

Report

Cabinet Member for Community & Resources

Part 1

Date: 30 December 2020

Subject Annual Information Risk Report 2019-20

Purpose To provide an assessment of the Council's information governance arrangements, identify key risks and agree the action plan for 20/21

Author Digital Services 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 eighth 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 2019-20 and proposed actions.

Action by Digital Services 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 £183 Million to British Airways

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.	L	H	Digital strategy sets the overall direction for the management of information. Day to day operational guidance provided by Digital and Information service. The strategy needs to be 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 2019/20 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

Endorsement of the Annual Information Risk Report 2019-20 and proposed actions will have no adverse budgetary impact as the action plan will be delivered using existing budgets and staff. Whilst approving the report itself has no financial impact it is worth noting the potential financial penalties resulting from data breaches and the importance of the governance arrangements in place and action plan.

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, including further development of privacy notices, the development of a data protection policy and the carrying out of various data protection impact assessments. Confirmation of PSN compliance was received in February 2020. The number of reported security incidents has increased compared with last year but only one was referred to the ICO and the Council assisted with another incident reported by a high school, both of which were closed with no formal action being taken against the Council or the school. 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

There are no direct staffing implications arising from this report although it notes that staff awareness of information security is vitally important and is generally achieved through training supported by other forms of communication. This is particularly important as we operate within the current restrictions as a result of COVID 19. We have more staff working remotely than ever before and our arrangements to secure our data and information are more critical than ever to support our staff to operate effectively and safely.

The Well-being of Future Generations (Wales) Act requires that the Council ensures it has robust risk management processes in place including information risk management. 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.

Comments of the Chief Internal Auditor

Having sound information governance arrangements in place strengthens the overall corporate governance arrangements in place for the Council. This report clearly demonstrates the Council has appropriate and effective arrangements in place for information governance and deals with further improvements in a transparent way through its action plan.

Comments of Cabinet Member

N/A

Local issues

No specific local issues.

Scrutiny Committees

Due to coronavirus and a large work programme it has not been possible for Scrutiny Management Committee to review this report this year. Comments are invited from members in line with the normal member consultation process. This report is non statutory and needs to be considered in this context.

Equalities Impact Assessment and the Equalities Act 2010

The Equality Act 2010 contains a Public Sector Equality Duty which came into force on 06 April 2011. The Act identifies a number of 'protected characteristics', namely age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; sexual orientation; marriage and civil partnership. The new single duty aims to integrate consideration of equality and good relations into the regular business of public authorities. Compliance with the duty is a legal obligation and is intended to result in better informed decision-making and policy development and services that are more effective for users. In exercising its functions, the Council must have due regard to the need to: eliminate unlawful discrimination, harassment, victimisation and other conduct that is prohibited by the Act; advance equality of opportunity between persons who share a protected characteristic and those who do not; and foster good relations between persons who share a protected characteristic and those who do not. The Act is not overly prescriptive about the approach a public authority should take to ensure due regard, although it does set out that due regard to advancing equality involves: removing or minimising disadvantages suffered by people due to their protected characteristics; taking steps to meet the needs of people from protected groups where these differ from the need of other people; and encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Children and Families (Wales) Measure

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

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

Crime and Disorder Act 1998

No specific considerations.

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: 13th November 2020

Annual Information Risk Report 2019/20

Created by	Information Governance
Date	13/11/20
Reviewed by	Tariq Slaoui
Date	13/11/20

Document Control

Version	Date	Author	Notes / changes
V0.1	05/08/2019	Tariq Slaoui	Initial draft based on previous report
V0.2	21/08/2019	Tariq Slaoui	Updates
V0.3	25/11/2019	Tariq Slaoui	Updates
V0.4	03/12/2019	Tariq Slaoui	Updates
V0.5	29/01/2020	Tariq Slaoui	Updates
V0.6	27/04/2020	Tariq Slaoui	Updates
V0.7	04/05/2020	Tariq Slaoui	Updated
V0.8	05/05/2020	Mark Bleazard	Updated draft for review by Information Governance Group
V0.9	27/05/2020	Mark Bleazard	Informal draft for Cabinet Member with Cyber Stock Take added
V1.0	13/11/2020	Mark Bleazard	Changes to reflect lack of Scrutiny time to review

