Annual Information Risk Report 2022/23

Created by	Information Governance
Date	14/7/2023
Reviewed by	Tariq Slaoui
Date	

Document Control

Version	Date	Author	Notes / changes
V0.1	24/04/2023	Tariq Slaoui	Initial draft
V0.2	21/06/2023	Tariq Slaoui	Updates to draft
V0.3	28/06/2023	Tariq Slaoui	Updates to draft
V0.4	03/07/2023	Tariq Slaoui	Updates to draft
V0.5	12/07/2023	Mark Bleazard	Draft for Scrutiny briefing
V0.6	14/07/2023	Mark Bleazard	Draft for Scrutiny meeting

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. This is the eleventh 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)**
  - This has been especially challenging this year due to the timing of the IT Health Check and the impact of major projects
  - The council was not PSN compliant from 13th August 2022 but, following considerable work, PSN accreditation was achieved on 15th June 2023. It lasts until 15th June 2024
  - A new IT Health Check was carried out and various improvements made since last year mean that the council and SRS are much better prepared
- **Payment Card Industry (PCI) standard**
  - In July 2022, with the assistance of SRS, the council completed the remaining work required and were informed that we had been successful in achieving PCI compliance
  - Work has commenced to ensure we satisfy the requirements for July 2023 onwards
- **General Data Protection Regulation (GDPR) and Data Protection Act 2018**
  - GDPR came into force in the UK from 25 May 2018 as a result of the passing of the Data Protection Act 2018 in the UK. Following on from Brexit, the EU GDPR no longer applies to the UK. For organisations operating inside the UK, the Data Protection Act 2018 (DPA 2018) is applicable
- **Cyber Stock Take**
  - The council has submitted Cyber Stocktake 5 and at time of writing awaits the results

Information Governance culture and organisation

- Last year, the Information Management Service Level Agreement (SLA) was extended for a further three years for all primary schools and now includes three secondary schools
- Quarterly meetings of the officer Information Governance Group (IGG) and Data Protection Group take place to oversee information risk management in conjunction with other stakeholders including Shared Resource Service. The IGG Terms of Reference and structure has been reviewed to improve engagement

Communications and Awareness Raising

- The organisation continues to raise awareness with staff.
- Corporate staff training numbers have increased again and highest yearly attendance figures
- Social Services training numbers have increased
- Training is provided for schools and good attendance over the last three years
- GDPR e-learning uptake has been excellent
- MetaCompliance engagement has been very good, cyber security training can now be monitored for all IT users
- Phishing simulations were carried out in January and June 2023 and will continue regularly

Information Risk Register

- Continues to be maintained and is referenced in the Council's Annual Governance Statement

Security incidents

- An increase in reported incidents, possibly because of increased awareness around issues as a result of GDPR and the increase of staff working from home.
- One incident reported to the Information Commissioner's Office (ICO). The ICO took no action.

Information Sharing

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

Business Continuity

- There is an ever-increasing reliance on digital technology to support business activities
- The availability of systems should be improved by the completed SRS data centre move
- A more proactive move of systems to the cloud started in 2021/22 with one major system moved to the cloud in 2022/23 and a further two in progress to complete in 2023/24.

Technology Solutions

- Secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business
- The existing remote access solution has been replaced with Microsoft Always ON VPN
- A Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) is being implemented

Records Management

- Continued roll out of EDMS solution across the council
- We have reduced the number of paper records held in Modern Records by disposing of records which have reached their retention period although other paper records are identified for archive

Freedom of Information

- **Exceeded target for year, for ten out of the last twelve years and each of the last six years**
- Increase in number of requests over last two years but below previous record highs
- Continue to promote the use of open data sets and adding new ones where appropriate

Subject Access Requests

- The Subject Access Request target was not met for this year due in part to a large percentage increase in the number of requests received
- In 23/24 we will be looking to introduce extensions to complex SAR's for the first time and we anticipate improved performance in terms of meeting targets because of this

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 the Data Protection Act 2018. The council needs to be clear and transparent about what data is processed and how to give citizens confidence that their data is being handled appropriately. Whilst the council continues to consider information risks in the broadest sense, cyber security is an important part of the council's approach due to the increased risks over recent years.

