in ***Appendix 1 – Table 1 of this report.*** The compliance rate at 73% is below ICO expectations of 90%, however the ICO are not currently pursuing organisations failing to meet the 90% threshold, but this is highly likely to change in the future. CIGU are striving to meet the 90% target and will continue working with the relevant service areas to improve response times.

5.8 It should be noted that applicants appear to be content with the quality of responses received, which is supported by the low numbers of requests for an Internal Review.

5.9 ***Appendix 2 – Table 2 of this report***, details statistics for Data Subject Rights requests. There are 6 requestable rights under GDPR, however the vast majority are for the Right of Access, commonly called a Subject Access Request. The default compliance period for dealing with all Data Subject Rights requests is 1 calendar month, but this compliance period can be extended up to an additional 2 months for complex requests. The compliance rate for Data Subject Rights requests for 2024 was 88%.

5.10 In addition to dealing with requests for information, staff also provides an Information Governance Advice and Statutory Data Protection Officer service for Schools within the borough. Since service commencement all Schools have signed up via a Service Level Agreement.

INFORMATION RISK

5.11 Information Risk has the responsibility for assisting the Council in meeting its obligations in relation to compliance with data protection legislation including information risk. It does this by maintaining key data protection policies and guidance, and providing advice and assistance to the Council, in respect of the following areas:

- General data protection compliance.
- Data Protection Impact Assessments (DPIA).

- Data Processing Agreements (DPA).
- Data Sharing Agreements (DSA).
- Legitimate Interest Assessments (LIA).
- Privacy Notices.
- Maintaining an Information Asset Register in conjunction with service areas.
- Maintaining an Information Risk Register in conjunction with service areas.
- Due diligence checks on suppliers processing personal data on behalf of the Council.
- Providing and maintaining mandatory training in respect of data protection to officers and elected members.

5.12 The work undertaken in this area, together with the reports from Heads of Service via the Information Risk Register, provides the basis for the SIRO to write an assurance briefing for inclusion in the Annual Governance Statement, that form part of the Statement of Accounts.

5.13 This has been a challenging but successful period, providing Information Governance support and assistance to many of the workstreams within Mobilising Team Caerphilly. The work completed has been essential to assist in ensuring changes as a result of the MTC work, are compliant with data protection, where they involve processing personal data, and ensuring the required accountability measures are established, such as DPIA's, DPA's, DSA's, LIA's and Privacy Notices. It is anticipated the increased workload will continue for the foreseeable future.

5.14 Information Risk staff are also responsible for completing investigations in respect of data protection incidents and data protection complaints from the public, which would include:

- Investigation of the complaint / incident and determination if a breach of personal data had occurred.
- Assessment and notification to the Information Commissioners Office ('ICO') of high-risk data breaches within 72hrs.
- Assessment and notification to data subjects of high-risk data breaches including providing advice on how they can minimise the impact of the data breach.
- Ensuring the Council learns from data breaches to minimise the likelihood of similar occurrences.
- Maintaining a register of data breaches.
- Dealing with queries and investigations from the ICO in relation to data protection complaints and potential personal data breaches.

5.15 ***Appendix 1 – Table 3 of this report***, highlights that a total of 115 data protection incidents and 13 data protection complaints were investigated by the CIGU during 2024. While this resulted in high numbers of confirmed data breaches, the majority of these were extremely minor in nature and were not of risk to the individual's privacy. It is, however, important that these are investigated, and the Council learns from the incidents, to minimise the likelihood of similar occurrences. For 2024, only one data breach reached the criteria for reporting to the ICO.

RECORDS MANAGEMENT

5.16 Section 60 of the Local Government (Wales) Act directs Councils to have a scheme established to properly manage records from planning and creation through to disposal to fulfil the following objectives:

- Create and capture accurate, authentic, reliable and useable records to produce evidence and demonstrate accountability.
- Maintain records to meet the authority's business needs for as long as required for operational efficiency.
- Dispose of records that are no longer required in an appropriate manner.
- Protect vital records.
- Meet legal and statutory requirements relating to record-keeping.

