Agenda

Penderfyniadau dirprwyedig - Aelod cabinet dros drawsnewid sefydliadol

Dyddiad: Dydd Llun, 31 Hydref 2022

At: Cynghorwyr: D Batrouni

Eitem		Wardiau Dan Sylw
1	Adroddiad Blynyddol Risg Gwybodaeth 2022 *(Tudalennau 3 - 34)*	

Person cyswllt: ,
Ffôn:
E-bost:
Dyddiad cyhoeddi: Date Not Specified

Mae'r dudalen hon yn wag yn

Report

Cabinet Member for Organisational Transformation

Part 1

Date: 31 October 2022

Subject **Annual Information Risk Report 2021-22**

Purpose To provide an assessment of the council's information governance arrangements, identify key risks and agree the action plan for 22/23

Author Digital Services Manager/Information Manager

Ward General

Summary Local Authorities collect, store, process, share and dispose of a vast amount of information. The council must meet its statutory responsibilities effectively and protect the personal information it holds throughout its life cycle; from creation through storage; use, retention, archiving and deletion.

The purpose of the council's tenth Annual Information Risk Report is to provide an assessment of the information governance arrangements for the council and identify where further action is required to address weaknesses and make improvements.

Proposal **To endorse the Annual Information Risk Report 2021-22 and proposed actions.**

Action by Digital Services Manager/Information Manager
Head of People, Policy and Transformation

Timetable As reported

This report was prepared after consultation with:

- Head of Law and Regulation – Monitoring Officer, and Senior Information Risk Owner (SIRO)
- Head of Finance – Chief Financial Officer
- Head of People, Policy and Transformation
- Chief Internal Auditor
- Information Governance Group

Signed

Background

The purpose of this report is to provide an assessment of the information governance arrangements for the council and identify where action is required to address weaknesses and make improvements. The benefits of this report are as follows:

- Provide an overview of the council's information governance arrangements
- Highlight the importance of information governance to the organisation, the risks faced and the current level of risk
- Where relevant this report will compare performance with previous years and with the aim of continuous improvement
- Identify and address weaknesses and develop an action plan
- Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties. The fines associated with General Data Protection Regulation (GDPR) came in to place on 25th May 2018 with a maximum fine of 20 Million Euros or 4% of turnover.
- To identify the better use of data in designing, delivering and transforming public services to improve outcomes and drive efficiencies.

Report
This is attached as appendix to this Report and includes an Executive Summary of key highlights, including:

Compliance and audit

- **Public Services Network (PSN)** – whilst the council was PSN compliant from 13th August 2021, at time of writing the authority's PSN compliance lapsed on 13th August 2022
- **Payment Card Industry (PCI) standard**
    - **In July 2022, with the assistance of SRS, the council completed the remaining work required and were informed that we had been successful in achieving PCI compliance**
- **General Data Protection Regulation (GDPR) and Data Protection Act 2018**
    - GDPR came into force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. Following on from Brexit, the EU GDPR no longer applies to the UK. For organisations operating inside the UK, the Data Protection Act 2018 (DPA 2018) is applicable
    - Priority areas are supporting the Welsh Track, Trace and Protect (TTP) programme, Data Protection Impact Assessments (DPIA's), The Information We Hold
- **Cyber Stock Take**
    - Newport City Council scored well in Cyber Stocktake 4, with 3 scores above the Welsh average, 2 the same and 1 below the Welsh average

Information Governance culture and organisation

- At time of the report writing the Information Management Service Level Agreement (SLA) has been extended for a further three years for all primary schools and now includes three high schools
- Quarterly meetings of the Information Governance Group and Data Protection Group take place to oversee information risk management in conjunction with other stakeholders including Shared Resource Service

Communications and Awareness Raising

- Continue to raise awareness with staff
- **Corporate staff training numbers have improved in part due to Microsoft Teams delivery method**
- **Social Services training numbers have increased following Coronavirus pandemic challenges but more to be done**
- **Large amount of training provided for schools**
- **Specific training provided for Track, Trace and Protect (TTP) staff**
- GDPR e-learning uptake has been excellent

Information Risk Register

- Continues to be maintained with contribution to Annual Governance Statement as necessary

- In December 2021, the local authority was made aware of a world-wide vulnerability in systems that use a Java based logger known as Apache Log4J that was reviewed/actioned by SRS

Security incidents

- An increase in reported incidents, possibly as a result of increased awareness around issues as a result of GDPR and the increase of staff working from remotely from home.
- One significant incident reported to the ICO. The ICO took no action

Information Sharing

- Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)
- The Newport Intelligence Hub (NIH) has access to more data than ever to inform services and obtain greater insights into user needs and local places. The Information management team is committed to promote the lawful sharing of this data for these purposes.

Business Continuity

- There is an ever-increasing reliance on digital technology to support business activities as identified in Business Impact Analysis during the Coronavirus pandemic
- It is important to maximise the availability of systems that this is expected to be improved by the planned SRS data centre move
- A more proactive move of systems to the cloud took place in 21/22 including that of the www.newport.gov.uk web site in March 22. The proactive move of systems will continue

Technology Solutions

- As planned last year, secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business
- The existing remote access solution has been replaced with Microsoft Always ON VPN
- **A Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) proposed by SRS to partners has been agreed and a solution has been procured with implementation by March 2023**

Records Management

- Continued roll out of EDMS solution across council, project manager in post continues to progress deployment
- We have reduced the number of paper records held in Modern Records by disposing of records which have reached their retention period

Freedom of Information

- **Exceeded target for year**
- Increase in number of requests from last year but below previous record highs
- Continue to promote the use of open data sets and adding new ones where appropriate

Subject Access Requests

- Subject Access Request target not met for year but has increased from last year. There were still some difficulties in staff accessing Civic Centre paper records as a result of the Coronavirus pandemic and the requirements to work from home

Financial Summary

There is no specific cost associated with the report. Any costs incurred would be normal costs associated with the running of the service. However, the report is designed to highlight risks and to reduce potential penalties from the Information Commissioner's Office (ICO) if information risk is not managed effectively.

Risks

A huge amount of information is held by the organisation. This needs to be managed appropriately. Further details of risks are provided in the report and those identified below represent some high level risks.

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Data breach results in fine imposed by the Information Commissioner's Office or reputational damage	H	L	All the actions detailed in this report are designed to mitigate this risk.	Digital Services Manager and Information Management team
Council is unable to make best use of, and share the data it holds due to a lack of confidence in the integrity and security of the information.	H	L	Digital strategy sets the overall direction for the management of information and is being reviewed to ensure it meets future needs. Day to day operational guidance provided by Digital and Information service. The strategy is being reviewed and updated	Digital Services Manager and Information Management team

* Taking account of proposed mitigation measures

Information Risk is also incorporated into Corporate Risk Register reporting, as outlined in this report.

Links to Council Policies and Priorities

The council's Information Risk Management Policy sets out the council's approach to information risk management including roles and responsibilities. The policy also details the processes in place to manage information risks effectively, including the Annual Information Risk Report.

The Digital Strategy, approved by Cabinet October 2015 sets the overall direction for the management of information, and information governance is also considered in the Annual Governance Statement produced for the inclusion in the council's Annual Statement of Accounts and reported to Audit Committee. The actions outlined in this report form part of the People, Policy and Transformation service plan for 22/23.

