Annual Information Risk Report 2017/18

Created by	Information Governance
Date	09/04/2018
Reviewed by	
Date	

Document Control

Version	Date	Author	Notes / changes
V0.1	09/04/18	Mark Bleazard	Initial draft based on previous report
V0.2	17/04/18	Mark Bleazard	Updated draft for Information Governance Group
V0.3	30/04/18	Mark Bleazard	Further updates including FOI performance
V0.4	17/07/18	Tariq Slaoui	Review following Information Governance Group meeting
V0.5	28/09/18	Mark Bleazard	Updates on PSN for Cabinet Member briefing

Table of Contents

Contents

Executive Summary

The council has a statutory requirement to look after the data it holds in line with the Data Protection Act. From May 2018 this will requirement will be aligned to General Data Protection Regulation (GDPR) across the European Union. During 2017/18, the Information Commissioner's Office (ICO) has the power to fine organisations up to £500,000 for data breaches to ensure organisations take this responsibility seriously. **From May 2018, EU General Data Protection Regulation enables much higher fines of 20 Million Euros or 4% of turnover.**

This is the sixth 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:

- Accreditation and audit
    - Public Services Network (PSN) accreditation. There have been some delays as a result of scheduling the annual IT Health Check. At time of publication we are awaiting the result of re-submission
    - **As a result of EU General Data Protection Regulation, the council has carried out a large amount of work to comply with the new Data Protection Act 2018.** Work is on-going to improve openness and transparency to customers including:-
        - Awareness raising within the organisation especially for senior managers, general guidance in staff bulletins and amended staff training course
        - Incident Reporting – The Information Security Incident Reporting Policy has been amended and published, to align us with the requirements of GDPR
        - Individuals Rights – Individuals rights are being strengthened under GDPR and this is reflected in privacy notices published
        - Data Protection Officer role formally agreed to fit in duties of Digital Services Manager role
        - Subject Access Request procedure amended and £10 fee removed
    - Progress made on Payment Card Industry (PCI) data security standard but further work to ensure compliance with the latest PCI standards
    - Wales Audit Office – progress on disaster recovery/business continuity detailed in Business Continuity section
- Information Governance culture and organisation
    - Now a partner of the Shared Resource Service (SRS) which results in need to develop and maintain a key strategic and operational relationship with SRS. SRS represented on Information Governance Group
    - Information Asset Register needs to be extended in line with GDPR to document information processing activities
- Communications and Awareness Raising
    - Continue to raise awareness with staff and Members
    - **Highest ever number of staff trained in a year by the organisation as a result of additional Social Services training**
    - **Training for Members now planned for Autumn 2018**
    - Review of policies carried out including changes to the Information Security Incident Reporting Policy in line with GDPR
    - E-learning revised and re-published

- Information Risk Register
    - Continues to be maintained
    - Contribution to Annual Governance Statement
- Security incidents
    - **A further reduction in incidents which represents a new low of incidents recorded**
    - On-going management of incidents
    - One incident reported to the Information Commissioner's Office (ICO) during 17/18. This was investigated and closed by ICO with no formal action taken against the council
- Information Sharing
    - Development of Information Sharing Protocols (ISP's) continues along with Data Disclosure Agreements (DDA's)
- Business Continuity
    - As a result of previous guidance from the Wales Audit Office, the council is part way through a large project to improve business continuity. To date, new hardware has been set up with the migration of backups of key systems from tape to disk.
- Technology Solutions
    - As a result of our partnership with the Shared Resource Service, the council will pursue options for collaboration and simplification wherever practical.
    - Egress Data Loss Prevention facility enabled.
    - Xerox Mail "hybrid mail" system continues to be rolled out to streamline the production of paper and electronic outputs.
- Records Management
    - Resource issues slowed progress with the ongoing implementation of the corporate Electronic Document Management System (EDMS) across services. This resource issue has now been resolved and further progress is expected over the forthcoming year.
    - Some capacity issues for Modern Records facility being addressed
- Freedom of Information
    - Met target for year
    - **First reduction in the number of requests received since records began in 2011**
    - Publication of open data sets where appropriate
    - **Gender pay gap information published for the first time**
- Subject Access Requests
    - Subject Access Request procedure amended and £10 fee removed