A key requirement from now on is to ensure the alignment of new Digital Strategy 2022-2027 actions to the action plan in this report and that of the Annual Digital Report

The actions outlined in this report form part of the People, Policy and Transformations service plan and are 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, especially around cyber security
- 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
- This is the eleventh Annual Information Risk Report
- Reduce the risk of failing to protect personal data and any subsequent reputational and financial penalties
- 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. A new Digital Strategy for 2022-2027 has been developed and this was approved by Cabinet in April 2023. Primarily the work associated with this report fits within the 'Data and Collaboration' theme of the strategy. A key requirement from now on is to ensure the alignment of Digital Strategy actions to the action plan in this report and that of the Annual Digital Report. The Digital Strategy was developed following extensive external and internal engagement. It reiterates the council's commitment to secure systems and processes so that 'people have confidence in the council's management of their data.' Whilst the council continues to consider information risks in the broadest sense, managing cyber risks is a vital part of the council's approach. Key roles and responsibilities for individuals and groups are outlined below.

2.1. Compliance and Audit

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

Public Services Network (PSN) compliance

Whilst the council was PSN compliant from 13th August 2021, the authority's PSN compliance lapsed on 13th August 2022. The annual IT Health Check was carried out in July 2022 and we worked in conjunction with the SRS to develop a Remediation Action Plan (RAP). This has been particularly challenging this year due to the timing of the IT Health Check and the impact of major projects, primarily the data centre migration project led by SRS and the implementation of the new finance system. This resulted in a gap in accreditation. At time of writing, despite these significant challenges, PSN accreditation was achieved on 15th June 2023 and lasts until 15th June 2024. A new IT health Check was carried out in May 2023. The timing of this, combined with various improvements made since last year, mean that the council and SRS are much better prepared. In any case, a large amount of work is carried out on a daily basis to protect the council's systems and data 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). The council is committed to continued compliance with PSN standards as detailed in the Digital Strategy 2022-2027.

Payment Card Industry Data Security Standards (PCI-DSS)

Newport City Council has satisfied the requirements of the Payment Card Industry (PCI) Data Security Standards. The council procured assistance from an external organisation to undertake a gap analysis and subsequent plan to address any shortfalls. In July 2022, with the assistance of SRS, the council completed the remaining work required and were informed that we had successfully completed an assessment against the PCI-DSS v3.2.1 standard. This accreditation continues until July 2023 and the council has procured assistance with the aim of continued compliance as well as planning for Version 4 of the standard in 2024.

The UK General Data Protection Regulation (UKGDPR) and Data Protection Act 2018

The UK General Data Protection Regulation (GDPR) imposes certain requirements and responsibilities regarding data protection. The local authority must comply with the Data Protection Act 2018, which is the legislation that implements GDPR in the UK.

Under the Data Protection Act 2018, the local authority needs to ensure that personal data is handled securely and lawfully. We should document the personal data we hold and maintain a record of processing activities. In the event of a data breach, certain breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours.

Data subjects have specific rights, and the local authority must provide privacy notices which communicate these to individuals. We must respond to requests for personal data, known as Subject Access Requests, within 30 calendar days. We should also identify a lawful basis for each processing activity. Consent has been strengthened, but other lawful bases can also be used. Specific guidance is available regarding children's rights and their data protection.

The Data Protection Act 2018 also requires the local authority to conduct Data Protection Impact Assessments (DPIAs) for new projects and technology implementations and we must appoint a Data Protection Officer to oversee compliance.

The local authority should be aware that significant fines can be imposed by the ICO for non-compliance with the data protection regulations. The authority has a well-established Data Protection Group, which meets regularly to address data protection matters, raise awareness among staff, and ensure proper documentation of data assets and processing activities. Data Protection is a standing item on the quarterly Information Governance Group Agenda.

Cyber Stock Take

Newport City Council, along with all other local authorities in Wales, took part in the fifth 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. At the time of writing this report the results of the stock take have not been received. Once received the results will be analysed to see what actions may need to be taken.

It is hoped that some weaknesses identified previously will be improved by the implementation of a SIEM/SOC solution as detailed elsewhere in this report and increased awareness raising as a result of the MetaCompliance solution implementation. Further improvements identified will be pursued.