Options Available and considered

1. **Do nothing**
2. **Note the annual information risk report and endorse its findings.**

Preferred Option and Why

The preferred option is option 2 – note the Annual Information Risk Report 2021-22 and endorse its findings. This will provide an understanding of the current position in relation to information governance and give an opportunity to monitor progress on actions identified

Comments of Chief Financial Officer
There are no direct costs involved in or coming out of this report. It highlights current issues and work-plans associated with the Council's governance and control over data. There are significant potential risks and associated financial penalties for any breaches of the Council's duty in this respect, which would adversely impact on the Council's budget.

Comments of Monitoring Officer
There are no specific legal issues arising from the Report. The Annual Information Risk Report confirms that the council has in place robust information governance arrangements and security policies to meet its statutory obligations under the Data Protection Act, FOIA, PSN accreditation and information sharing protocols. Further work has been carried during the past twelve months in implementing the requirements of GDPR, cyber security and addressing the information security implications of home working and new technology. However, further work is still required to renew the PSN compliance. The number of reported security incidents has again increased, but this may be due to an increase in training and awareness and most reported data breaches were of a minor nature as a result of human error. Remote and home-working arrangements have significantly reduced the number of incidents of lost paper-work and devices. Only one significant data breach had to be referred to the ICO but no action was taken due to the steps taken to contain and rectify the breach. The updated action plan also sets out the on-going measures being taken to maintain and improve the integrity of the council's information security systems and to deliver further training to increase awareness and compliance.

Comments of Head of People, Policy and Transformation
As the report author, the comments of the Head of People, Policy and Transformation are recorded throughout.

This report acknowledges the current arrangements in place to safeguard the information and data used by the council, which enables the delivery of council services. The action plan included in this report demonstrates the council is proactively taking the necessary measures to safeguard council information and data from being lost, stolen, or misused.

The report notes how the Council's information governance arrangements are in line with the sustainable development principle under the Well-being of Future Generations Act. There are no HR issues arising directly from this report.

Comments of the Chief Internal Auditor
The report demonstrates the Council has relevant and appropriate controls in place to demonstrate effective management of Information Governance. Where gaps have been identified an appropriate action plan has been included to mitigate any risks and demonstrate how improvements will be made in future.

Local issues
No specific local issues.

Scrutiny Committees
This report was presented to Scrutiny Management Committee on 23rd September 2022 Scrutiny comments are as below and these are reflected in the report:-

- The committee were content with the report and its contents.
- The committee felt that there should be a stronger drive for the area to ensure that training is completed.
- The committee felt that it could be beneficial to include information regarding whether the disproportionate cost clause regarding Freedom of Information requests had been enacted in the report.

Fairness and Equality Impact Assessment

Wellbeing of Future Generations (Wales) Act 2015

The information risk management framework incorporates the five ways of working as below:

- Long term – organisationally this is a long term development with increased maturity of information risk management and continued commitment by the organisation
- Prevention – preventative measures are key to information risk management especially around staff awareness and training
- Integration – managing information risk is part of the council's wider risk management process including the corporate risk register as appropriate
- Collaboration – information risk is managed in conjunction with the council's IT service delivery partner, the Shared Resource Service (SRS) as well as with suppliers who process data on behalf of the council. In addition the council's support of the Wales Accord on the Sharing of Personal Information (WASPI) demonstrates its commitment to information sharing for effective collaboration
- Involvement – the council has direct contact with members of the public and businesses in relation to handling information and this is strengthened by GDPR

Equality Act 2010

Equalities is considered in service delivery and is an important consideration in the review of the council's Digital Strategy.

Socio-economic Duty

Service delivery also considers the Socio-economic Duty which will also be an important consideration in the review of the council's Digital Strategy. The Socio-economic Duty ("the Duty") highlights the Welsh Government's commitment to safeguarding equality and human rights.

The Duty gives us an opportunity to do things differently in Wales. It puts tackling inequality at the heart of decision-making and will build on the good work that public bodies are already doing.
The aim is for the Duty to become another key mechanism in supporting the most vulnerable in our society. By requiring public bodies to make better decisions, ones which place consideration of inequality of outcome which arises from socio-economic disadvantage at their heart, it will further help tackle the uncertainty of EU exit and our recovery from Covid-19, allowing us to move towards the reconstruction of a fairer and more prosperous Wales.

Welsh Language (Wales) Measure 2011

The requirements of the Welsh Language Act are considered in service delivery as well as the review of the council's Digital Strategy.

Children and Families (Wales) Measure

No specific consultation with children and young people is relevant as part of this report.

Consultation

Comments from members of the council's Information Governance Group have been included within the text of the report in line with their role as key strategic stakeholders.

Background Papers

Information Risk Management Policy
Annual Information Risk Report 20/21
Annual Governance Statement 20/21
Corporate Risk Management Strategy and Register
Digital Strategy 2015-2020

Dated: 21 October 2022

Annual Information Risk Report 2021/22

Created by	Information Governance
Date	24/03/2021
Reviewed by	Tariq Slaoui
Date	03/10/2022

Document Control

Version	Date	Author	Notes / changes
V0.1	23/03/2021	Tariq Slaoui	Initial draft
V0.2	11/10/2021	Tariq Slaoui	Updated
V0.3	31/12/2021	Tariq Slaoui	Updated
V0.4	11/07/2022	Tariq Slaoui	Updated
V0.5	18/07/2022	Tariq Slaoui	Updated
V0.6	28/07/2022	Tariq Slaoui	Updated
V0.7	10/08/2022	Tariq Slaoui	Updated
V0.8	16/08/2022	Tariq Slaoui	Updated
V0.9	23/08/2022	Mark Bleazard	Updated for Cabinet Member/Scrutiny
V1.0	26/08/2022	Mark Bleazard	Business continuity updated
V1.1	03/10/2022	Mark Bleazard	Updates following Scrutiny

Table of Contents

Contents

Executive Summary

Data and information is the lifeblood of the council and a critical strategic asset in the delivery of services, transformation and change. The council has a statutory requirement to look after the data it holds in line with General Data Protection Regulation (GDPR) and the associated Data Protection Act 2018. As a result of GDPR, the Information Commissioner's Office (ICO) has the power to fine organisations up to 20 Million Euros or 4% of turnover. **Many staff working from home as a result of the Coronavirus pandemic provides some specific challenges, especially with greater concerns over cyber attacks.**

This is the tenth Annual Information Risk Report which provides an assessment of the information governance arrangements for the council as outlined in the Information Risk Management Policy. The report highlights:

Compliance and audit

- **Public Services Network (PSN)** – whilst the council was PSN compliant from 13th August 2021, at time of writing the authority's PSN compliance lapsed on 13th August 2022
- **Payment Card Industry (PCI) standard**
    - **In July 2022, with the assistance of SRS, the council completed the remaining work required and were informed that we had been successful in achieving PCI compliance**
- **General Data Protection Regulation (GDPR) and Data Protection Act 2018**
    - GDPR came into force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. Following on from Brexit, the EU GDPR no longer applies to the UK. For organisations operating inside the UK, the Data Protection Act 2018 (DPA 2018) is applicable
    - Priority areas are supporting the Welsh Track, Trace and Protect (TTP) programme, Data Protection Impact Assessments (DPIA's), The Information We Hold
- **Cyber Stock Take**
    - Newport City Council scored well in Cyber Stocktake 4, with 3 scores above the Welsh average, 2 the same and 1 below the Welsh average

Information Governance culture and organisation

- At time of the report writing the Information Management Service Level Agreement (SLA) has been extended for a further three years for all primary schools and now includes three high schools
- Quarterly meetings of the Information Governance Group and Data Protection Group take place to oversee information risk management in conjunction with other stakeholders including Shared Resource Service

