Report

Cabinet Member for Community and Resources

Part 1

Date: 9 September 2021

Subject **Annual Information Risk Report 2020-21**

Purpose To provide an assessment of the Council's information governance arrangements, identify key risks and agree the action plan for 21/22

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 ninth 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 2020-21 and proposed actions.**

Action by Digital Services Manager/Information Manager
Head of People and Business Change

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 and Business Change
- 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 date a number of much larger fines have been issued including a proposed fine of £183M to British Airways. This was reduced to £20M partly due to the impact of Covid-19 on the airline industry, however this fine represents the largest imposed to date for breach of GDPR.

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. 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 and Business Change service plan from 20/21.

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 2020-21 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.

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 increased slightly compared with last year but most were of a minor nature and the only serious breach that was referred to the ICO was in relation to the accidental disclosure of personal data held on the NWIS TTP database by Public Health Wales, which was closed by the ICO with no formal action being taken. The Council was also satisfied with the PHW response, as the joint data-controller for the TTP data. 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 and Business Change

As the report author, the comments of the Head of People and Business Change 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. There are a couple of areas where the results of testing or surveys were outstanding at the time of pulling the report together; this would need to be followed up during 2021/22 and incorporated in next year's annual report.

Comments of Cabinet Member

The report highlights increased information risks as a result of the Covid pandemic with the majority of staff working from home. The council's actions to address these risks demonstrates its on-going commitment to this work.

Local issues

No specific local issues.

Scrutiny Committees

This report was presented to Scrutiny Management Committee on 9th July 2021. Scrutiny comments are as below:-

- The Committee acknowledged that it was the first time the report came to Scrutiny so the format was more detailed than usual presentations. Members appreciated that the last two presentations were comprehensive.

- The Committee therefore requested that in future, the presentations could be more of a brief overview so they can open up questioning from the scrutiny committee sooner.

- The Committee also recommended for the officers to slim down the reports but were reminded by the Scrutiny Adviser that they have reduced the number of agenda items hence why there is an extra meeting date to ensure the meetings are shorter.

- Discussion ensued and the Committee requested that the reports could be more slimmed down and the executive summary could be detailed with the main points included to help with questioning.

Fairness and Equality Impact Assessment

This report is not requesting a decision and does not reflect a policy change which would impact on staff or communities. Therefore, a formal Fairness and Equality Impact Assessment (FEIA) is not required. However, fairness and equality are considered in service delivery, and FEIAs are completed where relevant.

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

The council is currently developing a new Digital Strategy which will drive our future work programme. This will be subject to a full Fairness and Equality Impact Assessment which will take in to account the needs of, and impact on, people that share Protected Characteristics under the Equality Act.

Socio-economic Duty

The council is currently developing a new Digital Strategy which will drive our future work programme. This will be subject to a full Fairness and Equality Impact Assessment which will take in to account the need to mitigate and improve inequalities of outcome that arise as a result of socio-economic disadvantage.

Welsh Language (Wales) Measure 2011

The requirements of the Welsh Language (Wales) Measure 2011 and associated Welsh language standards are considered as part of ongoing service delivery and will also be considered in line with 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 18/19
Annual Governance Statement 18/19
Corporate Risk Management Strategy and Register
Digital Strategy 2015-2020

Dated: 25 August 2021

Annual Information Risk Report 2020/21

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

Document Control

Version	Date	Author	Notes / changes
V0.1	23/03/2021	Tariq Slaoui	Initial draft based on previous report
V0.2	28/04/2021	Tariq Slaoui	Update
V0.3	27/05/2021	Tariq Slaoui	Update
V0.4	03/06/2021	Tariq Slaoui	Update
V0.5	28/06/2021	Mark Bleazard	Update
V0.6	30/06/2021	Tariq Slaoui	Update
V0.7	12/07/2021	Mark Bleazard	Further update to include Scrutiny comments
V0.8	16/08/2021	Mark Bleazard	Cabinet member comments and PSN update

Table of Contents

Contents

Executive Summary

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. **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.**