Audit Wales

Audit Wales 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 2022/23 Audit Wales carried out a review on cyber security arrangements of the council and on the Digital Strategy development. At the time of writing this report, an initial draft report on cyber security has been shared with the council for comments. A previous Audit Wales report on cyber across Wales was presented as a 'Part 2' item to Governance and Audit Committee report in May 2021.

2.2. Information Governance Culture and Organisation

The council has been a partner of the Shared Resource Service (SRS) since April 2017. Representatives from the SRS attend various Newport City Council groups. There is also a client side role that sits within the Digital team and this relationship continues to develop and mature.

Information Governance Culture

Previous staff surveys highlighted good staff awareness and the importance of data protection. Ensuring the continued effectiveness of groups and individual roles is important and is reflected in commitments in the new Digital Strategy.

Organisation

Senior Information Risk Owner (SIRO) role
The council's Senior Information Risk Owner (SIRO) role is part of the Head of Law and Standards role. The SIRO role is the senior officer responsible for information risks within the organisation and is part of the council's Corporate Management Team. A new post holder commenced during the year and briefing sessions have been provided to go through the role and discuss challenges. Day to day operational management is provided by the Information Management team that reports to the Head of People, Policy and Transformation. As detailed below, the SIRO role is more senior and is distinct from the Data Protection Officer (DPO) role below.

Data Protection Officer (DPO) Role
Under the Data Protection Act 2018 the council needs to specify its Data Protection Officer (DPO). This role is incorporated within the duties of the Digital Services Manager post. As part of the Service Level Agreement (SLA) with primary schools, the Digital Services Manager post is also the DPO for these schools.

Information Governance Group
The Information Governance Group meets quarterly chaired by the Strategic Director – Transformation and Corporate. This, and the independent SIRO role, 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 to ensure that information risks are managed appropriately. Membership of the group includes representation from the Shared Resource Service (SRS) which will be a major contributor to this work. During this year the terms of reference of the group and membership were reviewed and changes made accordingly.

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 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. As detailed above, the SRS plays a vital part in achieving PSN accreditation and managing technical risks.

Councillor Data Protection
An important aim of this report is to ensure that members and senior officers are aware of the data protection responsibilities of the council and to enable guidance to be provided. This is especially relevant given the level of cyber risks facing the council and other organisations. 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 responsible Cabinet Member, Organisational Transformation is regularly briefed on information risks and on-going activity to mitigate these.

Information Asset Register
The development of an Information Asset Register 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. This has commenced and is part of the work of the Data Protection Group and Information Management team. This will become a complete Record of Processing Activities (RoPA). At present the authority has updated the Education and Adult Services registers. These registers are currently being recorded into the MetaCompliance solution. A cloud services register has been developed in line with our policy of deploying solutions to the cloud.

Schools
Schools are “data controllers” under the Data Protection Act and therefore need to handle data appropriately. Guidance is provided to schools by staff in Education and Information Management. A Service Level Agreement (SLA) originally just for primary schools with the Information Management team has now been extended until the end of the academic year 24/25 and this SLA now includes three secondary schools too. Regular guidance and advice has been provided to these schools as well as responding to queries raised by them. Training has also been provided as detailed below.

1.1. Communications and Awareness Raising

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

Staff Guidance

Regular reminders of good practice have been provided in the staff bulletin and on the intranet on various important subjects. During 2022/23, the council regularly reminded staff of the importance of subjects such as:

- Phishing e-mails
- Reminders of cyber threat escalation in relation to Russia/Ukraine relations
- Use of MetaCompliance
- The migration to the Always On VPN solution and removal of previous Netmotion solution
- Teams chat retention
- Phishing simulation results

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

Training Courses

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

- Social Services courses
- Corporate courses
- Councillor courses
- School 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 because of the Coronavirus pandemic. There will never be totally comprehensive technical measures to protect data. Training provided to staff is a key part of investigations carried out by the Information Commissioner's Office (ICO).

Social Services Courses

Social Services employees continue to represent a high-risk group due to the nature of the information they handle as part of their roles and training is compulsory for these staff. Face to face training is scheduled for Social Services staff who do not have access to technology.