Communications and Awareness Raising

- Continue to raise awareness with staff
- **Corporate staff training numbers have improved in part due to Microsoft Teams delivery method**
- **Social Services training numbers have increased following Coronavirus pandemic challenges but more to be done**
- **Large amount of training provided for schools**
- **Specific training provided for Track, Trace and Protect (TTP) staff**
- GDPR e-learning uptake has been excellent

Information Risk Register

- Continues to be maintained with contribution to Annual Governance Statement as necessary
- In December 2021, the local authority was made aware of a world-wide vulnerability in systems that use a Java based logger known as Apache Log4J that was reviewed/actioned by SRS

Security incidents

- An increase in reported incidents, possibly as a result of increased awareness around issues as a result of GDPR and the increase of staff working from remotely from home.
- One significant incident reported to the ICO. The ICO took no action

Information Sharing

- Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)
- The authority is committed to gaining a better understanding about the value of data in discharging its services, to share and better use data to:
    - design services around user needs
    - engage and empower citizens
    - drive efficiencies and transformation
    - promote the innovative use of data
    - be transparent and accountable

Business Continuity

- There is an ever-increasing reliance on digital technology to support business activities as identified in Business Impact Analysis during the Coronavirus pandemic
- It is important to maximise the availability of systems that this is expected to be improved by the planned SRS data centre move
- A more proactive move of systems to the cloud took place in 21/22 including that of the www.newport.gov.uk web site in March 22. The proactive move of systems will continue

Technology Solutions

- As planned last year, secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business
- The existing remote access solution has been replaced with Microsoft Always ON VPN
- **A Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) proposed by SRS to partners has been agreed and a solution has been procured with implementation by March 2023**

Records Management

- Continued roll out of EDMS solution across council, project manager in post continues to progress deployment
- We have reduced the number of paper records held in Modern Records by disposing of records which have reached their retention period

Freedom of Information

- **Exceeded target for year**
- Increase in number of requests from last year but below previous record highs
- Continue to promote the use of open data sets and adding new ones where appropriate

Subject Access Requests

- Subject Access Request target not met for year but has increased from last year. There were still some difficulties in staff accessing Civic Centre paper records as a result of the Coronavirus pandemic and the requirements to work from home

1. Background and Purpose

As a local authority we collect, store, process, share and dispose of a vast amount of information as part of our duties. These duties are defined in EU General Data Protection Regulation (GDPR) that commenced on 25th May 2018 and the associated UK Data Protection Act 2018. This legislation places a greater responsibility on the council to be more clear and transparent about what data is processed and how to give citizens confidence that their data is being handled appropriately. Accordingly. it is even more important that the council meets its statutory responsibilities effectively and **protect the personal information it holds throughout its life cycle;** from creation through storage, use, retention, archiving and deletion. The principle of using and securing data is outlined in the Digital Strategy that is currently being reviewed and draft themes have been developed. Data is a valuable organisational asset and a key development is the creation of the Newport Intelligence Hub. This team's role is to maximise the value of data to the organisation, especially for use in operational, tactical and strategic decision making by the organisation. This requires processing of information in line with GDPR.

The actions outlined in this report form part of the People, Policy and Transformations service plan and also considered in the Corporate Risk Management Strategy and Corporate Risk Register.

1.1. Purpose of the Report and Benefits

The purpose of this report is to provide an assessment of the information governance arrangements for the council and identify where action is required to address weaknesses and make improvements.
The benefits of this report are as follows:

- Provide an overview of the council's information governance arrangements
  - Highlight the importance of information governance to the organisation, the risks faced and the current level of risk
  - Where relevant this report will compare performance with previous years and with the aim of continuous improvement
- This is the tenth Annual Information Risk Report.
  - Identify and address weaknesses and develop an action plan
  - Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties. The fines associated with General Data Protection Regulation (GDPR) came in to place on 25th May 2018 with a maximum fine of 20 Million Euros or 4% of turnover.
  - Ensure that appropriate risks are escalated to the Corporate Risk Register

2. Current Position

This part of the report identifies the council's current position in relation to information governance; this includes a number of external compliance requirements. The principles of the current Digital Strategy are sound. However, it now feels slightly dated and a new strategy is being drafted to make it more relevant and up to date. It will continue to highlight the importance of effective information management and data sharing with robust information security to protect business and citizen data from threats, loss or misuse. Key roles and responsibilities for individuals and groups are outlined below.

2.1. Compliance and Audit

The council is subject to accreditation to the Public Services Network (PSN) by the Cabinet Office. The council is also required to comply with the Payment Card Industry Data Security Standards (PCI-DSS) when it handles card payments for customers. In addition, the council is subject to audit from Audit Wales (formerly Wales Audit Office) to ensure appropriate information governance is in place.

Public Services Network (PSN) compliance

Whilst the council was PSN compliant during from 13th August 2021, at time of writing the authority's PSN compliance lapsed on 13th August 2022. The annual IT Health Check has been carried out and we are awaiting the formal report, followed by the development of a suitable remediation action plan and submission will be made when appropriate. The Shared Resource Service (SRS) procures and schedules health checks for partners together. The number and variety of risks mean that work is required throughout the year to protect the council's data and systems, and this is included in the SRS' resource allocation. Risks around cyber security remain a specific concern as highlighted by the National Cyber Security Centre (NCSC) and they are included on the Corporate Risk Register and this remains a challenge to all organisations whether public or private sector. The council is committed to continued compliance with PSN standards.

Payment Card Industry Data Security Standards (PCI-DSS)

At the time of writing the council has now satisfied the requirements of the Payment Card Industry (PCI) Data Security Standards. Last year, the council procured assistance from an external organisation to undertake a gap analysis and subsequent remediation action plan to address any shortfalls. In July 2022, with the assistance of SRS, the council completed the remaining work required and were informed that we had successfully completed an assessment against the PCI-DSS v3.2.1

General Data Protection Regulation (GDPR) and Data Protection Act 2018

General Data Protection Regulation (GDPR) is a regulation that strengthens and unifies data protection for individuals within the European Union (EU). GDPR came into force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. This legislation has been in place for about 4 years now and the UK has subsequently left the European Union because of Brexit. In this regard the UK has to demonstrate that its data protection regime is suitable for holding the data of EU citizens. The Information Commissioner's Office (ICO) leads on this for the UK. On the 28th June 2021, the EU Commission announced that adequacy decisions for the UK have been formally approved. This means that organisations in the UK can continue to receive and send data to and from the EU without having to make any changes to their data protection practices. Following on from Brexit, the EU GDPR no longer applies to the UK. For organisations operating inside the UK, the Data Protection Act 2018 (DPA 2018) is applicable.

DPA 2018 is a standard agenda item for the Information Governance Group. A Data Protection Group meets quarterly in recognition that data protection is an on-going activity.

As a reminder a summary of the DPA 2018 is detailed below:

- The maximum fine is 20 Million Euros or 4% of turnover
- There is a requirement to document the personal data held and keep a record of our processing activities.
- Data breach reporting is mandatory for certain data breaches. The ICO should be informed of significant data breaches within 72 hours.
- Enhanced rights for data subjects. Privacy notices are mandatory and the organisation must identify a 'lawful basis' for each of our processing activities. Consent has been strengthened. However, this is just one of several lawful bases. Specific guidance relating to children and their rights is available
- Local authorities cannot rely upon "legitimate interests" as a legal basis for processing data.
- The authority must respond to requests for personal data. These are known as Subject Access Requests and we aim to process and respond to request within 30 calendar days.
- Requirement for Data Protection Impact Assessments, particularly for new projects and/or technology implementations.
- Requirement for Data Protection Officer role
- Further consideration of data stored outside the EU although an adequacy decision has been approved.