5.17 Staff within CIGU assists the Council to fulfil its obligations in this area by maintaining 3 Corporate Records Centres, providing secure managed storage for approximately 4 linear miles of hard copy records which equates to circa 45,000 transfer cases of records. All records are logged and tracked using specialist software and a twice weekly record request service is provided, as well as an express service for urgent requests, for those service areas who require access to their deposited records. Once records are no longer required, with the approval of the relevant service, confidential disposal is arranged maintaining an audit trail of the disposal.

5.18 Staff have had a successful 12 months arranging and receiving new deposits and maintaining existing records. Staff are also responsible for maintaining the Corporate Records Management and Records Retention and Disposal Policies and providing Records Management advice and assistance.

5.19 Over recent years the focus of staff has been on the management of Electronic Records across the Council. Developing Records Management guidance on the migration of records from staff's personal Y Drive to OneDrive together with drafting a Corporate Teams Policy, which is currently being consulted upon by staff across the Council.

5.20 More recently there's been a focus on managing the implementation of SharePoint Online, which is cloud based, as the new Corporate records repository, which will replace the current storage on the network drives. The implementation phase of the project commenced in January 2025 and is estimated to take circa 18 months to complete, due to the different approaches and complexities to each service area across the Council.

5.21 There is approximately 25 TB of data (equivalent to 500 linear miles of hard copy records) currently on network drives that has to be cleansed of Redundant, Obsolete and Trivial ('ROT'), restructured were necessary, prior to being migrated to SharePoint Online. It is estimated that approximately 70% of this data can be eliminated as ROT from the experience of other local authorities who have gone through this process.

5.22 The migration of these records to SharePoint Online will have significant benefits for the Council, including:

- Advanced security and disaster recovery.
- Enhanced oversight of data.
- Increased audit and compliance functions.

- Advanced user search facilities.
- Enhanced records management functionality including automated retention.
- Cost savings as SharePoint storage is included in our current Microsoft licenses.

5.23 Large scale data centres such as those provided by Microsoft, who host SharePoint Online, can also dramatically reduce our carbon emissions in respect of the storage of these electronic records compared to the Council's Data Centre, which hosts the current network drives. In respect of the 25TB of data, it is estimated that this will result in a 90% reduction, and if we were to reduce the column of records being stored by 70%, this would equate to a 97% reduction.

5.24 The work in the area is extremely important to the Council, modernising the way we store this information and setting a framework for Electronic Records Management for the foreseeable future. This is the largest task of this type that the Council has undertaken, and the team are being supported by staff from the Information Risk, Digital Cloud Services, Cyber Security and IT Training.

6. CYBER SECURITY

TEAM

6.1 The team continues to provide support across the Council including Corporate and Education. This includes attending a variety of collaborative forums both internal and external to the Council. An example of the forums includes:

- Corporate Cyber Security Forum
- Education Cyber Security Forum
- Cyber Incident Response Forum
- Mobilising Team Caerphilly (Mainly Unavoidable Change)
- Digital Solutions Board ('DSB')
- Warning Advice & Reporting Point ('WARP')
- Gwent Local Resilience Forum ('LRF')
- CymruSOC Programme Business Case Steering Group
- Joint Information Systems Committee ('JISC')
- WLGA Cyber Assessment Framework ('CAF') Delivery Group
- WLGA Cyber Assessment Framework ('CAF') Reference Group

STRATEGY AND ACTION PLAN

6.2 The Council has continued to make positive progress with regard to the Critical Success Factors within the Strategy and Action Plan. Staff have frequent meetings regarding the Action Plan to ensure key workstreams are being prioritised and moved forward. The current Strategy runs until December 2025 and will be revised and updated to ensure continuity with our approach is fully maintained.