Table of Contents

Contents

Executive Summary	1
Background and Purpose.....	3
1.1. <i>Purpose of the Report and Benefits</i>	<i>3</i>
1. Current Position	3
1.1. <i>Compliance and Audit.....</i>	<i>3</i>
Public Services Network (PSN) compliance	4
General Data Protection Regulation (GDPR)	4
Payment Card Industry Data Security Standards (PCI-DSS)	6
Cyber Essential Plus	6
Cyber Stock Take	6
Audit Wales	6
1.2. <i>Information Governance Culture and Organisation.....</i>	<i>7</i>
Information Governance Culture	7
Organisation	7
2.3. <i>Communications and Awareness Raising</i>	<i>9</i>
Staff Guidance	9
Training Courses	9
Information Policy Development	11
2.4. <i>Information Risk Register.....</i>	<i>12</i>
2.5. <i>Information Security Incidents.....</i>	<i>12</i>
2.6. <i>Information Sharing.....</i>	<i>13</i>
2.7. <i>Business Continuity.....</i>	<i>14</i>
2.8. <i>Technology Solutions</i>	<i>14</i>
2.9. <i>Records Management.....</i>	<i>17</i>
2.10. <i>Freedom of Information and Subject Access Requests</i>	<i>17</i>
2. Risk Management and Associated Action Plan	19
2.1. <i>Risk Management.....</i>	<i>19</i>
3.2. <i>Action Plan.....</i>	<i>22</i>

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**.

This is the eighth 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) accreditation achieved in February 2020 lasts until February 2021**
 - **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 was developed to communicate the rights of individuals to staff, especially around Subject Access Requests
 - Data Protection Impact Assessment (DPIA) carried out for Customer Relationship Management (CRM) system and the Civil Parking Enforcement project.
 - Payment Card Industry (PCI) standard
 - Work is required for PCI as a priority now PSN accreditation achieved
 - Cyber Stock Take
 - Newport City Council scored well but action plan required to make improvements
- Information Governance culture and organisation
 - **Service Level Agreement now in place with primary schools and developing on-going action plan to support**
 - **As a result of a change in guidance, Newport City Council councillors are no longer required to be registered individually as data controllers under the Data Protection Act**
 - 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
 - GDPR e-learning module produced
- Information Risk Register
 - Continues to be maintained with contribution to Annual Governance Statement as necessary
- Security incidents
 - An increase in reported incidents, possibly as a result of increased awareness around issues as a result of GDPR
 - One incident was reported to the ICO and we assisted a high school in the reporting of another. Both instances were closed with the ICO requiring no further action.
- Information Sharing
 - Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)

- Business Continuity
 - Review disaster recovery/business continuity improvements following previous WAO review as a result of SRS cloud strategy and the number of key systems that have already been moved to the cloud
- Technology Solutions
 - **Office 365 deployed across the organisation for e-mail in cloud including Microsoft Multi Factor Authentication (MFA) and Advanced Threat Protection (ATP)**
 - **Deployed Microsoft Teams instant messaging/video conferencing solution to the organisation in March 2020**
 - Increased the percentage of laptops across the organisation which has been invaluable with Coronavirus and people working from home in large numbers
 - Nearly all devices now running Windows 10 with extended support for small number of Windows 7 devices
- Records Management
 - Continued roll out of EDMS solution across council, project manager now in post to progress deployment.
- Freedom of Information
 - **Exceeded target for year**
 - Slight decrease in number of requests from last year
 - Continue to promote the use of open data sets and adding new ones where appropriate
- Subject Access Requests
 - Guidance to staff included in new Data Protection Policy and all SAR's recorded in FOI system now
 - New SAR target exceeded for year

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 now defined in EU General Data Protection Regulation (GDPR) and the associated UK Data Protection Act 2018 that places a greater responsibility on the council. The council must continue to 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. GDPR requires organisations to be more clear and transparent about what data is processed and how to give citizens confidence that their data is being handled appropriately. The principle of using and securing data is outlined in the [Digital Strategy](#). 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 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 eighth 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 a proposed fine of £183 Million 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

1. 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. In 2015 the [Digital Strategy](#) was developed which 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.