A number of large fines have been issued to date demonstrating the greater power that the Information Commissioner's Office (ICO) and other national regulators have. The largest UK fine to date is of £20 Million to British Airways. The largest public sector fine is a fine to the Cabinet Office £500,000 for disclosing postal addresses of the 2020 New Year Honours recipients online.

A GDPR Task and Finish Group was established in 2017, with representation from each service area and schools. The group has evolved into the corporate Data Protection Group and continues to meet on a quarterly basis. The council has embedded many processes and is prioritising the following development areas:

- Awareness raising – the Data Protection group has ensured that data protection is the subject of discussion at the various service area management meetings. The group is well attended and now includes representatives from primary schools. The Information Management team have used E-bulletins and corporate communications throughout the Coronavirus pandemic to provide corporate updates. Specifically, communications have been undertaken to ensure that staff working from home are doing so in a secure manner. The Information Management team produce and communicate monthly Primary Schools newsletters with advice and guidance on Data Protection, Freedom of Information and Information security matters. The Meta Compliance solution will be utilised in future to increase awareness across the authority
- Data Protection Impact Assessments – DPIA's are mandatory for new technology implementations and projects that involve the systematic monitoring of individuals and/or the large-scale processing of special category data. In response to the Coronavirus pandemic and as a joint data controller to the Welsh Test, Trace and Protect (TTP) service, we assisted in the development of an all Wales TTP DPIA both for the service and the IT systems. Others are being considered but the screening process will ultimately determine this. The SRS have confirmed that all technology requests from Newport City Council are subject to DPIA screening
- The Information We Hold – the accountability principle states that we should document the data that we hold along with records of processing activities. The council already manages an Information Asset Register which is based upon the systems that have been identified as a priority. The Information Management team, in conjunction with Digital services and The Data Protection Group is expanding this register to include paper records. This work will also seek to identify cloud-based provision of services and the governance arrangements around these
- Significant Information Governance work has been undertaken to support the Welsh Track, Trace and Protect (TTP) programme during 2020/21 and 2022. Further work has been undertaken to support information sharing in relation to the arrival of Ukrainian refugees

Cyber Stock Take

Newport City Council, along with all other local authorities in Wales, took part in the fourth Cyber Stock Take exercise designed to give an indication of each local authority's maturity in cyber security. This was compiled by means of a self-assessment questionnaire and the results of the benchmarking are below. A specific action plan has been developed, the results of which will be included in the Cyber Stocktake 5 submission.

Leadership, Reporting and Ownership:
Newport City Council 93% (83%, 73% & 90% in previous years), **All Wales Average is 84%**

Governance, Structure and Policies:
Newport City Council 92% (67%, 80% and 92% in previous years). **All Wales Average is 78%**

Partnerships, Information advice and guidance:
Newport City Council 100% (100%, 100% and 100% in previous years). **All Wales Average is 100%**

Technology Standards and Compliance:
Newport City Council 83% (77%, 75% and 77% in previous years). **All Wales Average is 83%**

Training and Awareness Raising:
Newport City Council 67% (65%, 60% and 65% in previous years). **All Wales Average is 82%**

Overall Maturity Score:
Newport City Council 87% (71%, 78% and 84% in previous years). **All Wales Average is 80%**

Weaknesses identified are already being addressed in most cases including the implementation of a SIEM/SOC solution as detailed elsewhere in this report and increased awareness raising as a result of the Metacompliance solution. Further improvements identified will be pursued.

Audit Wales

Audit Wales, formerly known as the Wales Audit Office (WAO) carries out audits annually of the risks around financial systems which involve IT and Information Governance. This work generally has some recommendations that need to be acted upon.

2.2. Information Governance Culture and Organisation

The council has been a partner of the Shared Resource Service (SRS) since April 2017. Since then, representatives from the SRS attend various Newport City Council groups. There is also a client side role sits within the Digital team and this relationship has developed since joining the partnership.

Information Governance Culture

The information governance culture has previously been investigated by virtue of staff surveys. These demonstrated good staff awareness of information governance issues and good buy in.

Organisation

Senior Information Risk Owner (SIRO) role
The council's Senior Information Risk Owner (SIRO) role is part of the Head of Law and Standards role. The SIRO role is the senior officer responsible for information risks within the organisation and is part of the council's Corporate Management Team. Day to day operational management is provided by the Information Management team that reports to the Head of People, Policy and Transformation. As detailed below, the SIRO role is more senior and is distinct from the Data Protection Officer (DPO) role below.

Data Protection Officer (DPO) Role
Under General Data Protection Regulation) the council needs to specify its Data Protection Officer (DPO). This role is incorporated within the duties of the existing Digital Services Manager post. As part of the Service Level Agreement with primary schools, the Digital Services Manager post is also the DPO for primary schools.

Information Governance Group
The Information Governance Group meets quarterly chaired by the Strategic Director – Transformation and Corporate. This ensures that there is no conflict of interests of the operational lead for information governance also being the chair of this group. Strategic information governance issues are discussed by this group with standard agenda items that includes GDPR. Membership of the group includes representation from the Shared Resource Service (SRS) which will be a major contributor to this work.

Shared Resource Service (SRS) - The IT Service became a partner in the Shared Resource Service (SRS) in April 2017. As well as Newport City Council the SRS is made up of Torfaen County Borough Council, Monmouthshire County Council, Blaenau Gwent County Borough Council and Gwent Police. There is SRS representation on the council's Information Governance Group as well as other groups such as the Digital City Board. The client-side role is managed by the Digital team and this important relationship in service delivery as well as information governance continues to develop. The SRS has a small team that provides a complementary and slightly more technical function within the SRS that works closely with the Information Management team in Newport.

Councillor Data Protection
An important aim of this report is to ensure that members and senior officers are aware of the data protection responsibilities of the council and to enable guidance to be provided. This is especially relevant given GDPR and the Data Protection Act 2018. The annual risk report represents a useful opportunity for the Scrutiny Management Committee to comment and make suggestions on the past year's performance and improvements going forward. This has been beneficial in shaping the actions going forward.

Information Asset Register
The development of an Information Asset Register, based on a template from The National Archives was completed for priority systems during 2016/17. This identifies the owner of information, the information stored within the system, how this is shared and various other pieces of information. Further work is required to extend the Information Asset Register for all the information the council holds and this has now commenced and will be part of the work of the Data Protection group and Digital Services as appropriate. This will ultimately become a Record of Processing Activities (RoPA). A cloud services register has been developed in line with our policy of deploying solutions to the cloud.

Schools
Schools are "data controllers" under the Data Protection Act and therefore need to be equipped to handle data appropriately. Guidance is provided to schools by staff in Education and Information Management. A Service Level Agreement (SLA) for primary schools with the Information Management team has been in operation for nearly three academic years now. Regular guidance and advice has been provided to primary schools on this basis and this service has been well received. The Information Management team has also provided specific training for schools as detailed elsewhere in this report with further positive feedback. In January 2022, the Information Management team extended the SLA offer to include high schools. At time of the report writing the SLA has been extended for a further three years for all primary schools and now includes three high schools.

1.1. Communications and Awareness Raising

Employees are often the weakest link in terms of preventing incidents. The information security incidents section reflects this, and technical measures will never be totally effective especially given the increased sophistication of cyber-attacks including phishing. The move to home working has increased the risk of this and so employee awareness is more important than ever. This is generally achieved via staff training together with other forms of communication to improve awareness.