A breakdown per year is included below.

Year	Number of staff who attended
2022/23	66
2021/22	31
2020/21	0
2019/20	172
2018/19	157
2017/18	237
2016/17	144
2015/16	147
2014/15	182
2013/14	226

Corporate Courses

These courses continue to be scheduled monthly, primarily for staff other than Social Services. The number of staff that attended the corporate course has increased 228 in 2022/23. Whilst attendance does vary a little year on year the number of staff attending remains consistent.

Year	Number of staff who attended
2022/23	228
2021/22	181
2020/21	74
2019/20	98
2018/19	105
2017/18	114
2016/17	118
2015/16	114
2014/15	152
2013/14	93
2012/13	57

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

Councillor Courses

Councillors, like all council staff, need to undertake mandatory e-learning before they are provided with access to the council's network. More detailed information security training is also provided. The information management team provided two training sessions for councillors in June 2023. 32 out of 51 members attended the courses which represents excellent attendance.

Schools Courses

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

Year	Number of staff who attended
2022/23	87
2021/22	119
2020/21	78

Training for primary schools, and now some secondary schools, remains a priority for the return to classrooms in September 2023.

Other Courses and Presentations

45 staff received specific training relating to their area, such as the Additional Learning Needs team (ALN), Community Safety Wardens, Social Services duty and assessment team and the Passenger Transport Unit.

Information Management Team Training

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

E-Learning

All staff that need access to the council's computer network are currently required to undertake GDPR e-learning before they can access the network. The GDPR e-learning module provides guidance to staff on their obligations under the Data Protection Act 2018**. In 2022/23 641 staff completed the NCC GDPR e-learning module.**

MetaCompliance Solution

In early 2022, the council procured the MetaCompliance Solution which allows us to deliver cyber security related content to users' desktops. Following on from successful user testing, the Information Management team began using the solution in July 2022. The solution is designed to improve the Council's awareness of information security and data protection by complementing existing training. It includes a suite of security awareness training capabilities including: -

- Security awareness training
- Policy management
- Phishing simulation

The following interactive training has been deployed to NCC staff across the organisation.

Course	Date	Completed	Not completed
NCC password training	July 2022	72.4%	27.6%
Phishing – The Essentials	November 2022	56.7%	43.3%

The solution also allows us to target officers and departments with appropriate content as shown below.

Course	Date	Completed	Not completed
PCI – DSS Training	March 2023	84.2%	15.8%
An introduction to FOI	June 2023	60.0%	40.0%

In January 2023, we sent out a simulated phishing e-mail to all staff to establish our understanding of the threat of phishing e-mails. The phishing e-mail appeared to be from Microsoft inviting the individual to click on a link to update their account. The individual would then be invited to submit their details via an online form.

The purpose of this was to raise awareness of the risks associated with phishing, accordingly we plan to carry out regular simulations in future.

Many employees informed the Information Management team and/or SRS of this e-mail. The results of the exercise are highlighted in the diagram below, 9.2% of IT users clicked the link and 4.0% of IT users input data into the form. Those who clicked the link were informed of the simulation and some brief training was provided.

The intention is improve awareness by further content and reminders on content already published.

Information Policy Development

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

Updated Policies

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

- Information and IT Security Policy
- Mobile phone 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. The Information and IT Security Policy has been reviewed and updated with some major changes. A further review of policies is required to ensure they are all up to date and valid. This is planned for the coming year.

2.4. Information Risk Register

An information risk register is maintained that identifies key information risks, their likelihood, impact and the measures in place to mitigate the risk. The risk register is regularly updated and shared with the Information Governance Group as appropriate 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 a specific concern that is considered along with wider information risks. 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 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.

103 security incidents were recorded in 2022/23 compared with 80 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. During the pandemic, 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. However, the number of incidents relating to lost or stolen hardware increased to 22 in 2022/23 which has an impact on the total number of incidents recorded.