This is the ninth 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)** – two submissions unsuccessful. Escalated and prioritised by NCC/SRS. Update 13/8/21 Third submission successful and certificate received
- **General Data Protection Regulation (GDPR). Progress was made in a number of areas**
    - Particular emphasis on the development of privacy notices across the organisation.
    - A Data Protection Policy is in place to communicate the rights of individuals to staff, especially around Subject Access Requests
    - Data Protection Impact Assessment (DPIA) carried out for Countryside, HWRC and Housing staff bodycams
- **Payment Card Industry (PCI) standard**
    - Work is required for PCI as a priority and the Council has engaged with PCI consultants to develop a gap analysis
- **Cyber Stock Take**
    - Newport City Council scored well in Cyber Stocktake 2. Cyber Stocktake 3 has been submitted and we await the findings

Information Governance culture and organisation

- Service Level Agreement is in place with primary schools and we continue to support schools across Newport
- A staff survey on GDPR was carried out and results analysed
- Continue to develop and manage relationships with Shared Resource Service (SRS)
- Quarterly meetings of the Information Governance Group and Data Protection group to oversee information risk management in conjunction with other stakeholders including Shared Resource Service

Communications and Awareness Raising

- Continue to raise awareness with staff including monthly newsletter produced and issued to Primary schools across Newport as part of new SLA
- Specific schools training delivered
- GDPR e-learning uptake has been excellent
- Staff GDPR survey will inform how we communicate this year

Information Risk Register

- Continues to be maintained with contribution to Annual Governance Statement as necessary
- Cyber threat has been added as a specific risk on the corporate risk register

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 major incident reported to the ICO. Newport was not at fault but share responsibility as a Joint Data Controller.

Information Sharing

- Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)

Business Continuity

- The first phase of this project was achieved with replication of offsite backups from tape to disk
- Business continuity/disaster recovery plans will be reviewed with SRS and revised accordingly to align with planned data centre move and cloud migrations plans need to be reviewed with SRS

Technology Solutions

- Work commenced on the replacement of Egress facilities for secure e-mail and large/secure file transfer
- **We will consider the benefits of Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) proposed by SRS to partners**
- We plan to replace the existing remote access solution with Microsoft Always ON VPN
- Small number of Windows 7 devices remain as a result of laptop supply issues but these will be replaced by Sep 21

Records Management

- Continued roll out of EDMS solution across council, project manager in post continues to progress deployment.

Freedom of Information

- **Exceeded target for year**
- Decrease in number of requests from last year due to Covid-19.
- Continue to promote the use of open data sets and adding new ones where appropriate

Subject Access Requests

- Guidance to staff included in the Data Protection Policy and all SAR's recorded in FOI system now
- SAR target not met for year due to difficulties in accessing Civic Centre paper records as a result of the Covid-19 emergency 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. 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 and Business Change 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
  - The staff survey enables specific comparisons with previous years together with specific questions on the impact of the Coronavirus pandemic
- This is the ninth 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. To date a number of much larger fines have been issued including the highest fine of £20M to British Airways In cases where data breaches are referred to the ICO, its investigations highlight the importance of effective governance arrangements to reduce risks
  - 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 existing Digital Strategy highlights the importance of effective information management and data sharing with robust information security to protect business and citizen data from threats, loss or misuse. This will be at least as important as previously when the new Digital Strategy is created.

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

An annual IT Health Check was undertaken by a certified contractor in September 2020 and an initial submission to the Cabinet Office was made in March 2021. A Remediation Action Plan (RAP) was developed to mitigate and prioritise the high risks identified in the report This was submitted in March 2021 but was rejected by the Cabinet Office as a number of the vulnerabilities were still outstanding. A further submission was made in June 2021 which was also rejected. Despite good progress, a number of vulnerabilities remain. At the time of writing, this work has been escalated and prioritised within SRS to accelerate progress and resolve the outstanding vulnerabilities urgently. Update 13/8/21 Third submission successful and certificate received 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.