Staff Guidance

Regular reminders of good practice have been provided in the staff bulletin and on the intranet on various important subjects especially because of home working during the Coronavirus pandemic. During 2021/22, the council regularly reminded staff of the importance of subjects such as:

- Phishing emails
- Effective redaction
- Guidance on working from home
- The appropriate use of video conferencing services
- The use of social media messaging for work purposes
- Email message encryption and how to send files securely

The team regularly assess information from the Information Commissioner's Office (ICO) and other sources to ensure that key messages are communicated to employees including good and bad practice. The development of the Service Level Agreement with primary schools means that information is provided to primary schools too with appropriate revision as necessary.

Training Courses

The council continues to provide classroom style training to staff to provide the most interaction possible and improved learning experience. This is now provided virtually using Microsoft Teams and this has been very well received with good attendance. This complements e-Learning that is required to be completed by new starters and for refresher purposes. The content is regularly kept up to date to reflect developments in this area and relevant news coverage.

- Meta Compliance Policy Management Solution
- Social Services courses
- Corporate courses
- Councillor courses
- School courses
- Other courses and presentations
- Information Management team training
- E-learning

In early 2022, the council procured the Meta Compliance Policy Management Solution which allows us to deliver cyber security related content to users' desktops. A project plan is currently being developed to ensure that utilisation is high.

Training courses represent a continued commitment to information security by the council with a revised delivery method using Microsoft Teams. Training is a key area as people are generally considered the weakest link in relation to information security, especially when working from home as a result of the Coronavirus pandemic. There will never be totally comprehensive technical measures to protect data. Training provided to staff is a key part of investigations carried out by the Information Commissioner's Office (ICO).

Social Services Courses

Social Services employees continue to represent a high-risk group due to the nature of the information they handle as part of their roles and training is compulsory for these staff. In 2020/21, no courses were scheduled due to difficulties of certain staff in particular roles accessing Teams based training. These courses have now recommenced and some staff have attended the corporate training course.

A breakdown per year is included below.

Year	Number of staff who attended
2021/22	31
2020/21	0
2019/20	172
2018/19	157
2017/18	237
2016/17	144
2015/16	147
2014/15	182
2013/14	226

Corporate Courses

These courses continue to be scheduled on a monthly basis, primarily for staff other than Social Services. The number of staff that attended the corporate course has increased from 74 in 2020/21 to 181 in 2021/22. Whilst attendance does vary a little year on year the number of staff attending remains consistent.

Year	Number of staff who attended
2021/22	181
2020/21	74
2019/20	98
2018/19	105
2017/18	114
2016/17	118
2015/16	114
2014/15	152
2013/14	93
2012/13	57

Feedback from staff attending courses is gathered for each training course held and continues to be positive. The change to virtual training using Microsoft Teams has been well-received.

Councillor Courses

The last training course for councillors took place in November 2018 with 24 out of the 50 councillors attending. Councillors, like all council staff, need to undertake mandatory e-learning before they are provided with access to the council's network. Following on from the local government elections tin May 2022, the Information Management team plans to deliver further training for new and existing elected members.

Schools Courses

Schools have been engaged with the Information Management team in relation to GDPR including representation on the Data Protection Group. A service level agreement for primary schools for information management has been agreed which includes regular training. This SLA has recently been widened to include elements of cyber security awareness. As a new development in 2022/23, the SLA has also been offered to high schools. **In 2021/22 119 school staff were trained.**

Year	Number of staff who attended
2021/22	119
2020/21	78

Training for primary schools, and now some high schools, remains a priority for the return to classrooms in September.

Other Courses and Presentations

104 staff received specific training relating to their area, including 59 contact tracing staff.

Information Management Team Training

All four current members of the Information Management team have passed the British Computer Society (BCS) Certificate in Data Protection including three members of staff on the updated legislation. In addition to this, the Information Manager is a Certified Information Security Manager (CISM)

E-Learning

All staff that need access to the council's computer network are currently required to undertake GDPR e-learning before they can access the network. The GDPR e-learning module provides guidance to staff on their obligations under the Data Protection Act 2018**. In 2021/22 422 staff completed the NCC GDPR e-learning module.**

Information Policy Development

Policies form an invaluable way of documenting legal requirements and best practice. They provide guidance for employees to ensure information governance is integrated into the way the council operates. As well as developing new policies where appropriate, it is also necessary that existing policies are updated to ensure that they remain fit for purpose, including any changes as a result of the partnership with the Shared Resource Service (SRS). Staff are reminded of these policies where appropriate.

Updated Policies

An extensive review of policies took place in 2019 to reflect the changes in the new GDPR legislation. As such, there has not been a requirement to make further significant changes other than general reviews to ensure that they are still valid and up to date. The following were updated this year:

- Schools Information Security Policy

Staff are made aware of policy changes with reminders through the regular staff bulletin. All policies use 'key messages' for ease of understanding and are published as part of the overarching Information and IT Security Policy and on the council's intranet, with appropriate version control. A further review of policies is required to ensure they are all up to date and valid. This is planned for the coming year.

2.4. Information Risk Register

An information risk register is maintained that identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. The risk register is regularly updated and shared with the Information Governance Group to keep them informed of risks. In December 2021, the local authority was made aware of a world-wide vulnerability in systems that use a Java based logger known as Apache Log4J. The vulnerability has the potential to allow unauthorized access to NCC systems. The SRS have been updating the affected systems with the latest patch releases to limit the authority's exposure to the threat.

Information risks are considered as part of the council's Annual Governance Statement and the Corporate Risk Register. Cyber Security is now formally recorded as a risk on the corporate risk register. The Chief Internal Auditor is a member of the Information Governance Group which helps to join up services. The control strategies for information risk are detailed within this report.

2.5. Information Security Incidents

All information security incidents are reported, logged and investigated. Information security incidents range from lost phones/other devices, password issues all the way to data breaches where data is lost or passed to the incorrect recipient. Lessons need to be learned from these incidents to improve practice in future to minimise the risk of recurrence. In line with GDPR, serious incidents that meet certain criteria must be communicated to the ICO within 72 hours and data subjects informed without delay.

66 security incidents were recorded in 2020/21 compared with 62 in the previous year. It is difficult to establish whether this reflects our position or if there has been an increased level of reporting. Given the increased awareness around GDPR and internal communications relating to incident reporting procedures, it is likely that that the increase can be attributed to GDPR awareness. The move to remote, home working in March 2020 resulted in a decrease in the amount of lost/stolen paperwork as staff needed to work more digitally and relied less on paperwork. There was also a significant drop in the number of incidents relating to lost or stolen devices. This is likely to be attributed to staff largely working from home using Microsoft Teams to hold meetings instead of travelling or moving around offices.

Details of reported incidents over previous years are provided below:

Year	Total incidents	Disclosed in Error	Lost or Stolen Hardware	Lost or Stolen Paperwork	Non secure disposal – paperwork	Other - non principle 7 (now DPA 2018 principle 6) incident	Other - principle 7 (now DPA 2018 principle 6 - security of personal information) incident	Technical security failing
2021/22	80	58	7	1	0	0	9	5
2020/21	66	48	3	1	1	0	10	3
2019/20	62	39	11	4	1	0	6	1
2018/19	46	29	7	3	1	0	4	2
2017/18	34	18	6	4	0	0	4	2
2016/17	43	25	5	0	0	1	8	4
2015/16	62	23	12	2	0	9	11	5
2014/15	66	14	23	0	2	18	0	9
2013/14	64	14	9	6	1	8	4	22
2012/13	63	No split by category available						

Analysis by category is always to some extent subjective as incidents could easily be categorised in more than one category. Therefore, these categories should be seen as indicative only.