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 6 incident	Other - principle 6 incident security of personal information) incident	Technical security failing
2022/23	103	63	22	3	0	2	11	2
2021/22	80	58	7	1	0	0	9	5
2020/21	66	48	3	1	1	0	10	3
2019/20	62	39	11	4	1	0	6	1
2018/19	46	29	7	3	1	0	4	2
2017/18	34	18	6	4	0	0	4	2
2016/17	43	25	5	0	0	1	8	4
2015/16	62	23	12	2	0	9	11	5
2014/15	66	14	23	0	2	18	0	9
2013/14	64	14	9	6	1	8	4	22
2012/13	63	No split by category available						

Analysis by category is always to some extent subjective as incidents could easily be categorised in more than one category. Therefore, these categories should be seen as indicative only. It should be noted that not all incidents result in a breach of data. For example, phishing incidents are recorded as principle 6 DPA incidents, however, users may not have clicked the link or our technical solutions prevented the threat from escalating further.

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

- Incidents arising as result of human error form most 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
- An increase in lost/stolen council issued encrypted devices (laptops, smartphones with no personal data so low risk)

The most significant incident during this year was:

In November 2022, an officer e-mailed unredacted adoption documents to the wrong recipient in error. The individuals affected were informed and we reported this incident to the Information Commissioner's Office (ICO) who investigated and subsequently took no action. During our internal incident investigation, actions were taken to minimise the possibility of any further occurrences.

2.6. Information Sharing

Partnership and collaborative working drives sharing of increased amounts of information between the council and other organisations. The Wales Accord on the Sharing of Personal Information (WASPI) requires public sector organisations to follow agreed guidance in the development of Information Sharing Protocols (ISP's). The council signed up to WASPI in January 2011 and most recently, the authority has been consulted on a proposal for WASPI to be an approved Code of Conduct for the ICO. The authority responded positively to this and we wait for the outcome of the consultation. The Information Management team leads on this work and has developed a number of ISP's with services and other organisations. The following represents developments in 2022/23:

Information Sharing Protocols (ISP's)

- Identifying the triggers – Llanwern project – June 2022
- Practitioners Forum ISP – September 2022
- Ukrainian Refugees programme ISP – June 2022

Data Disclosure Agreements (DDA's)

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

Data Disclosure Agreements have been developed as follows:

DDA's in 2022/23:

- Cardiff University – research into criminally exploited children – March 2023
- Pupil Information to Support School Health based Programmes – September 2022
- Nest Warm homes scheme – August 2022

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 should be improved by the data centre move that was completed in May 2023. Improvements to backups have also been made to provide greater resilience as this is vitally important in the event of cyber incidents including ransomware.

A more proactive move of systems to the cloud took started in 2021/22. This is designed to provide greater resilience as suppliers scale solutions for lots of customers, update systems proactively and have greater expertise to support their own systems. In March 2023 the Capita One education system was moved to the cloud and the IDOX Uniform migration is due to go live in July 2023. This is designed to provide greater availability and better business continuity/disaster recovery. The council's primary finance system is also due to move to the cloud in late 2023.

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

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

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

1.1. Technology Solutions

Numerous technical solutions are in place to minimise risk to information and the corporate network generally. PSN and PCI compliance together with the development of business continuity requirements continue to drive technical improvements for information governance. As a result of our partnership with the Shared Resource Service and its partner organisations, the council will pursue options for collaboration and simplification wherever practical.

Devices
The council now almost exclusively uses laptops for flexibility and mobility and this has been useful for increased flexible working over the last few years. Laptops will always be issued unless there is a specific reason that a desktop device is required in very limited scenarios. Windows 10 is deployed to all devices with regular updates required.

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

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

Security Information and Event Management (SIEM) system and Security Operations Centre (SOC)
The implementation of a Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) with SRS is designed to monitor potential cyber attacks and provide improved preventative measures as a result. This has now been implemented and complements existing solutions.

Devices for Members
Members have tablets and, in combination with laptop devices, provide a comprehensive solution for their role. The refresh of member laptop devices is included within the wider laptop refresh cycle so where new devices are required they are provided. Following local government elections in May 2022 tablets and mobile phones were re-issued or new devices provided where necessary.

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 of new infrastructure as part of the data centre move and other developments.

Remote Access Virtual Private Network (VPN) Solution
The council now uses the Microsoft Always On VPN solution. This enables all staff who need to work from home to do so. It provides the ability to carry out password resets and Windows updates due to its “always on” connection type enhancing security. Staff are able to work from anywhere where a wireless network is available (subject to geographical restrictions), as if they were sat at their desk, which also reduces the requirement to carry paper documents.