1.1. 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 the 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 July 2019 and an initial submission to the Cabinet Office was made in November 2019. A Remediation Action Plan (RAP) was developed to mitigate and prioritise the high and medium risks identified in the report and on the 28th February 2020 we received confirmation of our compliance for a further year (expires 28th February 2021). The Shared Resource Service (SRS) now procures and schedules health checks for partners together which simplifies and streamlines the process. The number and variety of risks mean that work is required throughout the year to protect the council's data and systems. Risks around cyber security remain a specific concern such that they have been 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 by which the European Parliament, the European Council and the European Commission 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. As well as greater responsibilities on data controllers, the theme is to be more open and transparent to citizens in terms of how their data is processed. The UK's exit from the European Union (Brexit) will not have any real impact on the need to comply with the regulation as it is embedded in the Data Protection Act 2018..

There are major implications as a result of GDPR and this is a standard agenda item for the Information Governance Group. A GDPR Task and Finish Group has now changed to a Data Protection Group in recognition that data protection is an on-going activity not a one off task.

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

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 proposed fine is of £183 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 Information Management team has attended service area management meetings across the organisation, to provide specialist input. An intranet presence has been set up and content uploaded. E-bulletins have been issued to provide corporate updates. Specifically, a communications campaign has been undertaken to ensure that staff are aware of the process to follow for Subject Access requests (SAR's). 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 – under GDPR, the council needs to demonstrate proactively to individuals, how we are processing their data. 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. This forms audit has now been completed and the relevant privacy notices published. 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 managers/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 now mandatory for new technology implementations and projects that involve the systematic monitoring of individuals and/or the large scale processing of special category data. DPIA's were undertaken for the Customer Relationship Management (CRM) implementation and the Civil Parking Enforcement systems/procedure.. 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. Staff have been advised to report any suspected incidents to the information management team in a timely manner.
- 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 Data Protection Group is currently working to expand this register to other areas of the authority, and to include paper records.
- The rights of individuals – the rights of individuals and how to access them under GDPR have been reflected in the [privacy notices published](#) (see above). We have published our new Subject Access Request procedure, to align us with the requirements of GDPR. The discretionary £10 fee has been removed and we have formally reduced the amount of time that we have to process a request, from 40 calendar days, down to 1 month. The new process has been extensively communicated to the organisation.
- 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 have contacted those organisations and communicated the changes to them. The procurement team have now updated all new contracts to reflect the new GDPR clauses. Standard Controller/Processor and Controller/Controller clauses have been developed for inclusion in future contracts.

- Staff Training – Information Security Training has been updated to cover all aspects of GDPR. The information management team have developed a GDPR e-learning module to facilitate desktop learning. The team continue to reach out to departments and service areas who are unable to attend corporate training. Recent training has been delivered to Customer Services, GEMS and Gwent Music.
- Data Protection Policy – a Corporate Data Protection Policy was developed and agreed following all member consultation. This has been published and communicated to the organisation.

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. Recently, PSN compliance (see above) has been prioritised over PCI compliance. Now PSN compliance has been achieved there will be a focus with SRS on addressing the issues and consideration of a formal submission for PCI compliance.

Cyber Essential Plus

Welsh Government has provided funding for 2 years to facilitate local authority accreditation to Cyber Essentials Plus. The Cyber Essentials Plus project is a project by the Welsh Local Government Association (WGLA) to ensure that all 22 local authorities and the 3 fire & rescue services in Wales are certified to Cyber Essentials Plus (as well as IASME certification). Newport City Council has commenced work on this in conjunction with the SRS and a submission was made in December 2019. The organisation managing our submission, went into administration towards the end of 2019, and as such, our submission has not been reviewed. We wait for further information and options going forward from the WLGA.

Cyber Stock Take

Newport City Council, along with all other local authorities in Wales, took part in a Cyber Stock Take designed to give an indication of each local authority's maturity in cyber security. This was compiled by means of a self-assessment questionnaire. An extract from the report is below:-

Overall, your organisation scored well across all the sections of the Stocktake 2 compared to your peers. With 4/5 sections scoring GREEN. Your weakest section, similar to your peers, is the implementation of a successful Cyber Security Training & Awareness Raising.