As is the pattern in previous years, the majority of security incidents were not of real significance. Some of the themes which are similar to previous years are as follows:

- Incidents arising as result of human error form the majority of incidents. This trend is typical across local government and other sectors.
- E-mails sent to the incorrect recipient or including information that that shouldn't have been included
- Paper documents sent to the incorrect recipient or including information that that shouldn't have been included
- Reduction in lost council issued encrypted devices (laptops, smartphones with no personal data so low risk)

The most significant incident during this year was:

During the course of a minor breach investigation that included a redacted PDF version of a sensitive report, we became aware that the redaction had not been carried out appropriately. There was no evidence to suggest that the recipients were aware of the error and would be highly unlikely to access the redacted information. The individuals affected were informed and we reported this incident to the Information Commissioner's Office (ICO) who investigated and subsequently took no action. During our internal incident investigation actions were taken to minimise the possibility of any further occurrences.

2.6. Information Sharing

Partnership and collaborative working drives sharing of increased amounts of information between the council and other organisations. The Wales Accord on the Sharing of Personal Information (WASPI) requires public sector organisations to follow agreed guidance in the development of Information Sharing Protocols (ISP's). The council signed up to WASPI in January 2011. The WASPI guidance has recently been updated to reflect the issues as a result of Coronavirus pandemic. The Information Management team leads on this work and has developed a number of ISP's with services and other organisations. Documentation for WASPI has been reviewed by the WASPI Team in NWIS to ensure that it is appropriate for GDPR. A full list of the council's ISPs is published on the Intranet. The following represents developments in 2021/22:

Information Sharing Protocols (ISP's)

An ISP for the Newport Practitioners Forum has been developed and quality assured. An ISP to support the sharing of information for Ukranian Refugees Programme was developed and assured in June 2022.

Data Disclosure Agreements (DDA's)

Data Disclosure Agreements (DDA's) are for one way disclosure of information from one organisation to another. These are recommended as part of the WASPI initiative and are seen as best practice for formalising such information disclosure.

Data Disclosure Agreements have been developed as follows:

DDA's in 2021/22:

- Baby and me Barnardo's programme
- Council Tax data acquisition – Office for National Statistics
- Flytipping Overt CCTV

2.7. Business Continuity

There is an ever-increasing reliance on digital technology to support business activities and it is therefore important to maximise the availability of systems. Increased resilience was a factor in the decision to join the Shared Resource Service (SRS) and this is expected to be improved by the planned data centre move now expected earlier than planned within 22/23.

A more proactive move of systems to the cloud took place in 21/22 and will continue. This is designed to provide greater availability and better business continuity/disaster recovery. One especially important cloud migration is that of the www.newport.gov.uk web site to the cloud in March 22.

Under the Civil Contingencies Act 2004 the council has a statutory duty to put in place business continuity management arrangements. The council is committed to ensuring robust and effective business continuity management as a key mechanism to restore and deliver continuity of key services in the event of a disruption or emergency. One of the essential components of delivering this commitment is to understand how a disruptive event would impact service areas and their ability to continue their key service delivery. To achieve this, each service area is required to undertake a 'Business Impact Analysis Form For Critical Service Delivery'.

Although the programmed Corporate Business Continuity Management (BCM) work was suspended on the onset of the Coronavirus pandemic in March 2020, to assist the council's preparations and response to the pandemic, each service area assessed the potential impacts of the pandemic to their key business delivery using a Business Impact Analysis template. On the recommencement of this work, it was noted that there has been a significant change in service areas considerations in completing their Business Impact Analysis submissions pre and post pandemic.

For example, findings indicate that, where before the pandemic, the loss of the main operational building would have provided significant challenges with little mitigation available, the well tested and efficient agile working processes with which staff are now familiar provides improved resilience. However, where remote working is now cited as a contingency measure to mitigate the disruption to or loss of the main operational base, the reliance on the continuity of access to digital infrastructure such as servers, home working and internet and applications whether corporately maintained or by third parties, is now highlighted as essential and a heightened risk.

1.1. Technology Solutions

Numerous technical solutions are in place to minimise risk to information and the corporate network generally. PSN and PCI compliance together with the development of business continuity requirements continue to drive technical improvements for information governance. Audit Wales annually review the controls applied to key financial systems (also reported to Audit Committee). As a result of our partnership with the Shared Resource Service, the council will pursue options for collaboration and simplification wherever practical.

Devices
The council now almost exclusively uses laptops for flexibility and mobility. Laptops will always be issued unless there is a specific reason that a desktop device is required in very limited scenarios. The availability of laptops has been invaluable during the Coronavirus pandemic with a large number of staff working from home. Windows 10 is deployed to all devices now. A number of Windows 10 updates will also be required for a large number of devices.

Microsoft 365 (formerly Office 365)
The council previously migrated its e-mail solution to Microsoft 365 with e-mail in the cloud. This provides improved collaborative, agile working facilities and information security. The solution uses Microsoft Multi Factor Authentication (MFA). In addition, the Microsoft Advanced Threat Protection (ATP) solution protects against attachments and links sent in e-mails. The e-mail configuration includes the use of Transport Layer Security (TLS) to encrypt e-mail to external e-mail systems set up to the same standard which should include all local authorities and the public sector generally. Other security standards for e-mail system hygiene have also been implemented.

Microsoft Teams continues to provide instant messaging/chat facilities as well as video/audio conferencing facilities. These facilities are used extensively and enable the organisation to hold a large number of virtual meetings and informal discussions. This has been invaluable to the organisation given the impact of the Coronavirus pandemic and the solution is regularly updated by Microsoft with additional features and other improvements. The latest version of the Microsoft 365 client is rolled out to all Windows devices.

Security Information and Event Management (SIEM) system and Security Operations Centre (SOC)
Consideration was given by all SRS partners to the potential implementation of a Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) with SRS and suppliers to improve preventative measures. This was approved to be funded and implemented by Newport and other partners. This is designed to monitor potential cyber attacks and provide improved preventative measures as a result. It is designed to complement existing solutions. This is due to be implemented by the end of March 2023.

Devices for Members
The first Annual Digital Report highlighted the procurement of tablet devices for members. These, in combination with existing laptop devices have provided a good solution for members in carrying out their role and have been especially beneficial. The refresh of member laptop devices are now included within the wider laptop refresh cycle so there is no need for a capital programme for members at the local government elections in May 2022. Tablet and mobile phone devices will be re-issued as necessary for the turnover of members.

Digital Champions
The council has approximately 30 “Digital Champions” who are advocates for the use of digital technology. They provide a key contact point for services using digital technology. They were a key part of the testing for the roll out of the Microsoft Always On VPN solution and a number of other initiatives.

Remote Access Virtual Private Network (VPN) Solution
The council has commenced the migration from its existing remote access solution to Microsoft Always On VPN solution. This will enable all staff who need to work from home to do so. It will provide the ability to carry out password resets and Windows updates due to its “always on” connection type that will enhance security. Staff are able to work from anywhere where a wireless network is available, as if they were sat at their desk, which also reduces the requirement to carry paper documents.

Multi-Function Devices
‘Follow Me’ print is available to all users, who are able to access council printers from any location with a device. A Multi-Function Device (printer/copier/scanner) contract commenced in October 2017 and an upgrade is planned to provide the latest version of the print management solution. Due to the impact of the Coronavirus pandemic there has been much reduced use of these devices and consideration will be given to what is an appropriate number of devices in future given the likely changes to the number and frequency of staff attending some buildings. This will be included in procurement for a new contract

Secure/Large File transfer solution
As planned last year, secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business.