Multi-Function Devices
‘Follow Me’ print is available to all users, who are able to access council printers from any location with a device. An upgrade took place to the software that supports Multi-Function Device s (printer/copier/scanner).

Secure/Large File transfer solution
Secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business.

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

Wireless Staff Access
Wireless Access points are provided in many council buildings. This includes appropriate security controls in place. Following the completion of the data centre move new infrastructure will be implemented to improve Wi-Fi at key sites.

Wireless Public Access
Public Wi-Fi is available in the city centre (Newport City Connect), over 50 public buildings (Newport Community Cloud) and on buses.

Physical Security
Major buildings are limited to staff with physical access cards 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

The 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, Teams etc. For those that just need calls and texts, basic phones are provided as they are much cheaper. All phones are managed using a Mobile Device Management (MDM) solution to limit access and the ability to wipe phones remotely if required.

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

2.8. Records and Data Management

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

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

Developments in 2022/23 include:

- Merger of corporate and social care environments

Tens of boxes of archived files passed their destruction date during the year and these are securely destroyed. This continues to free up capacity in Modern Records although other paper files are regularly identified from other locations that offset this at times..

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

2.9. Freedom of Information and Subject Access Requests

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

Freedom of Information
This is the ninth time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2022/23 was 992 which is an increase from last year (953). 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 several FOI requests and the number tends to reflect the level of public interest. The Covid pandemic almost certainly had an impact on the number of requests since 2020/21, however, the number has risen in the last two years, and we are nearly back to previous highs in 2018/19. Performance for 2022/23 was 91.0% of requests responded to within 20 working days. This was above the target of 88% of requests. The council has met its target for ten of the twelve years since a target was identified including each of the last six years.

A breakdown per year is included below:

Year	Number of requests	Performance (Target)
2022/23	992	91.0% (88%)
2021/22	953	89.5% (88%)
2020/21	797	90.8% (88%)
2019/20	1100	90.2% (88%)
2018/19	1167	90.1% (88%)
2017/18	1037	88.3% (88%)
2016/17	1087	84.1% (88%)
2015/16	914	92.3% (87%)
2014/15	895	87.7% (87%)
2013/14	869	87.1% (87%)
2012/13	698	90.4% (87%)
2011/12	540	84.4% (87%)

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
- 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
- Social Media House Rules
- Links to Privacy Notices

Subject Access Requests
Subject Access Requests (SAR's) are requests for personal information requested by the data subject and care needs to be given to ensure that personal information relating to other data subjects is removed. As a result of General Data Protection Regulation, fees have not been charged since April 2018. A new Data Protection Policy was developed, and this includes the rights of individuals under the Data Protection Act 2018. Specific guidance on processing Subject Access Requests is included in the policy and guidance to staff has been provided on the intranet and in staff bulletins. A personal information request form is used to identify specific subject areas for requests as well as gathering details of the requestor. It is crucial to gather proof of identity so personal data is not disclosed to a third party accidentally. The council narrowly missed its performance target for dealing with Subject Access Requests. 70.9% of requests were responded to within the deadline, against a target of 75%. Gaining access to paper records has been a greater challenge because of the Coronavirus pandemic and the subsequent move to more remote working.

Under normal circumstances, the authority has to respond to the SAR within one month. However, there are certain situations where the compliance period can be extended. This means that we can take longer than one month to respond to the SAR if the request is deemed to be particularly complex. In 2023/24 we will be looking to introduce extensions to complex SAR's for the first time and we anticipate improved performance in terms of meeting targets because of this.

Year	Number of requests	Performance (Target)
2022/23	103	70.9% (75%)
2021/22	76	71.0% (75%)
2020/21	70	60.0% (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 increase in the number of staff working from home provides some specific challenges, especially with greater concerns over cyber attacks.