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 under the existing Data Protection Act (1998) and other legislation. General Data Protection Regulation (GDPR) requirements, as a result of EU legislation are more stringent with enhanced rights for citizens and this will place 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. A key focus of GDPR is for organisations to be more clear and transparent about what data is being processed and how. This is designed 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, developed from the existing Spatial Data team is designed 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 further detail incorporated in the Digital team annual business plan. Information Risk is 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 sixth Annual Information Risk Report. Last year's report referenced a five year position. This report focuses on the last year only.
- 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. At the time of writing, the Information Commissioners Office (ICO) can issue a fine of up to £500,000 for data breaches. As detailed last year, the fines associated with General Data Protection Regulation (GDPR) come in to place on 25th May 2018 at which point the maximum fine is 20 Million Euros or 4% of turnover. In cases where data breaches are referred to the ICO, its investigations highlight the importance of effective governance arrangements to reduce risks
- Ensure that appropriate risks are escalated to the Corporate Risk Register

2. Current Position

This part of the report identifies the council's current position in relation to information governance; this includes a number of external compliance requirements. 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.

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 the Wales Audit Office to ensure appropriate information governance is in place.

Public Services Network (PSN) compliance

In line with PSN requirements, an annual IT Health Check was undertaken with an approved contractor. As a result of some scheduling issues, there was delay in undertaking the Annual IT Health Check. Following the original draft of this report, a PSN submission was made in May 2018. This submission was rejected by the Cabinet Office due to some outstanding vulnerabilities identified in the Remediation Action Plan. These vulnerabilities were prioritised by the IT Service and the majority are now completed. At the time of publication a resubmission has been made to the Cabinet Office and we are awaiting the outcome. There are always challenges to compliance given the variety of risks and work is required throughout the year to protect the council's data and systems. Risks around cyber security have increased and this is 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 applies in the UK from 25 May 2018. 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.

There are major implications as a result of GDPR and this is a standard agenda item for the Information Governance Group.

A summary of some of the changes are detailed below:

- The maximum fine is 20 Million Euros or 4% of turnover
- Greater requirement to document the personal data held
- Data breach reporting will become mandatory for certain data breaches
- Enhanced rights for data subjects including improved privacy notices and increased focus on consent that must be unambiguous and not assumed
- Specific guidance relating to children and their rights
- Requirement to establish legal basis for sharing beyond "legitimate interests"

- 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
- Requirement for Data Protection Officer
- Further consideration of data stored outside the EU

A GDPR Task and Finish group was established with representation from each service area. With the assistance of the group, Newport City Council has made progress in the following areas;

- Awareness raising – The task and finish 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 to provide specialist input, including a meeting of the heads of secondary schools in Newport. An intranet presence has been set up and content uploaded. E-bulletins have been issued to provide corporate updates.
- Communicating Privacy Information – The task and finish group have 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. Under GDPR, Newport City Council will need to demonstrate proactively to individuals, how we are processing their data. A draft Corporate Privacy Notice has been created and published to allow us to be more accountable and transparent about this.
- Consent – The rules around consent have been significantly strengthened under GDPR. A consent checklist has been drawn up to assist mangers/service areas who rely on consent as the lawful basis for processing personal data.
- Data Protection Impact Assessments – DPIA's are now mandatory for new technology implementations and projects that involve systematic monitoring of individuals and/or the large scale processing of special category data. It is envisaged that the Customer Relationship Management and Civil Parking Enforcement projects will require a DPIA, but the screening process will ultimately determine this.
- Incident Reporting – The Information Security Incident Reporting Policy has been amended and published, to align us with the requirements of GDPR. 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.
- The Information We Hold – The accountability principle states that we should document the data that we hold along with records of processing activities. Newport City Council already manages an Information Asset Register which is based upon the systems that have been identified as a priority. The task and finish group is currently working to expand this register to other areas of the authority, and to include paper records.
- Individuals Rights – Individuals rights are being strengthened under GDPR and this will be reflected in the privacy notices published (see above). We have amended and published our 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.
- Data Processor Responsibilities – Data Processors (organisations who process personal data on our behalf/contractors) will have further obligations under GDPR, and we need to include these obligations within our contracts with them. We have held discussions with the procurement team and the legal team to implement new contract clauses from 25th May 2018 and we are looking to communicate the changes in the law to existing contractors.