PSN ACCREDITATION AND INFORMATION TECHNOLOGY HEALTH CHECK ('ITHC')

6.3 A significant amount of work has been undertaken by staff across Customer & Digital Services in consultation with our PSN assessor, subsequently the Council

achieved PSN Compliance on 23 September 2024. Staff are maintaining momentum with the drive to secure our PSN Compliance for 2025/26. Work is currently underway to remediate issues from our most recent ITHC, which was undertaken in December 2024.

6.4 It is important to highlight that it is impossible to be 100% secure, due to the ever-changing nature of Cyber Security, however ITHC assessors (via their report) complimented several of the measures the Council has implemented. An example is in relation to passwords, which has been a key focus for the Council.

AUDIT WALES

6.5 The Council has recently participated in a Cyber Security Audit, undertaken by Audit Wales. The focus was on the status of Cyber Security across the Council and our alignment with the National Cyber Security Centre ('NCSC') 10 Steps.

6.6 There is a separate report to be presented at the Council's Governance and Audit Committee. Overall, the feedback is positive on the Council's approach to Cyber Security and the main area for improvement is in relation to Cyber Incident and Business Continuity Plans (both Corporate level and individual Service Areas). An extract from the Audit Wales report states "The Council has good technical arrangements in place to monitor and respond to cyber security incidents."

6.7 These areas were identified on our Action Plan prior to the Audit and progress has already been made on remediating these issues across the Council via staff within Customer & Digital Services and Emergency Planning.

SECURE SCORE

6.8 Microsoft Secure Score is a Microsoft generated Key Performance Indicator ('KPI') of how 'secure' the Council is from the viewpoint of our Microsoft Defender suite. This includes scoring on how well configured our different Defender aspects are, together with the rules that are established on our systems.

6.9 In our last Cyber Security Update our score had just hit 80+%. Currently our score is in excess of 90%. For context, an organisation of our size on average scores in the range of 45-50%.

TRAINING

6.10 The Matobo 'Cyber Ninja' training has continued for staff, with the addition of the 'Refresher' module for those who have previously undertaken the full course. As of early March 2025, 2721 staff are up to date with training, which equates to 98.7% of staff with a Corporate email account. The Matobo 'Cyber Ninjas 4 Councillors' training, also received a positive response, with 61 Councillors completing the training, prior to expiry of the course, due to Welsh Government ('WG') withdrawing the funding.

6.11 During 2024 Microsoft Attack Simulator campaigns were implemented. This functionality involves staff and Councillors receiving 2 x 'phishing' emails per year, where interaction with the phishing email (via clicking a link) can be recorded and areas for additional guidance can be identified on a more granular

level.

6.12 A WLGA funded Cyber Incident workshop was recently conducted with several key stakeholders from across the Council. The workshop included a simulation of a major cyber incident that impacted the Council with a number of scenarios to navigate based on the incident and subsequent consequences. The workshop was well received, and the Council is using the lessons learned from the session to guide our approach to our Cyber Incident Response Plan. Please refer to sections 6.6 and 6.7 above.

CYBER ASSESSMENT FRAMEWORK ('CAF')

6.13 The Council is continuing to engage with WLGA and Welsh Government on the implementation of CAF. This is a different methodology to measuring our approach to Cyber Security. The Council is represented on the WLGA CAF Delivery Group and CAF Reference Group, with the aim of establishing the CAF throughout Welsh Councils and other Welsh public Sector bodies by the end of 2025. The CAF requirements are being factored into our Action Plan and decision-making processes.

CYMRUSOC PROJECT

6.14 The CymruSOC is a Welsh Government collaborative initiative with the aim of introducing a cross-public sector Security Operations Centre ('SOC'). The Council continues to actively participate in the project and is in the final stages of Phase 1. This involves a connection being established between Socura (third party commissioned by Welsh Government) and the Council's Microsoft Defender suite, enabling our Defender suite to be continuously monitored (24/7, 365 days of the year). This will improve the Council's overall security posture and will ensure there is always a human eye overseeing the system in addition to Defenders automated capabilities.

7. CONCLUSION

7.1 The report highlights that the Council is continuously monitoring and improving its Information Governance and Cyber Security arrangements.