Xerox Mail "hybrid mail"
More services have been set up to use the "hybrid mail" system to streamline the production of paper and electronic outputs. This enables documents to be sent to production printers in the print room and then processed through the mail room folder/inserter machine. This improves security by ensuring that print outputs are split into envelopes automatically in the folder/inserter machine. The system's use continues to increase led by the EDMS Project Manager with the Digital team

Wireless Staff Access
Wireless Access points are provided in many council buildings. This includes appropriate security controls in place. Major updates planned for 20/21 were delayed due to the impact of the Coronavirus pandemic and equipment ordered has been delayed due to global supply chain issues.

Wireless Public Access
Wireless public access is provided in select council locations and this is protected using appropriate security measures where users can create logins for a limited period. Public Wi-Fi is available in the city centre (Newport City Connect), over 50 public buildings (Newport Community Cloud) and on buses. Gov Wi-Fi is available in various public buildings too.

Physical Security
Major buildings are limited to staff with physical access tokens and alarmed outside of opening hours. As detailed in the physical access policy:

- IT facilities must be located in secure areas protected from unauthorised access
- Any visitors to IT secure areas must be signed in and accompanied at all times
- Computer rooms are subject to additional security measures to protect them from unauthorised access, damage and interference
- Plans are in place to upgrade the system used for door access in the Civic Centre

The policy and Building Access policy also require staff to display identity badges at all times.

Mobile Phones
The council has a large number of mobile phones issued to staff. The vast majority are now smart phones with e-mail, internet access etc. For those that just need calls and texts, basic phones are provided as they are much cheaper. All phones are managed using a Mobile Device Management (MDM) solution to limit access and the ability to wipe phones remotely if required.

Tablets
A relatively small number of tablets are in use across the organisation for specific purposes including tablets for members. These devices are managed using the same Mobile Device Management (MDM) solution as for mobile phones.

2.8. Records and Data Management

Much of the information held by the council would conventionally be stored as paper copies, on network file shares or within teams and service areas. The use of an Electronic Document Management System (EDMS) provides the council with a modern, efficient, electronic system for managing documents, improving the way information and documents are used and the flow of information around the council.

EDMS has a number of benefits including security, access to information and records management by storing all service related documents securely in one place. EDMS is key to ensuring appropriate retention periods of documents stored in the system.

Developments in 21/22 include

- Housing Strategy implementation now complete
- Environmental Health (Food Team) – in progress
- Highway's implementation – in progress
- System version upgrade

As in previous years, several hundred boxes of archived files passed their destruction date during the year and these have been securely destroyed. This has freed up capacity in Modern Records which should remove the need for any further, temporary storage elsewhere in the building.

Newport City Council has centralised much of our systems administration as part of the corporate Newport Intelligence Hub. This has ensured that systems, and system information are managed in an effective and consistent way.

2.9. Freedom of Information and Subject Access Requests

As a public authority, the council also handles requests for information and data. There are risks associated with responding to Freedom of Information and Subject Access requests. With Freedom of Information requests, care should be taken not to include any personal information as part of responses, for instance when sending out spread sheets that might originally include personal data.

Freedom of Information
This is the eighth time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2021/22 was 953 which is a significant increase from last year (797). The impact of the Coronavirus pandemic from March 2020 probably accounts for this reduction in the number of requests last year. It is always difficult to understand the reasons behind variation in numbers as there are a number of factors that may impact on the figures, especially issues that are of particular local or national interest e.g. Brexit. These tend to generate a number of FOI requests and the number tends to reflect the level of public interest. Performance for 2021/22 was 89.5% of requests responded to within 20 working days. This was above the target of 88% of requests. The council has met its target for nine of the eleven years since a target was identified.
.
A breakdown per year is included below:

Year	Number of requests	Performance (Target)
2021/22	953	89.5% (88%)
2020/21	797	90.8% (88%)
2019/20	1100	90.2% (88%)
2018/19	1167	90.1% (88%)
2017/18	1037	88.3% (88%)
2016/17	1087	84.1% (88%)
2015/16	914	92.3% (87%)
2014/15	895	87.7% (87%)
2013/14	869	87.1% (87%)
2012/13	698	90.4% (87%)
2011/12	540	84.4% (87%)

The existing system for managing FOI requests is being extended on a quarterly basis with options being considered for future years.

Publishing data
Government and ICO guidance encourage the publication of data as good practice for public bodies and this is referenced in the ICO model publication scheme as part of our commitment to openness and transparency. The transparency page was developed to improve signposting of council data.

This page includes:

- Council spend over £500
- Councillor allowances and expenses
- Business rates data
- Public health funerals
- Council pay and grading including gender pay gap information
- Pupil numbers in Newport
- Newport Matters production costs
- Housing Information
- Contact Centre statistics

Subject Access Requests

Subject Access Requests (SAR's) are requests for personal information requested by the data subject and care needs to be given to ensure that personal information relating to other data subjects is removed. As a result of General Data Protection Regulation, fees have not been charged since April 2018. A new Data Protection Policy was developed, and this includes the rights of individuals under the Data Protection Act 2018. Specific guidance on processing Subject Access Requests is included in the policy and guidance to staff has been provided on the intranet and in staff bulletins. A personal information request form is used to identify specific subject areas for requests as well as gathering details of the requestor. It is crucial to gather proof of identity so personal data is not disclosed to a third party accidentally. The council narrowly missed its performance target for dealing with Subject Access Requests. 71% of requests were responded to within the deadline, against a target of 75%. Gaining access to paper records has been a greater challenge as a result of the Coronavirus pandemic and the subsequent move to remote working.

Year	Number of requests	Performance (Target)
2021/22	76	71% (75%)
2020/21	70	60% (75%)
2019/20	77	77.9% (75%)

3. Risk Management and Associated Action Plan

The sections above highlight the work required to address the obligations under General Data Protection Regulation (GDPR) and the associated Data Protection Act 2018. The number and complexity of services the council provides means this remains a very large task. **The majority of staff working from home as a result of the Coronavirus pandemic provides some specific challenges, especially with greater concerns over cyber attacks.**

Compliance and Audit
Maintaining compliance with the Public Services Network is always a challenge and this will be a priority especially in the short term, given that compliance has recently lapsed. The council has achieved PCI compliance for the first time in a number of years and this needs to be maintained with a likely change to the standard required for next year's assessment. The annual Welsh Cyber Stock Take is a useful process. The council has scored better again, remains above average across Wales and aims for continuous improvement. GDPR came into force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. Following on from Brexit, the EU GDPR no longer applies to the UK. For organisations operating inside the UK, the Data Protection Act 2018 (DPA 2018) is applicable. Priority areas are supporting the Welsh Track, Trace and Protect (TTP) programme, Data Protection Impact Assessments (DPIA's) and The Information We Hold.

Information Governance Culture and Organisation
At time of the report writing, the Information Management Service Level Agreement (SLA) has been extended for a further three years for all primary schools and now includes three high schools. Quarterly meetings of the Information Governance Group and Data Protection Group take place to oversee information risk management in conjunction with other stakeholders including Shared Resource Service

Communications and Awareness Raising
We continue to raise awareness with staff. Corporate staff training numbers have improved in part due to Microsoft Teams delivery method. Social Services training numbers have increased following Coronavirus pandemic challenges but more to be done. Large amount of training provided for schools as well as specific training provided for Track, Trace and Protect (TTP) staff. GDPR e-learning uptake has been excellent.

Information Risk Register
The Information Risk Register continues to be maintained on an on-going basis. One notable risk identified was a world-wide vulnerability in systems that use a Java based logger known as Apache Log4J that was reviewed/actioned by SRS.