The results of the stock take were only released in April 2020 so further evaluation and an associated action plan is 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.

1.2. Information Governance Culture and Organisation

On 1st April 2017, the council formally became a partner of the Shared Resource Service (SRS) as detailed further below. 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. It is intended to carry out a survey at a suitable time

Organisation

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 Role

As detailed last year, under General Data Protection Regulation (see section above) the council needs to specify its Data Protection Officer. This role is incorporated within the duties of the existing Digital Services Manager post.

Shared Resource Service (SRS) - The IT Service became a partner in the Shared Resource Service (SRS) on 1/4/17. 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

All councillors were registered as data controllers under the Data Protection Act in 2018/19. 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.

If any member is only processing personal data in connection with their functions as members of House of Lords, elected representatives, or in connection with any activity where the sole or principle purpose is their future election then they will not need to pay the data protection fee. If however, any member also processes personal data for any other non-exempt purpose, for example a business owner that processes personal data or if the use of CCTV for business/crime prevention purposes in connection with that business, then as that processing is not exempt they must pay the data protection fee.

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.

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 will be part of the work of the Data Protection group.

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.

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.

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 was agreed and signed off. This SLA provides additional funding to enable the provision of a service to primary schools similar to that being provided corporately. The post was filled and the service is now operation and complements the service provided corporately. A number of actions are being pursued to improve understanding and awareness in primary 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. Awareness for employees is vitally important and 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 including GDPR.

An information security leaflet is provided to all staff attending training which was revised to reflect the new Data Protection Act 2018. The team regularly assess information from the Information Commissioner's Office (ICO) 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 complements e-learning required to be completed by new starters. The content had minor updates to reflect events and keep it relevant. A major revision of the training content was undertaken to reflect GDPR (see further details within this report). The courses run are:

- 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. Training is a key area as people are generally considered the weakest link in relation to information security. 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) as highlighted in the 'Security Incidents' section below.

In early 2020 the Information Management team scheduled primary schools training, to be delivered by cluster, however, the Coronavirus emergency forced us to cancel these sessions. We anticipate rescheduling this training for later on in the year and we will consider the use of Microsoft Teams if necessary.

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. 11 courses were delivered in 2019/20, the planned course in March 2020 was cancelled due to the Coronavirus outbreak in the same month. Therefore, in 2019/20 the number of staff that attended the 11 courses was 172 which compares with 157 in 2018/19. Please note that at the beginning of the year we agreed to increase capacity to accommodate increased demand in training at Brynglas House.

A breakdown per year is included below.

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

Feedback from staff attending courses is gathered for each training course held and continues to be positive.

Corporate Courses

These courses continue to be scheduled on a monthly basis, primarily for staff other than Social Services. 12 courses were scheduled for 2019/20, 2 were cancelled due to poor uptake and 1 cancelled in March due to the Coronavirus outbreak in the same month. Following the cancelled courses in April and May of 2019 we published a series of staff bulletins encouraging staff to attend and the following 9 courses were well attended. The number of staff that attended the corporate course was 98 compared with 105 in 2018/19. Whilst attendance does vary a little year on year the number of staff attending remains consistent.

Year	Number of staff who attended
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.

Councillor Courses

Three sessions 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. As detailed elsewhere in this report, whilst all Councillors were registered as data controllers this is not now required following ICO guidance. It is anticipated that further Councillor training will be planned for November 2021 or earlier as required.

Schools Courses

Schools have been engaged with in relation to GDPR including representation on the Data Protection Group. As above a service level agreement for primary schools for information management has been agreed and this will include regular training. Planned training will be re-scheduled appropriately.

Other Courses and Presentations

In June 2019, Data Protection training was provided to the Civil Parking Enforcement team. The information Management team presented at the GEMS training day in September 2019, staff at Gwent Music were trained in February 2020.

Information Management Team Training

Three current members of the Information Management team have passed the British Computer Society (BCS) Certificate in Data Protection including two members of staff on the updated legislation. The one remaining team member undertook this training in March 2020, however, the exam was postponed due to the Coronavirus outbreak.