- Staff Training – The existing Information Security Training has been updated to cover all aspects of GDPR. An on-line version of the training will be created to cover any shortfall in training requirements.

Payment Card Industry Data Security Standards (PCI-DSS)

The council was previously compliant with Payment Security Industry (PCI) Data Security Standards. A previous audit carried out in conjunction with the internal audit team identified issues to be addressed. This action plan is not yet complete and this is currently being pursued by the SRS with the Information Management team. Accordingly, the council's PCI compliance has lapsed to ensure these issues are formally resolved to meet PCI requirements. Security scans continue to be carried out quarterly to ensure card data is secure when it is transmitted across the internet to the council's payment providers. No issues have been addressed by these scans which mitigates the risk of current non-compliance.

Wales Audit Office (WAO)

The Wales Audit Office (WAO) carries out audits annually which involve IT and Information Governance. The WAO visited to review a number of items in May 2016. One key area of improvement expected is to the council's business continuity and disaster recovery plans. Phase 1 of the project is complete but phase 2 now needs to be carried out by the Shared Resource Service (SRS). Information on the improvements being made are detailed further in the Business Continuity section of this report. Wales Audit Office is planning a 'Digital Risk Diagnostic' with the council with dates to be scheduled. This will provide an important external view of digital services.

2.2. 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. This is a major organisational change that affects governance for the council. The 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. Consideration will be given to a further survey to staff.

Organisation

The council's Senior Information Risk Owner (SIRO) role, responsible for Data Protection within the organisation, is part of the Head of Law and Regulation role. Day to day operational management is provided by the Information Management team that reports to the Head of People and Business Change. In line with requirements for GDPR, options are being considered for the role of Data Protection Officer which will be incorporated in to an existing job role as appropriate.

Data Protection Officer Role
Under General Data Protection Regulation (see section above) the council needs to specify its Data Protection Officer. Following a review of possible options this role was agreed to fit within the duties of the existing Digital Services Manager post. This has been formally agreed by the organisation and the Information Commissioner's Office (ICO) informed accordingly.

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. This represents a significant organisational change in the delivery of IT services. There is SRS representation on the council's Information Governance Group as well as other groups such as the council's Digital Board. The client side role is managed by the Digital team and this important relationship in service delivery as well as information governance will develop over time. Specific Governance arrangements are in place for the SRS including a Strategic Board, Finance and Governance Board and a Business and Collaboration Board.

Councillor Data Protection
Following guidance from the ICO, all councillors were registered as data controllers under the Data Protection Act. This is specifically for processing personal data in their advocacy role. Councillors will be registered every year on this basis.

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. This is being extended to meet the requirements of General Data Protection Regulation (GDPR) as detailed elsewhere in the report.

An important aim of this report is to ensure that members and senior officers are aware of the information security responsibilities of the council and to enable guidance to be provided. Council elections took place in May 2017 and there were a number of changes to members as a result. The annual risk report represents a useful opportunity for the Scrutiny Committee for Community Planning and Development to comment and make suggestions for scrutiny of 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 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. School representation was provided on the GDPR task and finish group.

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 weekly staff bulletin and on the intranet on various important subjects including GDPR.

An information security leaflet is provided to all staff attending training and is provided to other staff as necessary. 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.

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 is planned 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. **Attendance on classroom training courses this year is the highest ever completed by the organisation with a particular focus on Social Services staff** as detailed below.

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. There has been a particular emphasis on Social Services training following a serious incident reported to the Information Commissioner's Office (ICO) in 2015/16.Prioritisation of staff training has been carried out and additional courses were run to meet these demands. In 2017/18 the number of staff attending was 237 compared with 144 in 2016/17. **This is the highest number of Social Services staff trained in a single year.**

A breakdown per year is included below.

Year	Number of staff who attended
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 are scheduled on a monthly basis, primarily for staff other than Social Services although the content of courses was consolidated in 2015/16. The number of staff attending the corporate course was 114 compared with 118 in 2016/17. Attendance has been consistent over a number of years. Senior managers continue to be targeted and checks on attendance will continue.