8. ASSUMPTIONS

8.1 There are no assumptions associated with this report.

9. SUMMARY OF INTEGRATED IMPACT ASSESSMENT

9.1 The Council will be unable to deliver its Well-being objectives in the absence of effective Corporate governance arrangements.

9.2 Strong Corporate governance arrangements are a key element in ensuring that the Well-being Goals within the Well-being of Future Generations Act (Wales) 2015 are met.

9.3 There are no equalities implications arising from this report in relation to any other equalities issues.

10. FINANCIAL IMPLICATIONS

10.1 There are no financial implications in respect of the recommendations in this report.

11. PERSONNEL IMPLICATIONS

11.1 There are no personnel implications in respect of the recommendations in this report.

12. CONSULTATION

12.1 This report has been sent to the Consultees listed below and all comments received are reflected within the report.

13. STATUTORY POWER

13.1 Local Government and Elections Act 2021.

Authors: Ian Evans, Procurement and Information Services Manager
Carl Evans, Information Governance Manager and Data Protection Officer
Matthew Cuthbert, Information Security Manager

Consultees: Richard (Ed) Edmunds, Chief Executive
Mark S Williams, Executive Director for Corporate and Regeneration
Corporate Management Team (on 19 March 2025)
PDM (on 9 April 2025)
Corporate and Regeneration Scrutiny (on 13 May 2025)
Elizabeth Lucas, Director of Transformation, Digital and Procurement
Lai Beale, Principal Information Governance Compliance Officer (Risk)
Nicola Grimstead, Senior Records Management Officer
Wesley Colyer, Senior Information Security Officer
Edward Thomson, Information Security Officer
Cyber Security Forum, Corporate
Cyber Security Forum, Education

Appendix 1 FOIA/EIR Statistics for 2024

Appendix 1

Table 1 – FOIA/EIR Statistics for 2024

	Quarter 1 (Jan – Mar)	Quarter 2 (Apr -Jun)	Quarter 3 (Jul – Sep)	Quarter 4 (Oct – Dec)	Year Total
Total number of requests received	402	350	342	273	1367
Total number of open requests	422	433	361	320	-
Open with permitted extensions					
- Public interest Test	0	0	0	0	0
- Complex	0	0	0	0	0
Total closed					
- Within statutory deadline	261	286	218	208	973
- Within extended deadline	0	0	0	0	0
- Outside of deadline	74	119	91	78	362
Total closed					
- Provided in full	284	352	269	251	1156
- Part provide / part refuse	31	32	14	13	90
- Refused in full	20	21	26	22	89
Compliance Rate	78%	71%	71%	73%	73%
Total Internal Reviews	4	4	2	2	12
Total clarifications					
- Stopped the clock	4	9	5	4	22
- Paused the clock	0	0	0	0	0

Table 2 –Data Subject Rights Statistics 2024

	Quarter 1 (Jan – Mar)	Quarter 2 (Apr -Jun)	Quarter 3 (Jul – Sep)	Quarter 4 (Oct – Dec)	Year Total
Total number of requests received	37	35	44	25	141
Total number of open requests	51	54	52	41	-
Total closed					
- Within statutory deadline	25	36	28	18	107
- Within extended deadline	3	5	4	3	15
- Outside of deadline	4	5	4	4	17
Compliance Rate	88%	89%	89%	84%	88%
Total Internal Reviews	1	5	2	0	8

Table 3 – Data Breach Incidents / Complaints 2024

	Quarter 1 (Jan – Mar)	Quarter 2 (Apr -Jun)	Quarter 3 (Jul – Sep)	Quarter 4 (Oct – Dec)	Year Total
Incidents					
- Incidents reported	25	37	36	17	115
- Confirmed data breaches	24	29	31	17	101
Complaints					
- Complaints received	2	3	5	3	13
- Confirmed data breaches	2	2	2	3	9
Number of data breaches reported to ICO within 72 hrs, where legally required	0	0	0	1	1