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is a regulation that strengthens and unifies data protection for individuals within the European Union (EU). GDPR came in to 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 3 years now and the UK has subsequently left the European Union as a result 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. Currently an interim agreement on the adequacy of UK data protection has been provided and it is anticipated that this will be formally agreed in the near future. 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 data from the EU without having to make any changes to their data protection practices.

GDPR 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 some of the changes are detailed below:

- The maximum fine is 20 Million Euros or 4% of turnover
- There is now a requirement to document the personal data held and keep a record of our processing activities.
- Data breach reporting is now 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 now 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 a number of lawful bases. Specific guidance relating to children and their rights
- Local authorities can no longer rely upon "legitimate interests" as a legal basis for processing data
- The removal of maximum fee for Subject Access Requests and reduction in days to process (from 40 calendar days down to 30)
- 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 fine to date is of £20 Million to British Airways.

A GDPR Task and Finish Group was established in 2017, with representation from each service area and schools. The group continues to meet on a quarterly basis and with the assistance of the group, the council has progressed in the following areas:

- Awareness raising – the Data Protection group has ensured that GDPR 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 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.
- Communicating Privacy Information – The council must demonstrate proactively to individuals, how we are processing their data and the lawful basis for doing so. A Corporate Privacy Notice has been developed and published to allow us to be more accountable and transparent about this. The Data Protection group has undertaken a forms audit to understand what types of personal data we are collecting from individuals and to establish a lawful basis for processing this data. All relevant privacy notices are published on the Councils website and all appropriate services are covered. However, we continue monitor new services and changes in services to ensure appropriate coverage.
- Consent – the rules around consent have been significantly strengthened under GDPR. A consent checklist has been drawn up to assist mangers/service areas who rely on consent as the lawful basis for processing personal data. It is important to recognise that consent is only one of six lawful bases under GDPR and consent should only be used where the other lawful basis have been ruled out. The Information Management team continue to provide advice and guidance to service areas in this respect.
- 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 2020/21, DPIA's were undertaken for the deployment of Body Worn Video Cameras (BWVC) at the Household Waste and Recycling Centre, The Mission Court Housing Scheme and the use of BWVC's for countryside officers. Also, in response to the Covid emergency 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.
- Incident Reporting – the Information Security Incident Reporting Policy is aligned with the requirements of GDPR and the key points have been communicated to the organisation. As

noted above, the maximum fine is now 20 Million Euros or 4% of turnover and there is a specific requirement to notify the ICO of significant breaches within 72 hours. In certain circumstances, there will be a requirement to notify data subjects of breaches of their data. In light of the Covid-19 emergency, staff have been advised to remain vigilant and to report any suspected incidents to the information management team in a timely manner. In 2020/21 66 reported incidents were investigated by the Information Management team, a full breakdown of these are in section 2.5 of this report.

- 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 currently prioritising work to expand this register and to include paper records. This work will also seek to identify cloud based provision of services and the governance arrangements around these.
- The rights of individuals – the rights of individuals and how to access them under GDPR are contained in the www.newport.gov.uk/privacynotice (see above). We have also published the Subject Access Request procedure and we continue to support the organisation and primary schools to meet these obligations.
- Data Processor/Joint Controller responsibilities – Data Processors (organisations who process personal data on our behalf/contractors) and joint controllers have further obligations under GDPR. Where possible, we continue to contact those organisations and communicate the changes to them. The procurement team have now updated all new contracts to reflect the clauses. Standard Controller/Processor and Controller/Controller clauses have been developed for inclusion in all contracts of this nature.
- Staff Training – Information Security Training is available to the organisation and to the primary schools. The pandemic has meant that face to face training has been switched to training via MS Teams. The GDPR e-learning module continues to be well attended and complements traditional learning methods. The team continue to reach out to departments and service areas who are unable to attend corporate training. Recent training has been delivered to all primary schools in Newport as part of our Service Level Agreement.
- Data Protection Policy – a Corporate Data Protection Policy is in place to provide guidance to staff on processes and procedures. This has been published and communicated to the organisation.
- Significant Information Governance work has been undertaken to support the Welsh Track, Trace and Protect (TTP) programme during 2020/21. A joint controllership agreement was established with all local authorities and Health Boards in Wales and an Information Sharing Protocol was developed to allow the sharing of data between organisations during the pandemic.