Year	Number of staff who attended
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

No Councillor training took place this year although training has been carried out previously. All 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, all Councillors have been registered as data controllers under the Data Protection Act based on the processing they carry out in their advocacy role for constituents. Following discussion it was agreed that councillor training sessions be arranged probably in Autumn 2018.

Schools Courses

No specific information security courses for schools were run during 2017/18.Schools have been engaged with in relation to GDPR including representation on the task and finish group. Specific awareness raising sessions on GDOR were held with Primary and Secondary Head Teachers.

Other Courses and Presentations

For consistency and operational purposes staff are encouraged to attend standard corporate course where possible. Accordingly no other courses were run during the year.

Information Management Team Training
As a result of a vacancy both existing members of the Information Management team hold the British Computer Society (BCS) Certificate in Data Protection. One of the team attended a BCS conversion course for GDPR. Following recruitment it is anticipated that the new staff member will attend a BCS GDPR course.

E-Learning
All staff that need access to the council's computer network are required to undertake e-learning before they can access the network and this e-learning was revised during the year. This provides staff with an appreciation of their obligations in conjunction with a signed form to request access and agree to abide by the council's guidance. The e-learning is also published on the intranet as reference to staff and as a refresher.

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.

Updated policies

To ensure the Information Security Incident Reporting Policy reflects changes required for GDPR (see elsewhere in the report) this policy has been reviewed and updated accordingly. Policies are also reviewed generally to ensure that they are still valid and up to date.

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. The biggest risk identified is that of cyber security as the global threats have increased. Following guidance from central government staff guidance has been provided.

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. As above cyber security is considered one of the highest risks currently. High level information risks may be escalated up in to the Corporate Risk Register. Currently no information risks are identified as high level risks in the corporate reports. 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.

34 security incidents were recorded in 2017/18 compared with 43 in the previous year. This is the lowest number of recorded incidents during the period that the information risk report has been produced. It is difficult to establish whether this reflects an improved position or a reduced level of reporting. Previous consistency over the number of incidents would suggest that the reduced number of incidents is a positive sign.

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 incident	Other - principle 7 (security of personal information) incident	Technical security failing
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 usual, 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 procedures not being followed correctly – human error
- 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 mobile devices (with no personal data so low risk)
- Some personal printed information left on printers internally

The increased used of the corporate Electronic Document Management System (EDMS) and the further roll out of the Xerox Mail solution will continue to reduce the amount of paper handled and reduce the potential for mail errors.

The most significant incident during this year was one where old paper records where accidentally left in a property that was sold. These paper records were found by the new owner who notified the council. These records were collected from the new owner and stored/destroyed appropriately. The quantity of paper records and the type of information contained it were significant enough for this to be reported to the ICO. This incident was reviewed internally by the Information Management team with the service concerned and improvements made as a result. The ICO investigated the incident thoroughly and ultimately too no action against the council. Preventative measures taken and a comprehensive response to questions raised by the ICO were important factors in this decision making process.

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.

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 Information Management team leads on this work and has developed a number of ISP's with services and other organisations. Documentation for WASPI is being 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 2017/18:

Information Sharing Protocols (ISP's)

The Flying Start ISP went through the formal quality assurance process so is now complete. No Information Sharing Protocols have been completed and quality assured during this year.

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:-

Finalised DDA's in 2017/18:
Primary school to secondary school data transfer
Primary school and Assessment Foundation
WCCIS system for system go live

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).

As a result of previous guidance from the Wales Audit Office, the council is part way through a large project to improve business continuity. To date, new hardware has been set up with the migration of backups of key 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 progressed by the SRS.

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

The council plans to move to Microsoft Office 365 to provide improved collaborative, agile working facilities and information security.

Digital Champions

The council has approximately 50 “Digital Champions” who are advocates for the use of digital technology. They provide a key contact point for services using digital technology. They are one method of communicating messages to staff and also for testing the application of new systems.

Mobility solution

The use of a mobility solution has been rolled out for agile workers. This has improved 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. A security update to the solution has been rolled out.

Secure/Large File transfer solution

The roll out of the Egress Switch has now been completed with 2,590 users currently. 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 has enhanced Data Loss Prevention (DLP) facilities to scan e-mail for personal data. These facilities were made live during the year 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.

Identity Management

Microsoft Forefront Identity Management (FIM) software has been rolled out to enable users to reset network passwords themselves.