E-Learning

All staff that need access to the council's computer network are currently required to undertake e-learning before they can access the network and this e-learning was revised in November 2019. The new GDPR e-learning module will provide guidance to staff on their obligations under the Data Protection Act 2018. The e-learning is also published on the intranet as reference to staff and as a refresher. An information security e-learning module is planned for 2020.

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. The main policy developed during this period is the Data Protection Policy detailed below.

Data Protection Policy

This policy was developed and has now been formally signed off. 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. The Information Security Incident Reporting Policy was extensively reviewed and updated to reflect changes required for GDPR (see elsewhere in the report). Policies are also reviewed generally to ensure that they are still valid and up to date. All policies were reviewed in 2019/20 and the following were updated this year:

- Access To Network and Email Policy
- Postal Services Policy
- Data Protection 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.

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 shared with the Information Governance Group to keep them informed of risks and is maintained by the Information Management team. Cyber Security remains a risk that needs to be managed.

Information risks are considered as part of the council's Annual Governance Statement and the Corporate Risk Register. The Chief Internal Auditor is a member of the Information Governance Group which helps to join up services. Cyber security has previously been included on the Corporate Risk Register but is not currently included. 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.

62 security incidents were recorded in 2019/20 compared with 46 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 the increase can be attributed to GDPR awareness.

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
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 major 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 the local government sector 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

- Lost council issued encrypted devices (laptops, smartphones with no personal data so low risk)

The most significant incidents during this year were:

Confidential Waste - it was established that no formal contract was in place for the disposal of the council's confidential waste although it was believed that a contract did exist. Further investigation highlighted potential concerns with the supplier in terms of suitability including a lack of suitable accreditation and if it carried out appropriate processes for confidential waste. We subsequently established a confidential waste contract with a suitable, accredited, provider. The ICO took no formal action, stating that the threshold for reporting had not been met.

All information security incidents are investigated with incident reports compiled following discussion with those involved in the incident. An overview is also reported to the SIRO and Information Governance Group.

In January 2020, the Information Management team developed an out of hours reporting procedure with our Civil Contingencies office and other stakeholders such as WARP (Warning, Advice, Reporting Point) group and the NCSC (National Cyber Security Centre). This plan details the out of hours reporting procedures in the event of a major cyber incident.

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 2019/20:

Information Sharing Protocols (ISP's)

An ISP for Newport's Youth Engagement and Progression Framework (YEPF) Not in Education, Employment or Training (NEET) Partnership is currently being developed and ready to be sent for quality assurance.

Newport Refugee Practitioners Forum (under development)

Supporting People (under development)

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 2019/20:

- Torfaen Hearing Impairment Service
- HM Armed forces support (In development)
- Pupil Transfer Data (updated to reflect GDPR)

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). The SRS provides an on call service and the systems covered by the SRS in this arrangement have been reviewed and agreed with a new procedure in operation across the council to reflect this.

The Coronavirus resulted in most of the council's employees and members working from home. This has been very successful in the circumstances and demonstrates the council's ability for employees and members to work successfully in this way. Virtual meetings have been enabled by the rapid roll out of Microsoft Teams. Employees and members can work effectively from home as a result of the mobility solution detailed in the Technology section below.

As a result of previous guidance from the Wales Audit Office, the council is part way through a large project to improve business continuity. New hardware was set up with the migration of backups of all systems from tape to disk. The next phase is to provide access to systems should both server rooms at the Civic Centre not be available. This is being reviewed as a result of the SRS cloud strategy as well as the council's move of a number of systems to the cloud already.

1.1. 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. Wales Audit Office 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.

Microsoft Office 365 now including Teams

The council migrated its e-mail solution during the last half 2019 to Microsoft Office 365. This 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, the planned roll out of Microsoft Teams was accelerated as a result of Coronavirus and rolled out to the whole organisation. 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 in the circumstances and will continue to be a very beneficial facility.

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 use of this as detailed above.

Mobility solution

The use of a mobility solution is rolled out for workers who need to work from home following improvements in response to the Coronavirus. This has extended the ability for users to access their information whilst away from their usual place of work. 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 now uses Microsoft Multi Factor Authentication (MFA) as used for

Office 365 access. The mobility solution has enabled the council's staff to work effectively with the challenges surrounding the Coronavirus.