Payment Card Industry Data Security Standards (PCI-DSS)

The council was previously compliant with Payment Security Industry (PCI) Data Security Standards. A previous audit identified issues to be addressed. Accordingly, the council's PCI compliance has lapsed. To ensure these issues are formally resolved to meet PCI requirements, the council procured assistance from an external organisation. Staff from the council and SRS are working with this company to undertake a gap analysis and subsequent remediation action plan to address any shortfalls. Work to date has been very beneficial and positive but there has been a slight delay to this project due to unexpected resource issues in the company. The project has commenced again and should be completed by October 21.

Cyber Stock Take

Newport City Council, along with all other local authorities in Wales, took part in the third 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 we await the results of the benchmarking exercise.

The results of the stock take will require further evaluation and an associated action plan may be required.

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. During this period Audit Wales issued a report on cyber resilience across the public sector in Wales. This report was based on self-assessments of each organisation's preparedness on cyber resilience and was designed to identify potential themes and any concerns. Due to the sensitivity of the themes in the Audit Wales report and its requirement to discuss these appropriately, the report and the council's response was discussed excluding the public by a "part two" item at the Governance and Audit Committee in May 2021. The council's stance is certainly not complacent but it has robust and mature governance arrangements and implemented a specific solution designed to reduce the impact of ransomware.

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. A revised survey has been designed incorporating some previous and some new questions. The Coronavirus position delayed our plans for a staff survey in 2019/20, however a survey was carried out in 2020/21 a summary of which is included below.

GDPR Staff Survey 2020/21

254 responses were received over a period of 3 weeks (26th April – 14th May). This represents the biggest response to such a survey over numbers that responded in previous reports. A headline summary of the results is below.

64% of staff said that they were aware of the Councils Information Management training offering but only 45% said that they have attended. This may be due to the relatively large number of responses compared with previous surveys and increased e-learning take up.

62.9% of staff responded by saying that they felt they had received enough training.

When asked about the preferred training delivery method, we received the following responses. Please note that respondents could vote for multiple answers.

Training Method	**Number of responses**
e-Learning	171
Virtual classroom training (MS Teams)	146
Videos	48
Classroom training	53
Workshop style training	33
Other	0

e-Learning and virtual classroom training was significantly preferred to the more traditional methods of learning.

93% of staff understand their role in relation to information security, a small percentage were unsure.

85% understood the changes and implications of GDPR and 74% know the correct procedure in the event of an incident.

67% of staff agreed that information security practises are regularly communicated. 11.5% did not agree while the remainder were unsure.

65% know who to contact if they received a request for personal information, 35% of staff did not know.

69% of staff agreed that levels of information security are consistently high while 25% were unsure.

45% of staff disagreed that home working had a negative effect on data protection working practises and 35% were unsure.

62% of staff feel that more advice and guidance is required on home working and data protection, 23% were unsure.

Organisation

Senior Information Risk Owner (SIRO) role
The council's Senior Information Risk Owner (SIRO) role is part of the Head of Law and Regulation 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 and Business Change. 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 – Place. 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
As detailed in last year's report, councillors are exempt from data protection registration following Information Commissioner's Office (ICO) guidance from 1 April 2019. *The Data Protection (Charges and Information) (Amendment) Regulations 2019 exempted the processing of personal data for:*

- *Members of the House of Lords*
- *Elected representatives*
- *Prospective representatives – someone seeking to become an 'elected representative'*

'Elected representatives' is defined by the Data Protection Act 2018 and includes, but is not limited to, MPs, MSPs, AMs in Wales, MEPs, elected councillors in county councils, district councils, London boroughs, parish councils, elected mayors and police and crime commissioners. 'Prospective representative' refers to anyone seeking to become an elected representative as defined above.