Xerox Mail "hybrid mail"
A new "hybrid mail" system continues to be rolled out to streamline the production of paper and electronic outputs. This enables documents to be sent to production printers in the print room and then processed through the mail room folder/inserter machine. This improves security by ensuring that print outputs are split in to envelopes automatically in the folder/inserter machine. The system needs to 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.

Desktop technology
The council has increased the percentage of laptops as part of its total number of computers used. This is to encourage more flexible and agile working with access to information and records from a variety of locations. Laptops continue to represent about 65% of all devices.

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 2200 desktop users across the council and including voicemail and the ability to access telephony from non council locations.

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 during this year with increased security features together with enhanced scanning facilities to drive the move to digital.

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. Supplier accounts are disabled when not in use and they need to ring IT before they are given access. All users needing access have to be authorised and are issued with a token for two-factor authentication, a small number of suppliers who may be required to support IT systems outside IT hours are also issued with a token.

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. Improvement to this infrastructure are planned for 2018/19.

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) 52 public buildings and on public transport (NewportCommunityCloud). Friendly Wi-Fi accreditation has been achieved for this set up.

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.

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. There are inherent risks in this change, with other organisations effectively holding the council's data. There will be on-going work to ensure that appropriate controls are in place.

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

2.8. Records Management

Resource issues slowed progress with the ongoing implementation of the corporate Electronic Document Management System (EDMS) across services. This resource issue has now been resolved and further progress is expected over the forthcoming year. This will include major updates to the system for both Social Services and corporate systems. 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.

There have been capacity issues with the council's Modern Records facility at the Civic Centre as a result of building moves. Additional space has been developed to provide further capacity. Options are being considered for 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 fourth time that the number of Freedom of Information (FOI) requests has been included. The number of requests received in 2017/18 was 1037 which is the first reduction in request numbers since records began in 2011/12. This represents 50 less requests than last year, a reduction of 4.6%. It is difficult to draw any firm conclusions as there is always an amount of variation, but it is believed that the proactive publication of data has had a positive effect by reducing the number of requests to some extent. Analysis shows less requests than 2016-17 for 6 out of 8 Service Areas with significantly more requests for Regeneration, Investment and Housing. Further analysis is required to understand any specific themes. Performance for 2017/18 was 88.3% of requests responded to within 20 working days. This was above the target of 88% of requests.

The previous year there were issues in certain areas of the council and performance in these areas have now improved. This year's performance was as a result of an increasing number of requests received and specific issues in certain areas of the council. During this year 194 of the requests were received via the online form.

A breakdown per year is included below.

Year	Number of requests	Performance (Target)
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 has been extended for a further year with options being considered for future years.

Publishing data

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

This page includes:-

- Council spend over £500
- Councillor allowances and expenses
- Business rates data
- Public health funerals
- Council pay and grading including gender pay gap information (new)
- Pupil numbers in Newport
- Newport Matters production costs

Gender pay gap information has been added this year following new regulation. Further appropriate data sets will be added as they are identified. 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. General Data Protection Regulation means that there will be no fee chargeable from May 2018 and this fee was removed in March 2018 in preparation for the new legislation. 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.

3. Risk Management and Associated Action Plan

As highlighted above the organisation has carried out a comprehensive programme over 2017/18 including particular emphasis on General Data Protection Regulation (GDPR). GDPR means that organisations need to be clearer and more transparent about how they process data. Organisations need to get a better understanding of what data they hold and the legal basis for the processing. Citizens are also provided with enhanced rights. Information risks change regularly and it is important to monitor these and take appropriate steps to mitigate. Whilst it is not anticipated that excessive fines will be issues to organisations by the ICO, the theoretical maximum fine is now 20 Millions Euros.

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 and a digital review is planned in early 2018.

The Information Commissioner's Office (ICO) took no action against the council as a result of the incident referred to the ICO by the council. Incidents continue to be investigated when they arise to respond to the incident effectively and learn lessons to minimise the likelihood of re-occurrence.

The Information Governance Group continues its important work of monitoring risk across services and providing strategic direction with representation form the Shared Resource Service (SRS) and this will require a different method of operation. The SRS client side role has been developed and this is recognised as an important 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 plans are being developed by the SRS to this end.