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. The solution is live with enhanced Data Loss Prevention (DLP) facilities to scan e-mail for personal data which prompts users to encrypt e-mail if they include certain pieces of sensitive data. In line with the implementation of Egress Switch generally, the council will remove personal network storage for staff wherever possible.

In December 2019, NCC extended the Egress contract. The extension enables us to deploy an enhanced version hosted in the cloud. The enhancements include improvements in recipient experience and risk based protection. This extension also gives us time to investigate the potential for Office 365 message encryption to replace Egress in the future.

Xerox Mail “hybrid mail”

Further service 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/insert machine. This improves security by ensuring that print outputs are split in to envelopes automatically in the folder/insert machine. The system will be rolled out to other parts of the organisation to maximise the benefits to the council. This solution provides financial savings and reduces information risk. The Coronavirus has highlighted the need to accelerate the roll out of this solution.

DMARC ‘Domain-based Message Authentication, Reporting, and Conformance’

DMARC is a globally recognised email safeguarding protocol that authenticates email and controls what happens if an email fails authentication. In 2019/20 Newport City Council made significant enhancements to our DMARC policy to help combat malicious email practises. These enhancements are in line with NCSC (National Cyber Security Centre) recommendations. In December 2019 we amended our DMARC record to request that messages failing authentication be quarantined by the recipient. This is in line with Government Digital Service recommendations.

Desktop Technology

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. Laptops now represent over 80%% of all devices. The Coronavirus impact highlighted the benefits of laptops over desktop devices and the council's ability to function is largely as a result of the migration to laptop devices over a number of years. The intention going forward is that desktop devices will only be issued if there is a technical reason why a laptop can't be deployed. The council has deployed Windows 10 to nearly all its devices now. A small number have had support extended to ensure they can be patched and supported. All devices will be running Windows 10 as soon as possible.

Laptops and Desktop PCs

- All corporate laptops are protected using an end point protection solution
 - Encryption solution is used
 - A solution for schools laptops is under review
- Devices managed using Active Directory group policy management
- Mobile VPN for secure flexible and remote working as above
- All desktop PC's are protected using an end point protection solution
- Storage on networked home drives is recommended
- Unified Communications telephony solution has been deployed to all desktop users across the council including voicemail and the ability to access telephony from non council locations. This enabled staff to redirect calls to work or personal mobiles devices which supported the council's continued effective operation during the Coronavirus.

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) contract was rolled out in October 2017 with increased security features together with enhanced scanning facilities to drive the move to digital. A guest/partner printing solution has been implemented at the Newport East Community Hub

Remote Access Solutions

The council's secure VPN (Virtual Private Network) solution is used by ad-hoc agile workers and suppliers to identify and resolve issues with systems which they support. The solution was upgraded in February 20. Supplier accounts are disabled when not in use and they need to ring IT before they are given access. A small number of suppliers who may be required to support IT systems outside IT hours have a new solution using Microsoft Multi Factor Authentication (MFA).

Firewalls

Corporate firewall appliances are in place to protect the council's network from untrusted networks and a separate firewall protects the PSN network.

Wireless Staff Access

Wireless Access points are provided in many council buildings. This includes appropriate security controls in place. Major updates are planned for 19/20.

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 means that this provision is being reviewed in efforts to save money which may result in the provision being downgraded/removed in some of these sites.

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 and Information 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.

Digital and Technology Developments

The council's [Digital Strategy](#) outlines strategic objectives including a move to more 'cloud' based technologies. This includes the previous migrations of e-mail and Customer Relationship Management (CRM) systems to the cloud. The council's HR and Payroll system is now hosted by the supplier as a result of a major strategic review and re-development of the system. There are some risks in this change, with other organisations effectively holding the council's data and therefore work is required to ensure such systems and suppliers are appropriate.

Financial Systems

Wales Audit Office annually review the controls applied to key financial systems (reported to Audit Committee)

2.8. Records Management

The implementation of the corporate Electronic Document Management System (EDMS) across services includes retention facilities that assists with GDPR. An upgrade to the Social Services system took place and a similar upgrade to the corporate system is planned. 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.

A project manager was appointed who will focus on the increased use of the corporate Electronic Document Management System (EDMS) throughout the organisation. A plan for the further roll out of the Xerox Mail (Flexi Mail) solution will continue to reduce the amount of paper handled and reduce the potential for mail errors.