As a result of this change in guidance, Newport City Council councillors are no longer registered individually as data controllers under the Data Protection Act.

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 future improvements. This has been beneficial in shaping the necessary actions.

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).

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 two 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.

2.3. 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. Awareness for employees is vitally important and this is generally achieved via staff training together with other forms of communication to improve awareness.

Corporate Phishing Exercise

The Welsh Government secured funding for all local authorities in Wales to undertake a simulated Phishing exercise in conjunction with a provider. Human error is the most common cause of data breaches in cyber security and the accidental clicking of malicious links or divulging of personal information to unauthorised recipients is one of the largest risks to an organisation. The proposed exercise will simulate such an attack on the organisation and present a series of phishing emails to randomly selected (or targeted as appropriate) members of staff. If any staff click those links, they will be asked to complete some online e-Learning to warn them of the risks of responding to malicious email. This is intended to be a staff awareness raising exercise and will help us understand how much of a risk this is to the organisation.

Staff Guidance

Regular reminders of good practice have been provided in the staff bulletin and on the intranet on various important subjects especially as a result of home working during the Coronavirus pandemic

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 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.

- Social Services courses
- Corporate courses
- Councillor courses
- Schools courses
- Other courses and presentations
- Information Management team training
- E-learning

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).

Training for primary schools, delayed by the Coronavirus pandemic was carried out in early 2021 which is a positive step.

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. No courses were scheduled during this period due to certain staff in particular roles accessing Teams based training. Some staff have attended the corporate training course. These issues were escalated with Social Services and will be followed up on.

A breakdown per year is included below.

Year	Number of staff who attended
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. Due to the Coronavirus pandemic there were less courses run than normal. 9 courses were run virtually using Microsoft Teams and these were well attended. The number of staff that attended the corporate course was 74 compared with 98 in 2019/20. Whilst attendance does vary a little year on year the number of staff attending remains consistent.

Year	Number of staff who attended
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

Previous training courses 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. It is anticipated that further training sessions will follow the local government elections that take place in May 2022.

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. **Training commenced in 2021 with Lliswerry, Bassaleg, Eveswell and Somerton clusters with a total of 78 staff trained.** The remaining clusters to be scheduled appropriately.

Year	Number of staff who attended
2020/21	78

Other Courses and Presentations

In September 2020, 15 CYPS staff were trained to use Egress secure email.

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. The one remaining team member undertook this training in March 2020 and, following a delay, was successful with the exam and is now qualified with the BCS Certificate in Data Protection.

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. This e-learning was developed last year. The new GDPR e-learning module provides guidance to staff on their obligations under the Data Protection Act 2018**. In 2020/21 887 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, 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.

Data Protection Policy
This policy provides advice and guidance to staff in all aspects of data protection including guidance on the rights of individuals and specifically around Subject Access Requests (SAR's).

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:

- Biometrics Guidance for Schools

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.

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.

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
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:

In August 2020, Public Heath Wales (PHW) accidentally published the personal data of 18,105 Welsh residents who had tested positive for Covid-19, to a public facing website. The information only consisted of initials, date of birth, geographical area and sex. In the 20 hours it was online, it had been viewed 56 times. The number of Newport residents affected was 910. The ICO were informed and following on from an investigation by NWIS, they decided to take no further action, although the NWIS investigation findings did include a remediation plan. While Newport City Council was not a fault, we are a joint Data Controller for the Test, Trace & Protect programme in Wales and as such, are jointly liable for data breach incidents such as this.

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. 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 2020/21:

Information Sharing Protocols (ISP's)

An ISP for Newport's Youth Engagement and Progression Framework (YEPF) Not in Education, Employment or Training (NEET) Partnership has been developed and quality assured. An ISP to support the sharing of information for the Newport SPACE (Single Point of Access for Children's Emotional Wellbeing) Programme was developed and assured in March 2021.