Compliance and Audit
Maintaining compliance with the Public Services Network (PSN) is always a challenge. This has been particularly challenging this year due to the timing of the IT Health Check and the impact of major projects, primarily the data centre migration project led by SRS and the implementation of the new finance system. This resulted in a gap in accreditation. Despite these significant challenges, PSN accreditation was achieved on 15th June 2023 and lasts until 15th June 2024. A new IT health Check was carried out in May 2023. The timing of this, combined with various improvements made since last year, mean that the council and SRS are much better prepared. PCI compliance was achieved in July 2022 for the first time in a number of years and work has commenced to ensure continued compliance from July 2023 onwards. We await the results of cyber stock take 5. We will review the results and identify areas for improvement. We also await the formal report on Cyber Security undertaken by Audit Wales.

Information Governance Culture and Organisation
Last year, the Information Management Service Level Agreement (SLA) was extended for a further three years for all primary schools and now includes three secondary schools. Quarterly meetings of the Information Governance Group (IGG) and Data Protection Group take place to oversee information risk management in conjunction with other stakeholders including Shared Resource Service. The IGG Terms of Reference and structure has been reviewed to improve engagement.

Communications and Awareness Raising
We continue to raise awareness with staff. Corporate staff training numbers have increased again and highest yearly attendance figures. Social Services training numbers have increased. Large amount of training provided for schools with good attendance over the last three years. GDPR e-learning uptake has been excellent. MetaCompliance engagement has been very good, cyber security training can now be monitored for all IT users. Phishing simulations were carried out in January and June 2023.

Information Risk Register
The Information Risk Register continues to be maintained on an on-going basis.

Security incidents

- There was an increase in reported incidents, possibly because of increased awareness around issues as a result of GDPR. Also, the number of incidents relating to lost or stolen hardware increased to 22 in 2022/23 which has an impact on the total number of incidents recorded. One incident was reported to the ICO. The ICO took no action.

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

Business Continuity
There is an ever-increasing reliance on digital technology to support business activities and maximise the availability of systems that this should be improved as a result of the completed SRS data centre move. One major system was moved to the cloud in 2022/23 with two more due to be completed in 2023/24.

Technology Solutions
Secure and large file transfers are now provided using Microsoft Office Message Encryption and Microsoft One Drive for Business. The existing remote access solution has been replaced with Microsoft Always ON VPN. A Security Information and Event Management (SIEM) system and Security Operations Centre (SOC) is being implemented. Other security standards for e-mail system hygiene have also been implemented.

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

Freedom of Information
The council exceeded its target for the year but this always requires a large amount of effort. The council has met its target for ten of the twelve years since a target was identified including each of the last six years. The number of requests has increased over the last two years but still remains below its pre-pandemic peak. We continue to promote the use of open data sets and adding new ones where appropriate.

Subject Access Requests
The Subject Access Request target was not met for this year due in part to a large percentage increase in the number of requests received. In 23/24 we will be looking to introduce extensions to complex SAR's for the first time and we anticipate improved performance in terms of meeting targets because of this.

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 Roll out of policy management/e-learning solution Intranet content and staff bulletins Development of new policies and update of existing ones On-going role of Data Protection group and Information Governance Group The actions outlined in this report form part of the People, Policy and Transformations service plan and also considered in the Corporate Risk Management Strategy and Corporate Risk Register.	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	The new Digital Strategy has a specific theme of Data and Collaboration that recognises the value of data and the importance of using effectively and appropriately. Day to day operational guidance provided by Information Management team	Digital Services Manager (DSM) and Information Management team
PSN (Public Services Network) accreditation not gained	H	L	Ensure appropriate scheduling of Annual IT Health Check. Resolve vulnerabilities identified in latest Annual IT Health Check. Evidence information governance arrangements as detailed in this document. Ongoing patch management and other activities to reduce risks. Continued engagement with Members Proactive vulnerability scans run by SRS	Digital Services Manager (DSM) in conjunction with SRS
Delivery of IT Service by Shared Resource Service (SRS) provides less	M	M	Continue to strengthen relationship with the SRS and the complementary activities of SRS Security team. Security activity is a key part of SRS' workload	Digital Services Manager (DSM) in conjunction with Head of PPT / SRS management