Security incidents
During this year there was an increase in reported incidents, possibly as a result of increased awareness. Only one incident was referred to the Information Commissioner's Office (ICO) and the ICO took no action. Incidents are investigated and monitored with appropriate lessons learned and communicated.

Information Sharing
The Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's) to ensure appropriate and documented information sharing.

Business Continuity
There is an ever-increasing reliance on digital technology to support business activities and maximise the availability of systems that this is expected to be improved by the planned SRS data centre move and the move of systems to the cloud that took place. This will continue in 22/23 to improve business continuity. Business Impact Analysis was carried out in response to the Coronavirus pandemic and this highlighted the increasing importance of digital technology.

Technology Solutions
As planned last year, secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business. The existing remote access solution has been replaced with Microsoft Always ON VPN. Other security standards for e-mail system hygiene have also been implemented.

A Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) has been agreed and a solution has been procured with implementation by March 2023 to increase preventative security measures.

Records Management
The continued roll out of EDMS solution across council improves information security especially around paper records. The number of paper records held in Modern Records continues to reduce by disposing of records which have reached their retention period.

Freedom of Information
The council exceeded its target for the year but this always requires a large amount of effort .

Subject Access Requests
The Subject Access Request target was not met for the year but has increased from last year. There were still some difficulties in staff accessing Civic Centre paper records as a result of the Coronavirus pandemic and the expectation is that performance will increase in 22/23.

The council maintains a strong commitment to information governance as demonstrated by the organisation and activities detailed within this report.

3.1. Risk Management

Risk	Impact of Risk if it occurs* (H/M/L)	Probability of risk occurring (H/M/L)	What is the Council doing or what has it done to avoid the risk or reduce its effect	Who is responsible for dealing with the risk?
Risk of data breach and potential fine imposed by the Information Commissioner's Office or reputational damage	H	L	Staff awareness raising especially around GDPR Provision of data protection training Development of policy management/e-learning solution Intranet content and staff bulletins Development of new policies and update of existing ones On-going role of Data Protection group	Digital Services Manager (DSM) in conjunction with Information Management team
Council is unable to make best use of, and share the data it holds due to a lack of confidence in the integrity and security of the information.	H	L	Digital strategy sets the overall direction for the management of information and is being reviewed to ensure it meets future needs. Day to day operational guidance provided by Digital and Information service. The strategy is being reviewed and updated	Digital Services Manager (DSM) and Information Management team
PSN (Public Services Network) accreditation not gained	H	L	Resolve vulnerabilities identified as a priority. Evidence information governance arrangements as detailed in this document. Ongoing patch management and other activities to reduce risks. Continued engagement with Members Proactive vulnerability scans run by SRS	Digital Services Manager (DSM) in conjunction with in conjunction with SRS
Delivery of IT Service by Shared Resource Service (SRS) provides less control	M	M	Continue to develop relationship with the SRS Continue to develop complementary activities with SRS Governance team	Digital Services Manager (DSM) in conjunction with Head of PPT / SRS management
Do not meet requirements of EU General Data Protection Regulation	M	M	Staff Awareness raising especially senior management Standing agenda item at Information Governance Group	Digital Services Manager (DSM) in conjunction with Head of PPT / SRS management

PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	PCI compliance achieved in July 22 and will work to ensure continued compliance in future.	Digital Services Manager (DSM) in conjunction with in conjunction with SRS
Technical Solutions are not available to meet the needs of service delivery and data breach occurs	H	L	Microsoft Multi factor Authentication (MFA) solution for secure access to 365 e-mail. Microsoft Office Message Encryption and One Drive rolled out. Encrypted laptop devices Multi-Function Devices (printer/copier) has increased security features Data stored on servers and not on local devices unless encrypted Review solutions, identify and plug any gaps Maintain health check and compliance requirements Review the security of cloud based technical solutions including Data Protection Impact Assessments (DPIA's)	Digital Services Manager (DSM) in conjunction with Information Management team
Information is not shared appropriately and securely	H	L	Development of new Information Sharing Protocols and Data Disclosure Agreements and review of existing ones Advice and guidance	Digital Services Manager (DSM) in conjunction with Information Management team
Critical IT systems are not available to services	H	L	The SRS planned data centre move and NCC's plans to migrate systems to the cloud will improve availability and business continuity.	SRS in conjunction with Digital Services Manager and services
Information security is not considered for new projects	M	L	Data Protection Impact Assessments (DPIA's) carried out for new projects with further DPIA's required going forward. Use ICO process including screening	Digital Services Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Assess results of Annual IT health Check and develop plans to address vulnerabilities	Sep 22
Make submission for PSN prioritising this work in SRS/NCC	TBA
EU General Data Protection Regulation (GDPR) and Data Protection Act 2018	
Data Protection to be discussed as standard item at Information Governance Group and Data Protection Group	On-going
Review any new forms and associated privacy notices for the organisation. This will include the legal basis and consent where appropriate	On-going
Development of extended details of The Information We Hold	Dec 22
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
PCI accreditation	
Payment Card Industry Data Security Standard - prepare to ensure compliance with new PCI security standards prior to expiry of current compliance with external supplier to identify gaps and resolve these	Feb 23
Cyber Stock Take	
Review results of stock take 4 and develop action plan when results provided	Sep 22
Information Governance Culture and Organisation	
Contribute to information governance considerations across all SRS partners including Information Security Leadership Board	On-going
Quarterly meetings of the officer Information Governance Group to oversee information risk management in conjunction with other stakeholders including Shared Resource Services representation	On-going
Quarterly meetings of Data Protection Group to discuss operational data protection issues	On-going
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Members updated through Annual Information Risk Report, including review by Scrutiny Management Committee	Oct 22
Continue with action plan to take forward agreed Service Level Agreement with schools	On-going
Communications and Awareness Raising	
Regular data protection training sessions corporately and for Social Services including additional monthly courses to meet demand	On-going
Further policies and guidance will be developed to support the organisation	On-going
Review of information management policies	Mar 23
Provide advice and guidance to support primary schools in conjunction with Service Level Agreement	On-going
Develop and deliver training for members	Mar 23
Provide training for schools including high schools that join Service Level Agreement (SLA)	Dec 22
Develop action plan for roll out of Metacompliance solution	Sep 22
Information Risk Register	
Management of the information risk register	On-going
Information Security Incidents	
Investigation of security incidents and identification of issues to be followed up	On-going
Information Sharing	
Further Information Sharing Protocols will be developed to support collaborative working	On-going
Review existing Information Sharing Protocols	On-going
Develop additional Data Disclosure Agreements as required	On-going

Business Continuity	
SRS Data centre move for Newport to improve business continuity and reduce reliance on infrastructure at the Civic Centre	Mar 23
Migration of priority IT systems to the cloud to improve business continuity	On-going
Technology Solutions	
As a result of our partnership with the Shared Resource Service, the council will pursue options for collaboration and simplification wherever practical	On-going
Review technical solutions to ensure they meet information governance needs including cloud-based systems	On-going
Consider the need for new technical solutions to address weaknesses	On-going
Implement Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) with SRS and suppliers to improve preventative measures	Mar 23
Migration to AlwaysOn VPN solution for remote access	Apr 22
Extend use of Xerox Mail solution to improve mail distribution processes	On-going
Records Management	
Continued roll out of EDMS solution across council	On-going
Review options for Modern Records and storage including destruction of records past their destruction date	On-going
Freedom of Information and Subject Access Requests	
Freedom of Information	
Publication of further open data for suitable data sets	On-going
Subject Access Requests	
Work with services to improve performance on Subject Access Request responses	Mar 23

Mae'r dudalen hon yn wag yn