A Covid-19 Joint Controller Agreement was established between Local Authorities, Health Boards and organisations who need to share personal data in order to deliver a coherent and collaborative Test, Trace & Protect service in response to the Covid-19 outbreak in Wales.

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 2020/21:

- Care Inspectorate Wales Assurance Check for NCC Social Services
- Baby and me Barnardo's programme
- Council Tax data acquisition – Office for National Statistics
- Body Worn Cameras for Temporary Accommodation
- DDA Careers Wales
- Overt fly tipping camera's
- COVID – 19, £500 care workers payments
- COVID – 19, Start-Up grant fraud checking
- COVID – 19, Release of extremely vulnerable (Shielded) patient data
- COVID – 19, Testing of key workers

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.

As a result of previous guidance from Audit Wales, the council is part way through a new hardware was set up with the migration of backups of key systems from tape to disk. Previous plans to provide access to systems should both server rooms at the Civic Centre not be available are being reviewed in light of the improved resilience from a move to the new SRS data centre and the existing and planned migration of systems to the cloud.

A quicker and more proactive move of systems to the cloud will take place in 21/22 that is designed to provide greater availability and better business continuity/disaster recovery.

A number of staff took part in a simulated cyber exercise set up by the Local Resilience Forum and included a variety of stakeholders This was very useful to all concerned.

2.8. Technology Solutions

A number of 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 continues to increase the percentage of laptops as part of its total number of computers used to encourage more flexible and agile working with access to information and records from a variety of locations. This has been invaluable during the Coronavirus pandemic with the vast majority of staff working from home. Laptops are now estimated to represent about 95% of all devices. As detailed last year, the intention is that desktop devices will only be issued if there is a technical reason why a laptop can't be deployed. The council expected to complete the deployment of Windows 10 to all its devices but this was not possible due to major delays receiving deliveries of laptops. This means a small number of Windows 7 devices exist and extended support was purchased for these devices. These devices will be replaced. A number of Windows 10 updates will also be required for a large number of devices

Microsoft Office 365 including Teams
The council previously migrated its e-mail solution to Microsoft Office 365. This currently means the use of Office 2016 and e-mail within 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 was implemented to protect 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.

In March 2020 Microsoft Teams was rolled out. Teams provides instant messaging/chat facilities as well as video/audio conferencing facilities. These facilities have been used extensively since and enabled 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 Office 365 client will be rolled out to all Windows devices that will automatically updated as a result. As below, the plan is to migrate to Microsoft AlwaysOn VPN for remote access.

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. Given that paper documents have not been provided as a result of the Coronavirus pandemic, this is planned to continue with associated costs savings, environmental benefits, information security improvements and administrative efficiencies .

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 Microsoft Teams roll out and will be involved in 21/22 in the roll out of updated versions of Office 365 and associated features in 21/22.

Mobility solution
The use of a mobility solution is available to all staff who need to work from home following improvements in response to the Coronavirus pandemic in March 2019. 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. The solution uses Microsoft Multi Factor Authentication (MFA) as used for Office 365 access. The plan is to migrate to Microsoft AlwaysOn VPN that will be even easier to use and will be rolled out in 21/22.

Multi-Function Devices
‘Follow Me’ print is available to all users, who are able to access Council printers from any location. A new Multi-Function Device (printer/copier/scanner) contract was rolled out in October 2017 with increased security features together with enhanced scanning facilities to drive the move to digital. Due to the impact of the Coronavirus 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.

Secure/Large File transfer solution
Egress Switch is rolled out to all users. This enables the secure transfer of e-mails and associated documents to organisations and individuals without secure e-mail facilities. The solution provides the ability to restrict access to specific documents and audit access to the information provided. It also allows large files to be safely shared via email. In line with the implementation of Egress Switch generally, the council will remove personal network storage for staff wherever possible. The plan is to replace Egress functionality with that provided within Office 365 solutions including Office Message Encryption. It is expected that the roll out of these solutions will take place from June 2021.

Xerox Mail "hybrid mail"
Further 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 in to envelopes automatically in the folder/inserter machine. The system's use continues to increase including recently Planning consultation letters that has saved time and money and streamlined the consultation letter process.