control				
Do not meet requirements of EU General Data Protection Regulation	M	M	Staff Awareness raising especially senior management Standing agenda item at Information Governance Group	Digital Services Manager (DSM) in conjunction with Head of PPT / SRS management
PCI- DSS (Payment Card Industry Data Security Standards) compliance not achieved	M	M	PCI compliance achieved in July 2022 and working to renew in July 2023 Will work to ensure continued compliance in future.	Digital Services Manager (DSM) in conjunction with in conjunction with SRS
Technical Solutions are not available to meet the needs of service delivery and data breach occurs	H	L	Microsoft Multi factor Authentication (MFA) solution for secure access to 365 e-mail. Microsoft Office Message Encryption and One Drive rolled out. Encrypted laptop devices Multi-Function Devices (printer/copier) has increased security features Data stored on servers and not on local devices unless encrypted Review solutions, identify and plug any gaps Maintain health check and compliance requirements Review the security of cloud based technical solutions including Data Protection Impact Assessments (DPIA's) Cloud security measures	Digital Services Manager (DSM) in conjunction with Information Management team
Information is not shared appropriately and securely	H	L	Development of new Information Sharing Protocols and Data Disclosure Agreements and review of existing ones Advice and guidance	Digital Services Manager (DSM) in conjunction with Information Management team
Critical IT systems are not available to services	H	L	The SRS planned data centre move has been completed and NCC's plans to migrate systems to the cloud will improve availability and business continuity.	SRS in conjunction with Digital Services Manager and services
Information security is not considered for new projects	M	L	Data Protection Impact Assessments (DPIA's) carried out for new projects with further DPIA's required going forward. Use ICO process including screening	Digital Services Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Complete Remediation Action Plan for PSN	Jul 23
Assess results of Annual IT health Check and develop plans to address vulnerabilities	Jul 23
Make submission for PSN prioritising this work in SRS/NCC	Mar 24
Once received, review findings of final Cyber Security audit carried out by Audit Wales and take appropriate actions as necessary	TBA
EU General Data Protection Regulation (GDPR) and Data Protection Act 2018	
Data Protection to be discussed as standard item at Information Governance Group and Data Protection Group	On-going
Review any new forms and associated privacy notices for the organisation. This will include the legal basis and consent where appropriate	On-going
On-going development and maintenance of Record of Processing Activity (RoPA)	On-going
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
PCI accreditation	
Payment Card Industry Data Security Standard - carry out assessment and any necessary work prepare to ensure continued compliance with new PCI security standards. Develop plans for Version 4 of the standard required in 2024.	Jul 23
Cyber Stock Take	
Once received, review results of stock take 5 and develop action plan when results provided	TBA
Information Governance Culture and Organisation	
Contribute to information governance considerations across all SRS partners including Information Security Leadership Board	On-going
Quarterly meetings of the Information Governance Group to oversee information risk management in conjunction with other stakeholders including Shared Resource Services representation	On-going
Quarterly meetings of Data Protection Group to discuss operational data protection issues	On-going
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Members updated through Annual Information Risk Report, including review by Scrutiny Management Committee	Jul 23
Communications and Awareness Raising	
Regular data protection training sessions corporately, for Social Services and for SLA schools	On-going
Further policies and guidance will be developed to support the organisation	On-going
Review of information management policies	Oct 23
Provide advice and guidance to support primary schools in conjunction with Service Level Agreement	On-going
Develop and deliver training for members	Jun 23
Provide regular e-learning content via MetaCompliance solution	On-going
Monitor take up of e-learning content and monitor take up rates to increase awareness	On-going
Develop and deliver training for members	Jun 23
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	
Migration of priority IT systems to the cloud to improve business continuity	On-going
Technology Solutions	
As a result of our partnership with the Shared Resource Service, the council will pursue options for collaboration and simplification wherever practical	On-going
Review technical solutions to ensure they meet information governance needs including cloud-based systems	On-going
Consider the need for new technical solutions to address weaknesses	On-going
Extend use of Xerox Mail solution to improve mail distribution processes	On-going
Records Management	
Continued roll out of EDMS solution across council	On-going
Review options for Modern Records and storage including destruction of records past their destruction date	On-going
Freedom of Information and Subject Access Requests	
Freedom of Information	
Publication of further open data for suitable data sets	On-going
Subject Access Requests	
Work with services to improve performance on Subject Access Request responses including the ability to apply extensions where appropriate for complex requests	Jul 23