Capacity issues remain with the council's Modern Records facility at the Civic Centre as a result of building moves. Whilst additional space has been developed to provide further capacity, longer term options include the digitisation of some of the paperwork to provide alternative uses for the existing space.

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 sixth time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2019/20 was 1,100 which is a slight decrease from last year of 67 requests or 5.74%. This is only the second time that the number of requests has reduced from the previous year. The impact of the Coronavirus in March 2020 may account for some of 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 weeks. The figure for 2019/20 represents the second highest number of requests ever recorded (1167 in 2018/19). 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 2019/20 was 90.2% of requests responded to within 20 working days. This was above the target of 88% of requests. The council has met its target for seven of the nine years since a target was identified.

A breakdown per year is included below:

Year	Number of requests	Performance (Target)
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. The personal information request form used to identify specific subject areas for requests as well as gathering details of the requestor was amended to reflect the removal of any fee. It is crucial to gather proof of identity so personal data is not disclosed to a third part accidentally. We continue to issue corporate communications to ensure that these requests are recorded centrally and subsequently managed correctly. The Children and Young People Services team have been trained in the use of HOTH and provided with support as they are a key area for such requests. In 2019/20 we began recording corporate SAR performance against a target of 75% compliance and this was met despite a major impact to processing requests during March/April 2020 as a result of the Coronavirus;

Year	Number of requests	Performance (Target)
2019/20	77	77.9% (75%)

2. 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.

GDPR means that organisations need to be clearer and more transparent about how they process data. Many of the processes and tasks required to comply with this are well advanced with excellent progress made. In addition, organisations need to get a better understanding of what data they hold and the legal basis for the processing and this is well progressed with some work to do. Citizens are also provided with enhanced rights and these are 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 with the maximum to date being the proposed £182 Million fine for British Airways.

Maintaining compliance with Public Services Network and Payment Card Industry standards is challenging. This work is now dependent on the SRS to resolve on behalf of the council in conjunction with the Information Management team. Wales Audit Office will continue to provide an independent review of practice.

The Information Commissioner's Office (ICO) took no action against the council as a result of the single incident referred to the ICO by the council during this period. 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 from the Shared Resource Service (SRS) and this will require a different method of operation. 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 Teams and the SRS has further plans including a cloud strategy with its partners.

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

2.1. 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?
Staff unaware of information risks and data breach occurs	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	Digital Services Manager (DSM) in conjunction with Information Management team

			group	
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 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	Identify appropriate solutions to reduce risks and ensure card data is securely	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. Egress Data Loss Prevention (DLP) system rolled out and other improvements to e-mail security. Consideration of move to Microsoft e-mail encryption solution. Encrypted laptop devices New 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 considered	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 cloud strategy and NCC's plans to migrate systems to the cloud. Work with SRS to develop consistent IT system priorities across partners where possible 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 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	
Carry out annual IT Health Check	Aug 20
Develop remediation action plan and resolve as many vulnerabilities as possible prior to PSN submission	Jan 21
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 20
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
Complete the remaining GDPR audit requirements and actions	On-going
PCI accreditation	
Payment Card Industry Data Security Standard work to ensure appropriate controls in place and consideration of submission for formal accreditation	Sep 20
Cyber Essentials Plus	
Review findings if and when provided by assessing company	On-going
Cyber Stock Take	
Review results and develop action plan	Aug 20
Information Governance Culture and Organisation	
Circulate and analyse data protection staff survey	Dec 20
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 20
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
Complete review of Information and IT Security policy to be reviewed in reference to Data Protection Policy	Sep 20
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 planned Service Level Agreement	On-going
Re-schedule primary school data protection training	Dec 20
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 disaster recovery/business continuity improvements following previous WAO review as a result of SRS cloud strategy and the number of key systems that have already been moved to the cloud	Oct 20
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 cost/benefit of Office 365 message encryption against the Egress solution	Dec 20
Complete migration of all devices to Windows 10	Dec 20
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
FOI system options being considered including use of the new CRM system	Sep 20
Subject Access Requests	
Ensure all Subject Access Requests are recorded in FOI system and processed in line with Data Protection Policy	On-going