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 are now planned for 21/22 due to the impact of Coronavirus.

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 also now available as part of the 'Digital Newport' work in the city centre (Newport City Connect), over 50 public buildings and on public transport (Newport Community Cloud). Friendly Wi-Fi accreditation has been achieved for this set up. Gov Wi-Fi is available in various public buildings too. A budget saving proposal for 20/21 meant that this provision was being reviewed in efforts to save money but this review was deferred due to the impact of the Coronavirus and the impact of any removal of any public Wi-Fi services at any sites. This will be reviewed in 21/22 accordingly.

Physical Security
Major buildings (Civic Centre and Information Station) 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. The existing mobile phone contract continues due to the impact of Coronavirus and will be reviewed in 21/22 to ensure it is fit for purpose and offers value for money.

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.

2.9. Records 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. Documents are scanned on receipt into the mail room and made available to services in the EDMS system.

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.

Since the start of the Coronavirus Pandemic, a number of departments across the council have expressed an interest in using the EDMS solution, due to the many benefits it brings including the ability to support agile working. Despite challenges faced due to the Coronavirus Pandemic, 20/21 was a successful year for new implementations across the Council. Gwent Music Service, Communities for Work, and Private Sector Housing were implemented and are now live. In addition to this, over the past year two system upgrades have been achieved. One of which being a major upgrade, which involved training over 300 staff remotely and providing guidance to over 1000 users.

Looking ahead to 2021/22, Street Naming & Numbering, Flying Start, Strategic Housing, and Public Protection are in progress and expected to be delivered in the coming months. A new module called Email Connect is also expected to be deployed across file systems. This new module will create further efficiencies for departments, which aims to cut down document processing times.

Several hundred boxes of archived files passed their destruction date during the year. The majority of these have been securely destroyed with some further work required. This has freed up capacity in Modern Records. It is hoped that this will remove the need for any further, temporary storage elsewhere in the building.

2.10. 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 seventh time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2020/21 was 797 which is a significant decrease from last year of 303 requests or 27.5%. The impact of the Coronavirus from March 2020 probably accounts for this reduction in the number of requests but this also made the target more challenging with its impact on the council's operation especially in the early months. 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 2020/21 was 90.8% of requests responded to within 20 working days. This was above the target of 88% of requests. The council has met its target for eight of the ten years since a target was identified.
.
A breakdown per year is included below:

Year	Number of requests	Performance (Target)
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 including use of the new CRM system.

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

This data is free to re-use under the terms of the Open Government Licence.

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 missed its performance target for dealing with Subject Access Requests meetings the deadline for 60% of requests against a target of 75%. Gaining access to paper records has been a greater challenge as a result of the Coronavirus pandemic. This especially impacted on one area of the council which brought down the overall council performance. This has been addressed by the area concerned that should result in improved performance there with a positive effect on overall council performance.

Year	Number of requests	Performance (Target)
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.**

GDPR means that organisations need to be clearer and more transparent about how they process data. Organisations need to get a better understanding of what data they hold and the legal basis for the processing. Citizens are also provided with enhanced rights previously detailed in a new Data Protection Policy which provides guidance to staff and special emphasis on processes for Subject Access Requests. Information risks change regularly and these are managed by the Information Management team by an information risk register and other processes. The increase in the level of fines highlights the increased importance of the obligations under the Data Protection Act 2018 despite the UK's exit from the EU (Brexit). The theoretical maximum fine is now 20 Million Euros or 4% of turnover with the maximum to date being a £20M fine to British Airways that was greatly reduced from the original proposed fine.

Maintaining compliance with Public Services Network has been more of a challenge this year, mainly due to the timing in the cycles of Microsoft de-supported systems and issues with specific systems. This work is now dependent on the SRS to resolve on behalf of the council in conjunction with the Information Management team. Good progress has been made with Payment Card Industry data security standards and this is expected to be completed in summer 21. Audit Wales (formerly Wales Audit Office) continue to provide an independent review of practice.