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?
Staff unaware of information risks and data breach occurs	H	L	Staff awareness raising especially around GDPR Provision of information security training Intranet content and staff bulletins Development of new policies and update of existing ones	Digital Services Manager (DSM) in conjunction with Information Management team
PSN (Public Services Network) accreditation not gained	H	L	Progress resolution of vulnerabilities identified by IT health check Evidence information governance arrangements as detailed in this document Extension of Information Asset Register and improved governance arrangements 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	Develop relationship with the SRS Develop client side role to provide strategic input and performance monitoring	Digital Services Manager (DSM) in conjunction with Head of PBC / SRS management
Unprepared to implement EU General Data Protection Regulations	M	M	Staff Awareness raising especially senior management Task and Finish Group creation and management Regular discussion 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	Complete actions identified in audit report Resubmission of self-assessment questionnaire and successful compliance achieved Continue technical scanning service to ensure no technical concerns	Digital Services Manager (DSM) in conjunction with in conjunction with SRS
Technical Solutions are not available to meet the needs of service	H	L	Egress Data Loss Prevention (DLP) system rolled out Continued roll out of Xerox Mail solution Encrypted laptop devices New Multi-Function Devices	Digital And Information Manager (DAIM) in conjunction with

delivery and data breach occurs			(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	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	Continue to review and refine priorities for critical IT systems Implement disaster recovery/business continuity improvements at Shared Resource Service (SRS) Work with SRS to develop consistent IT system priorities across partners where possible	SRS in conjunction with Digital Services Manager and services
Information security is not considered for new projects	M	L	Extend the implementation of Data Protection Impact Assessments Use ICO process including screening	Digital Services Manager in conjunction with services

3.2 Action Plan

Action	Deadline
Compliance and Audit	
PSN accreditation	
Follow up on Remediation Action Plan to ensure PSN compliance	Sep 18
EU General Data Protection Regulation (GDPR)	
Review Information Commissioner's Officer guidance on GDPR	On-going
GDPR to be discussed as standard item at Information Governance Group	On-going
Review legal basis for data processing	On-going
Information Asset Register to be extended	Dec 18
Finalise priority privacy notices for the organisation	Nov 18
Develop Data Protection Policy based on existing Information and IT Security Policy together with the corporate privacy notice	Mar 19
Conduct Data Protection Impact Assessments (DPIA's) where necessary	On-going
DPIA for new CRM system	Dec 18
DPIA for Office 365	Nov 18
PCI accreditation	
Payment Card Industry Data Security Standard actions as a result of audit to follow prioritised PSN work	Mar 19
Information Governance Culture and Organisation	
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
SIRO and Cabinet Member to be briefed on relevant information governance issues	On-going
Agree post to undertake Data Protection Officer (DPO) duties	May 18
Members updated through Annual Information Risk Management Report, including review by Scrutiny Committee	Nov 18
Communications and Awareness Raising	
Regular information security training sessions corporately and for Social Services including additional monthly courses to meet demand	On-going
Target senior managers for information security training.	On-going
Provide regular reminders and checks on attendance corporately and in Social Services	On-going
Information security training courses for councillors to be provided	Nov 18
Further policies and guidance will be developed to support the organisation	On-going
Existing policies and guidance will be reviewed and updated including reference to the information risk register to identify gaps in identified risk and supporting policies.	On-going
Provide advice and guidance to support schools with the Education service.	On-going
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	
Complete disaster recovery/business continuity improvements following previous WAO review.	Mar 19
Work with Shared Resource Service to consider alignment of priority systems across partners	Mar 19
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
Roll out of Office 365	Dec 18
Reduce access to cloud based personal network storage systems for staff	On-going
Extend use of Xerox Mail solution to improve mail distribution processes	On-going
Consider options and controls required for cloud-based systems	On-going
Review technical solutions to ensure they meet information governance needs	On-going
Consider the need for new technical solutions to address weaknesses	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
Identify and procure a new FOI system if required	Dec 18
Subject Access Requests	
Review Subject Access Request processes in line with GDPR	Mar 18
Extend use of EDMS solution for redaction of Subject Access Requests	Mar 18
Extend use of FOI request system for managing Subject Access Requests	Mar 18
New projects	
Carry out Data Protection Impact Assessment for relevant projects in conjunction with GDPR requirements	On-going