Only one incident was referred to the Information Commissioner's Office (ICO) and this was due to the joint data controller status of the council and was not caused by the council directly. Incidents continue to be investigated when they arise to respond to the incident effectively and learn lessons to minimise the likelihood of re-occurrence.

The Information Governance Group continues its important work of monitoring risk across services and providing strategic direction with representation form the Shared Resource Service (SRS) and this will require a different method of operation. This group is complemented by the Data Protection Group that operates at a more operational and tactical level. The SRS client side role continues to develop and this is recognised as a crucial area to meet the digital needs of the council as an SRS partner organisation. The aim is for improvements in information security across all partners by a simplified and standardised infrastructure where possible and there has been progress with this including standardised laptops, the roll out of Microsoft Office 365 including Office Message Encryption and OneDrive. As part of a more proactive move to the cloud, all proposed services will be reviewed to ensure they meet data protection requirements.

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 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. 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	Undertake IT Health Check and resolve any vulnerabilities identified. Evidence information governance arrangements as detailed in this document. Ongoing patch management and other activities to reduce risks. Continued engagement with Members	Digital Services Manager (DSM) 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 Develop client side role to provide strategic input and performance monitoring Continue to develop complementary activities with SRS Governance team	Digital Services Manager (DSM) in conjunction with Head of PBC / SRS management
Do not meet requirements of EU General Data Protection Regulation	M	M	Staff Awareness raising especially senior management GDPR tracker being managed and shared with Data Protection Group Standing agenda item at Information Governance Group	Digital Services Manager (DSM) in conjunction with Head of PBC / SRS management

PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	Working with external supplier to identify gaps in compliance with a view to bridging this gap to achieve compliance	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 office 365 e-mail. Microsoft Office Message Encryption and One Drive to be rolled out to replace Egress system functionality 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	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	Phase 1 of disaster recovery solution completed by SRS. Review requirements for phase 2 as a result of SRS planned data centre move and NCC's plans to migrate systems to the cloud. Develop solutions to ensure business continuity as a result of Coronavirus	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. Use ICO process including screening	Digital Services Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Follow up on remediation action plans and make re-submission for PSN prioritising this work in SRS/NCC Update 13/8/21 Third submission successful and certificate received	Jul 21
Carry out annual IT Health Check - timing depends on existing PSN submission	TBA
EU General Data Protection Regulation (GDPR) and DPA 2018	
GDPR 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
Information Asset Register to be reviewed, updated and extended as necessary	Dec 21
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
PCI accreditation	
Payment Card Industry Data Security Standard work with external supplier to identify gaps and resolve these	Oct 21
Cyber Stock Take	
Review results of stock take 3 and develop action plan when results provided	TBA
Information Governance Culture and Organisation	
Further review and associated actions as a result of staff GDPR survey	Sep 21
Continue to develop and manage relationships with Shared Resource Service (SRS)	On-going
Contribute to information governance considerations across all SRS partners	On-going
Quarterly meetings of the 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 Committee	Jul 21
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
Work with Social Services to schedule suitable training course schedule	July 21
Further policies and guidance will be developed to support the organisation	On-going
Complete review of Information and IT Security policy to be reviewed in reference to Data Protection Policy	Dec 21
Existing policies and guidance will be reviewed and updated to ensure they are appropriate	On-going
Provide advice and guidance to support primary schools in conjunction with Service Level Agreement	On-going
Complete primary school data protection training	Jul 21
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	
Review business continuity/disaster recovery plans with SRS and revise accordingly to align with planned data centre move and cloud migrations	Oct 21
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
Consider the benefits of Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) proposed by SRS to partners	Jul 21
Replacement of Egress functionality using Microsoft Office Message Encryption and OneDrive	Jun 21
Migration to AlwaysOn VPN solution for remote access	Oct 21
Complete migration of all devices to Windows 10	Sep 21
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	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 to service areas to improve performance on Subject Access Request response given challenges as a result of Coronavirus pandemic	Sep 21